

The Open Group Snapshot

Technical Standard for SOSA™ Reference Architecture, Edition 2.0



You have a choice: you can either create your own future, or you can become the victim of a future that someone else creates for you. By seizing the transformation opportunities, you are seizing the opportunity to create your own future.

Vice Admiral (ret.) Arthur K. Cebrowski



NOTICE

Snapshot documents are draft standards, which provide a mechanism for The Open Group to disseminate information on its current direction and thinking to an interested audience, in advance of formal publication, with a view to soliciting feedback and comment.

A Snapshot document represents the interim results of an activity to develop a standard. Although at the time of publication The Open Group intends to progress the activity towards publication of a Preliminary Standard or (full) Standard of The Open Group, The Open Group is a consensus organization, and makes no commitment regarding publication. Similarly, a Snapshot document does not represent any commitment by any member of The Open Group to make any specific products available.

This Snapshot document is intended to make public the direction and thinking about the path we are taking in the development of the Technical Standard for SOSA Reference Architecture. We invite your feedback and guidance. To provide feedback on this Snapshot document, please send comments by email to ogsosa-admin@opengroup.us no later than March 1, 2023.

This Snapshot document is valid through March 1, 2023 only.

For information on joining The Open Group SOSA™ Consortium, please send email to ogsosa-admin@opengroup.us or visit our website at www.opengroup.org/sosa.

Approved for public release; distribution is unlimited.

Case: AFLCMC-2022-0161 CLEARED on 14 Jun 2022

For information on joining The Open Group SOSA™ Consortium, please send email to ogsosa-admin@opengroup.us or visit our website at www.opengroup.org/sosa.

Copyright © 2021, The Open Group

The Open Group hereby authorizes you to use this document for any purpose, PROVIDED THAT any copy of this document, or any part thereof, which you make shall retain all copyright and other proprietary notices contained herein.

This document may contain other proprietary notices and copyright information.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent or trademark of The Open Group or any third party. Except as expressly provided above, nothing contained herein shall be construed as conferring any license or right under any copyright of The Open Group.

Note that any product, process, or technology in this document may be the subject of other intellectual property rights reserved by The Open Group, and may not be licensed hereunder.

This document is provided “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at www.opengroup.org/library.

The Open Group Snapshot

Technical Standard for SOSA™ Reference Architecture, Edition 2.0

Document Number: S221

Authored by The Open Group SOSA™ Consortium.

Published by The Open Group, August 2022.

Comments relating to the material contained in this document may be submitted to:

The Open Group, 800 District Avenue, Suite 150, Burlington, MA 01803, United States

or by electronic mail to:

ogsosa-admin@opengroup.us

Contents

1	Introduction.....	1
1.1	Objective.....	1
1.2	Overview.....	2
1.2.1	Reference Architecture Description	3
1.2.2	Modular Open System Approach (MOSA) Fundamentals.....	3
1.2.3	Business Alignment.....	4
1.2.4	Reference Implementation Guide Description	5
1.3	Conformance Certification	5
1.4	Normative References.....	6
1.5	Terminology	6
1.6	Future Directions	6
2	Definitions.....	8
2.1.1	System Requirements	8
2.1.2	Specification Keywords	8
3	Architectural Drivers.....	10
3.1	Quality Attributes	10
3.2	Architecture Principles	12
3.2.1	Business-Oriented Architecture Principles.....	12
3.2.2	Technically-Oriented Architecture Principles	13
4	SOSA Architecture Overview.....	19
4.1	SV-1 (System Interface Description and Context)	19
4.1.1	SOSA Physical Context.....	20
4.2	SvcV-1 (Services Context Description).....	21
4.3	SvcV-2: Services Resource Flow Description.....	27
5	Technical Concepts and Overview.....	29
5.1	Taxonomy	29
5.2	Modular Decomposition Approach.....	31
5.3	Applying the Taxonomy to SOSA Procurable Units	31
5.4	System Management Approach	32
5.5	Airworthiness Concepts and Approach	33
5.5.1	Types of Equipment	34
5.5.2	Airworthiness of Mission Equipment.....	34
5.5.3	Qualification <i>versus</i> Airworthiness	34
5.6	Security Concepts and Approach.....	35
5.6.1	Security Manager	36
5.7	SOSA Data Model	36
5.7.1	Data Model Structure	36
5.7.2	DIV-1: Conceptual Data Model	36
5.7.3	DIV-2: Logical Data Model	37
5.7.4	DIV-3: Physical Data Model.....	37

	5.7.5	Data Model Formats and Usage	37
5.8		Inter-Module Interaction Approach	38
	5.8.1	Inter-Module Interactions	38
	5.8.2	SOSA Sensor Interconnects	38
6		System Management	40
6.1		System Management Architecture	40
	6.1.1	System Manager Functionality	42
	6.1.2	In-Band System Management Interactions	44
6.2		In-Band System Management Definitions	46
	6.2.1	In-Band System Management General Profile Technology Bindings	46
	6.2.2	In-Band System Management Definition Structure	47
	6.2.3	System Manager Module In-Band System Management Definitions	47
	6.2.4	Generic SOSA Module In-Band System Management Definitions	62
	6.2.5	Security Services Module In-Band System Management Definitions	67
	6.2.6	SOSA Chassis Manager In-Band System Management Definitions	76
	6.2.7	SOSA PIC In-Band System Management Definitions	83
	6.2.8	SOSA Plug-In Card with Software RTE In-Band System Management Definitions	92
6.3		Out-of-Band Hardware Management Overview	101
6.4		Out-of-Band Hardware Management Definitions	104
	6.4.1	Chassis Manager Out-of-Band System Management Definitions	107
	6.4.2	Hardware Element Out-of-Band System Management Definitions	107
6.5		SOSA Component State Management	111
	6.5.1	Sensor State Management	111
	6.5.2	PIC State Management	113
	6.5.3	Module State Management	116
	6.5.4	Secure System Start-Up	118
7		Task Management	124
7.1		Task Manager Module	124
	7.1.1	Module Definition	124
	7.1.2	Task Manager Interactions	125
	7.1.3	Task Manager Interaction Rules	127
8		Transmission/Reception	128
8.1		Conditioner-Receiver-Exciter	128
8.2		Emitter/Collector	130
8.3		RF Signal Layer Definitions	131
	8.3.1	Modular Open Radio Frequency Architecture (MORA)	132
	8.3.2	Application of MORA to RF Signal Layer Modules	132
	8.3.3	RF Conditioner-Receiver-Exciter Module	133
	8.3.4	RF Emitter/Collector Module	136
	8.3.5	RF Receiver-Exciter Interactions	138

8.3.6	RF Receiver-Exciter Rules	139
8.3.7	RF Signal Layer Interactions	139
8.3.8	RF Signal Layer Module Rules	147
8.4	EO/IR Definitions	148
9	Process Signals/Targets	149
9.1	Signal/Object Detector & Extractor	149
9.1.1	Signal/Object Detector & Extractor Interactions	150
9.1.2	Signal/Object Detector & Extractor Interaction Rules	150
9.2	Signal/Object Characterizer	150
9.2.1	Signal/Object Characterizer Interactions	151
9.2.2	Signal/Object Characterizer Interaction Rules	151
9.3	Image Pre-Processor	151
9.3.1	Image Pre-Processor Interactions	152
9.3.2	Image Pre-Processor Interaction Rules	152
9.4	Tracker	153
10	Analyze and Exploit	154
10.1	External Data Ingestor	154
10.2	Encoded Data Extractor	154
10.3	Situation Assessor	155
10.4	Impact Assessor & Responder	156
10.5	Storage/Retrieval Manager	156
11	Convey	158
11.1	Reporting Services	158
11.2	Reporting Services Interactions	158
12	Support System Operation	159
12.1	Security Services Module	159
12.1.1	Definition	159
12.1.2	Audit Subsystem	159
12.1.3	Key Management Service	162
12.1.4	Authentication Service	165
12.1.5	Authorization Service	168
12.1.6	Zeroization	169
12.1.7	Software Package Verification Service	170
12.2	Encryptor/Decryptor	171
12.2.1	Encryptor/Decryptor Common Rules	171
12.2.2	Encryptor/Decryptor Rules for Data-At-Rest Encryption (DARE)	175
12.3	Guard/Cross-Domain	176
12.4	Network Subsystem	176
12.5	Calibration Service	177
12.6	Nav Data Service	177
12.7	Time & Frequency Service	178
12.8	Compressor/Decompressor	178
12.9	SOSA Host Platform Interface	179
12.9.1	Definition	179
12.9.2	Host Platform Interface Interactions	180
12.9.3	Host Platform Interface Interaction Rules	180

12.10	Power	181
13	Hardware Element.....	182
13.1	PIC Use-Cases	182
13.2	SOSA Plug-in Cards Using OpenVPX.....	183
13.2.1	SOSA PICP Form Factors	183
13.2.2	SOSA PIC Common Electrical and Functional Requirements.....	183
13.2.3	Utility Plane Requirements	183
13.2.4	General Mechanical.....	185
13.2.5	Cooling Methods	189
13.2.6	Power Supply Card (PSC) General Rules	190
13.2.7	Mezzanine Cards	199
13.2.8	Maintenance Console Port.....	199
13.2.9	Overlays	201
13.2.10	Certificate of Volatility (CoV)	203
13.2.11	3U SOSA PICPs – General	204
13.2.12	6U SOSA PICPs – General.....	215
13.2.13	Legacy	223
13.3	Alternate Module Profile Scheme (AMPS)	226
13.3.1	SOSA AMPS Definitions.....	226
13.3.2	SOSA AMPS Introduction	226
13.3.3	Alternate Module Profile Scheme (AMPS) String Construct	232
13.3.4	SOSA 3U/6U Payload AMPS Format.....	235
13.3.5	SOSA 3U/6U Switch AMPS Format	238
13.3.6	Portion of the AMPS String for VITA 66 Connectors	240
13.3.7	SOSA AMPs Rules	241
13.3.8	Backplane Apertures for Analog and Optical Fiber	245
13.4	SOSA Plug-In Cards (PICs) Using VNX	252
13.4.1	Glossary.....	253
13.4.2	VNX+ Module Heights	253
13.4.3	VNX+ Connector and Aperture Fills	253
13.4.4	VNX+ System Clock.....	256
13.4.5	Utility Plane Requirements	256
13.4.6	General Mechanical.....	256
13.4.7	Thermal Design	257
13.4.8	VNX+ Payload Slot Profiles	257
13.4.9	Power Supply Cards (PSC) and Energy Storage Cards (ESC).....	264
13.4.10	Security Keying	264
13.5	SOSA Aperture and Chassis Electrical and Mechanical Interface Standard.....	265
13.5.1	Electrical Classes.....	265
13.5.2	SOSA Electrical Class 1 & 2 Sensor Electrical Interfaces	266
13.5.3	SOSA Electrical Class 3 Electrical Interfaces.....	309
13.5.4	SOSA Class 5 Electrical Mechanical Interfaces.....	344
13.5.5	SOSA Aperture Mechanical Interface Standard.....	350

14	SOSA Run-Time Environment	355
14.1	Overview.....	355
14.2	SOSA Configuration Files	357
14.3	FACE OSS Run-Time Environment Profile.....	359
14.3.1	FACE OSS Run-Time Environment	360
14.3.2	FACE OSS Module Software.....	361
14.3.3	FACE OSS Configuration File.....	361
14.4	SOSA Container Run-Time Environment Profile	361
14.4.1	SOSA Container Run-Time Environment.....	362
14.4.2	SOSA Module Software for Container Profile.....	363
14.4.3	SOSA Container Configuration File	364
14.5	SOSA Virtual Machine Run-Time Environment Profile	364
14.5.1	SOSA Virtual Machine Run-Time Environment	366
14.5.2	SOSA Module Software for Virtual Machine Profile	366
14.5.3	SOSA Virtual Machine Configuration File.....	366
14.6	Mixed Run-Time Environments	367
15	Inter-Module Interactions.....	368
15.1	Interactions on the SOSA Message Interconnect.....	368
15.2	Application Programming Interface (API)	370
15.3	Quality of Service (QoS)	371
15.4	Data Product and Task Management Interaction Implementation.....	373
15.4.1	Interaction Implementation Concepts.....	373
15.4.2	Interaction Binding Technology Selections	374
15.4.3	OMG DDS Technology Binding Rules.....	375
15.4.4	Protobuf + AMQP Technology Binding Rules	375
15.4.5	Protobuf +ZMTP Technology Binding Rules	376
15.4.6	NFS Transfer Technology Binding Rules	377
15.4.7	Default Technology Binding Rules	378
15.5	Inter-Module Abstraction Overview.....	378
15.6	Module Interaction Types.....	378
15.6.1	Security for Inter-Module Interactions.....	378
15.6.2	Interaction Endpoints and Roles.....	379
15.6.3	Interactions on a Wideband Low-Latency Interconnect.....	381
15.6.4	Interactions on a SOSA Message Interconnect	382
15.7	SvcV-3b: Services-Services Matrix.....	383
A	AV-2 Integrated Dictionary	384
B	SOSA Data Model and OpenAPI Specifications (Normative)	390
B.1	SOSA Data Model (DIV-1, DIV-2, and DIV-3).....	390
B.2	System Manager In-Band System Management Interface OpenAPI Specification Definition.....	390
B.3	Generic SOSA Module In-Band System Management Interface OpenAPI Specification Definition.....	390
B.4	Security Services In-Band System Management Interface OpenAPI Specification Definition.....	390
B.5	Chassis Manager In-Band System Management Interface OpenAPI Specification Definition.....	390
B.6	PIC In-Band System Management Interface OpenAPI Specification Definition.....	391

B.7	PIC with SW RTE In-Band System Management Interface OpenAPI Specification Definition.....	391
C	Security Attributes SOSA Security Module Overlay for Specialty Signals (Available on the Air Force VLD Website).....	392

Table of Figures

Figure 1.1-1: SOSA CV-1	2
Figure 1.2.2-1: SOSA Architectural Development Process	4
Figure 4.1-1: SV-1 for Nominal Case	20
Figure 4.1-2: SV-1 for Sensor Pod Special Case.....	20
Figure 4.2-1: SvcV-1 Top-Level SOSA Services Context Description	22
Figure 4.3-1: SvcV-2: Top-Level SOSA Service Resource Flow Description for Edition 1.0	28
Figure 5.1-1: SOSA Taxonomy.....	30
Figure 5.8.2-1: Default SOSA Sensor Interconnects.....	39
Figure 6.1-1: SOSA System Management Architectural Approach.....	41
Figure 6.1-2: SOSA Out-of-Band System Management Architectural Realization: VPX Form Factor	42
Figure 6.1.1-1: System Manager Functional Decomposition	42
Figure 6.1.2-1: SOSA System Management Client/Server Interactions Paradigm	45
Figure 6.1.2-2: SOSA In-Band System Management Manager/Agent Paradigm	46
Figure 6.3-1: SOSA Hardware System Management Logical Block Diagram	102
Figure 6.3-2: Example SOSA System Management Backplane/Chassis Implementation	103
Figure 6.3-3: Example SOSA System Management Plug-In Card Implementation.....	104
Figure 6.5.1-1: SOSA Sensor State and Transitions Diagram.....	112
Figure 6.5.2-1: SOSA PIC State and Transitions Diagram	114
Figure 6.5.3-1: SOSA Module State and Transitions Diagram	116
Figure 6.5.4-1: Sensor System Start-Up Decomposition.....	119
Figure 6.5.4-2: SOSA System Security States	120
Figure 6.5.4-3: SOSA PIC/Module Security States.....	121
Figure 7.1.2-1: Initiating Mission Task.....	125
Figure 7.1.2-2: Task Manager Coordinating Mission Execution Loop and Conveying Status to the Host Platform Interface Module	126
Figure 7.1.2-3: Task Manager Coordinating Mission Task Updates.....	126
Figure 8.3.2-1: RF Signal Layer Module Interactions.....	133
Figure 8.3.3-1: RF Conditioner Receiver/Exciter Interactions (Refer to Table 8.1-1).....	134
Figure 8.3.4-1: RF Emitter/Collector Interactions (Refer to Table 8.3.4-1).....	137
Figure 12.1.2.2-1: Sample of Audit Subsystem Configuration within a SOSA Security Services Module	160
Figure 12.2.1-1: SOSA-Aligned Data-At-Rest Encryption (DARE) Architecture and Use- Cases.....	172
Figure 13.1-1: High-Level SOSA Use-Case	182
Figure 13.2.4.2-1: Module Width of 100mm 3U VPX Card.....	187
Figure 13.2.4.2-2: Wedge Lock Location of 100m 3U VPX Card.....	188
Figure 13.2.4.3-1: PCB Depth of 100mm 3U VPX Card	188
Figure 13.2.9-1: AUXCLK/RECLK Distribution Overlay	202
Figure 13.2.11.1-1: ANSI/VITA 65.0 3U I/O-Intensive SBC Slot Profile SLT3-PAY- 1F1F2U1TU1T1U1T-14.2.16.....	205
Figure 13.2.11.2-1: ANSI/VITA 65.0 Payload Slot Profile SLT3-PAY- 1F1U1S1S1U1U2F1H-14.6.11-n	206
Figure 13.2.11.2-2: ANSI/VITA 65.0 Payload Slot Profile SLT3-PAY- 1F1U1S1S1U1U4F1J-14.6.13-n.....	206
Figure 13.2.11.3-1: ANSI/VITA 65.0 Switch Slot Profile SLT3-SWH-6F8U-14.4.15	209

Figure 13.2.11.4-1: ANSI/VITA 65.0 Data/Control Plane Switch Slot Profile SLT3-SWH-6F1U7U-14.4.14.....	210
Figure 13.2.11.4-2: ANSI/VITA 65.0 Data/Control Plane Switch Slot Profile SLT3-SWH-4F1U7U1J-14.8.7-n.....	210
Figure 13.2.11.5-1: ANSI/VITA 65.0 Radial Clock Slot Profile SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n.....	211
Figure 13.2.11.6-1: ANSI/VITA 65.0 3U External I/O Slot Profile SLT3-PAY-2U2U-14.2.17.....	213
Figure 13.2.11.7-1: ANSI/VITA 65.0 3U Payload Slot Profile SLT3-PAY-1F1U1S1S1U1U1K-14.6.14-n.....	214
Figure 13.2.12.1-1: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n.....	216
Figure 13.2.12.1-2: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n.....	217
Figure 13.2.12.2-1: ANSI/VITA 65.0 6U Data/Control Switch Slot Profile SLT6-SWH-14F16U1U15U1J-10.8.1-n.....	219
Figure 13.2.12.3-1: ANSI/VITA 65.0 6U External I/O Slot Profile SLT6-PAY-4U2U-10.2.8.....	221
Figure 13.2.12.4-1: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n.....	222
Figure 13.2.13.1-1: ANSI/VITA 65.0 Payload Slot Profile for SLT3-PAY-2F2U-14.2.3.....	224
Figure 13.2.13.2-1: ANSI/VITA 65.0 Switch Slot Profile for SLT6-SWH-16U20F-10.4.2.....	225
Figure 13.3.3-1: Alternative Module Profile Scheme (AMPS) String Construct.....	232
Figure 13.3.7.2-1: Ethernet Backplane Connectivity Decision Tree.....	243
Figure 13.3.8.1-1: PIC Signal Chain Position.....	246
Figure 13.3.8.3-1: ANSI/VITA 67.3 10_SMPM_contacts-6.4.5.6.3 Coaxial Pin Locations (viewed from the PIC side of the backplane).....	247
Figure 13.3.8.4-1: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Coaxial Pin Locations (viewed from the PIC side of the backplane).....	248
Figure 13.3.8.4-2: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Decision Tree.....	250
Figure 13.3.8.5-1: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Coaxial Pin Locations (viewed from the PIC side of the backplane).....	250
Figure 13.3.8.5-2: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Coaxial Pin Designations.....	251
Figure 13.3.8.5-3: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Decision Tree.....	252
Figure 13.4.2-1: 19mm VNX PIC with No Aperture.....	253
Figure 13.4.3-1: VNX+ PIC Small Aperture Dimensions.....	254
Figure 13.4.3-2: VNX+ PIC Large Aperture Dimensions.....	254
Figure 13.4.8.1.1-1: VNX+ 240-Pin Payload Slot Profiles.....	259
Figure 13.4.8.1.2-1: VNX+ 320-Pin Payload Slot Profiles.....	260
Figure 13.4.8.1.3-1: VNX+ 400-Pin Payload Slot Profiles.....	260
Figure 13.4.8.2.1-1: VNX+ 320-Pin DP/CP Switch Slot Profile, with Optical.....	261
Figure 13.4.8.2.2-1: VNX+ 400-Pin DP/CP Switch Slot Profile, no Optical.....	262
Figure 13.4.8.3.1-1: VNX+ 320-Pin Payload with Radial Clock Slot Profile.....	263
Figure 13.4.8.3.2-1: VNX+ 320-Pin Radial Clock Slot Profile.....	264
Figure 13.5.2.2-1: J1-DCPower Connector Pin Arrangement.....	269
Figure 13.5.2.3-1: J2-Signal Connector Pin Arrangement.....	271
Figure 13.5.2.3.9-1: Input Time Rollover Pulse (1 PPS) Signal Characteristics.....	280
Figure 13.5.2.4-1: J3-Video Connector Pin Arrangement.....	281
Figure 13.5.2.5-1: J4-Fiber Optics Connector Pin Arrangement.....	283
Figure 13.5.2.7-1: J6-DC Auxiliary Power Connector Pin Arrangement.....	286
Figure 13.5.2.8-1: J7-High Speed Electrical Connector Pin Arrangement.....	288
Figure 13.5.2.9-1: J8 RF Connector Pin Arrangement.....	292
Figure 13.5.2.9-2: Size 12 Pin and Socket.....	294

Figure 13.5.2.11-1: J9 RF Connector Pin Arrangement	295
Figure 13.5.2.11-2: Size 8 Pin and Socket	296
Figure 13.5.2.13-1: J10-AC Power Connector Pin Arrangement.....	297
Figure 13.5.2.14-1: J11 High Voltage DC Connector Pin Arrangement	299
Figure 13.5.2.15-1: J12 Key Fill Connector Pin Arrangement.....	300
Figure 13.5.2.16-1: J13 Key Fill Connector Pin Arrangement.....	302
Figure 13.5.2.17.1-1: Mechanical Transfer Ferrule Pin Out	304
Figure 13.5.2.17.2-1: J14 High Density Fiber Connector (4 MT).....	307
Figure 13.5.2.18-1: J15 High Density Fiber Connector (1 MT).....	308
Figure 13.5.2.19-1: J16 External Battery Connector Pin Arrangement.....	309
Figure 13.5.3.2-1: J1-DC Power Connector Pin Arrangement.....	313
Figure 13.5.3.3-1: J2-Signal Connector Pin Arrangement	315
Figure 13.5.3.4-1: J3-Video Connector Pin Arrangement.....	323
Figure 13.5.3.5-1: J4-Fiber Optics Connector Pin Arrangement.....	324
Figure 13.5.3.7-1: J6-DC Auxiliary Power Connector Pin Arrangement.....	326
Figure 13.5.3.8-1: J7-High Speed Electrical Connector Pin Arrangement.....	329
Figure 13.5.3.9-1: J8-RF Connector Pin Arrangement.....	334
Figure 13.5.3.9-2: Size 12 Pin and Socket	335
Figure 13.5.3.10-1: J9-Low Loss RF Connector Pin Arrangement	336
Figure 13.5.3.10-2: Size 8 Pin and Socket	337
Figure 13.5.3.12-1: J11 High Voltage DC Connector Pin Arrangement	338
Figure 13.5.3.13-1: J12 Key Fill Connector Pin Arrangement.....	340
Figure 13.5.3.14-1: J13 Key Fill Connector Pin Arrangement.....	341
Figure 13.5.3.15.2-1: J14 High Density Fiber Connector (2 MT).....	342
Figure 13.5.3.16-1: J15 High Density Fiber Connector (1 MT).....	343
Figure 13.5.3.17-1: J16-External Battery Connector Pin Arrangement	343
Figure 13.5.4.2-1: Class 3 J1 Pin Assignments	345
Figure 13.5.5.6.1-1: Mechanical Class c-2-5-15 Mounting Detail	354
Figure 14.1-1: SOSA Run-Time Environment Interface	355
Figure 14.1-2: Sample SOSA Composition with Multiple RTE Profiles	356
Figure 14.3-1: SOSA Operating System Run-Time Environment Profile.....	360
Figure 14.4-1: SOSA Container Run-Time Environment Profile	362
Figure 14.5-1: Type 1 Hypervisor	365
Figure 14.5-2: Type 2 Hypervisor	365
Figure 15.4.6-1: Sequence Diagram of General Flow of the File Transfer Interaction Type between the Writer and the Reader.....	377

Table of Tables

Table 3.1-1: SOSA Quality Attributes (in order of decreasing precedence)	10
Table 4.2-1: SvcV-1 Module Descriptions	22
Table 6.1.1-1: SOSA System Manager Functions (SvcV-4)	43
Table 6.2.3.1-1: SOSA System Manager Module In-Band System Management Functions	47
Table 6.2.3.2-1: System Manager Module In-Band System Management Interactions	56
Table 6.2.4.1-1: Generic SOSA Module In-Band System Management Functions	62
Table 6.2.4.2-1: Generic SOSA Module In-Band System Management Interactions	65
Table 6.2.5.1-1: Security Services Module In-Band System Management Functions	67
Table 6.2.5.2-1: Security Services Module In-Band System Management Interactions	73
Table 6.2.6.1-1: Chassis Manager In-Band System Management Functions	77
Table 6.2.6.2-1: Chassis Manager In-Band System Management Interactions	80
Table 6.2.7.1-1: SOSA Plug-In Card In-Band System Management Functions.....	84
Table 6.2.7.2-1: SOSA Plug-In Card In-Band System Management Interactions.....	88
Table 6.2.8.1-1: SOSA PIC with SW RTE In-Band System Management Functions.....	92
Table 6.2.8.2-1: PIC with SW RTE In-Band System Management Interactions.....	97
Table 6.4.2-1: Selected Specifications from ANSI/VITA 65.0 §3.3.1	108
Table 6.4.2-2: Selected Specifications from ANSI/VITA 65.0 §3.3.3	109
Table 7.1.1-1: Task Manager Module Description (SvcV-1)	124
Table 7.1.2-1: Task Manager Interactions	127
Table 8.1-1: Conditioner-Receiver-Exciter Functions (SvcV-4).....	128
Table 8.2-1: Emitter/Collector Functions (SvcV-4)	130
Table 8.3.3-1: Conditioner-Receiver-Exciter Functions.....	135
Table 8.3.4-1: Emitter/Collector Functions	137
Table 8.3.5-1: RF Receiver-Exciter Interactions	138
Table 8.3.7-1: RF Signal Layer Interactions	140
Table 9.1-1: SOSA SvcV-1: Module Descriptions.....	149
Table 9.1.1-1: Signal/Object Detector & Extractor Interactions	150
Table 9.2-1: SOSA SvcV-1 – Module Descriptions.....	150
Table 9.2.1-1: Signal/Object Characterizer Interactions	151
Table 9.3-1: SOSA SvcV-4 – Image Pre-Processor	152
Table 9.3.1-1: Image Pre-Processor Interactions.....	152
Table 10.1-1: SOSA SvcV-4 – External Data Ingestor	154
Table 10.2-1: SOSA SvcV-4 – Encoded Data Extractor	154
Table 10.3-1: SOSA SvcV-4 – Situation Assessor.....	155
Table 10.4-1: SOSA SvcV-4 – Impact Assessor & Responder	156
Table 10.5-1: SOSA SvcV-4 – Storage/Retrieval Manager	157
Table 11.1-1: SvcV-1 – Module Descriptions	158
Table 11.2-1: Reporting Services Interactions	158
Table 12.1.2.1-1: Identifies and Defines Terms Specific to the Audit Subsystem	159
Table 12.1.3-1: Key Management Interactions	164
Table 12.1.4-1: Authentication Interactions	167
Table 12.1.5-1: Authorization Interactions.....	169
Table 12.1.6-1: Zeroization Interactions	170
Table 12.1.7-1: Software Package Verification Interactions	171
Table 12.1.7-2: SOSA SvcV-4 – Security Services	171
Table 12.2.1-1: Zeroization Interactions	174

Table 12.2.2-1: SOSA SvcV-4 – Encryptor/Decryptor	175
Table 12.3-1: SOSA SvcV-4 – Guard/Cross-Domain Service	176
Table 12.4-1: SOSA SvcV-4 – Network Subsystem	176
Table 12.5-1: SOSA SvcV-4 – Calibration Service	177
Table 12.6-1: SOSA SvcV-4 – Nav Data Service	178
Table 12.7-1: SOSA SvcV-4 – Time & Frequency Service	178
Table 12.8-1: SOSA SvcV-4 – Compressor/Decompressor	179
Table 12.9.1-1: SvcV-1 Module Descriptions	179
Table 12.9.2-1: Host Platform Interface Interactions	180
Table 12.10-1: SOSA SvcV-4 – Power	181
Table 13.2.4.2-1: Primary Side Retainer Dimensions for 3U Conduction Cooled Cards	186
Table 13.2.4.2-2: Secondary Side Retainer Dimensions for 3U Conduction Cooled Cards.....	187
Table 13.2.5-1: SOSA PIC Cooling Methods	189
Table 13.2.6-1: 3U P0 Connector Pin Out.....	191
Table 13.2.6-2: 6U P0 Connector Pin Out.....	192
Table 13.2.6-3: 6U P1 Connector Pin Out.....	193
Table 13.2.6.5-1: ENABLE* and INHIBIT* Values	197
Table 13.2.8.4-1: Maintenance Console Port Signal Levels.....	200
Table 13.2.9-1: SLT3-PAY-1F1F2U1TU1T1U1T-14.2.16 Overlay Description	202
Table 13.2.9-2: SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n Overlay Description	202
Table 13.2.11.2-1: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U2F1H- 14.6.11-n.....	207
Table 13.2.11.2-2: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U4F1J- 14.6.13-n.....	207
Table 13.2.11.4-1: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U4F1J- 14.8-7-n	211
Table 13.2.11.5-1: ANSI/VITA 65.1 Slot Profiles for SLT3x-TIM-2S1U22S1U2U1H- 14.9.2-n.....	212
Table 13.2.11.5-2: Selected Rules from ANSI/VITA 65.0	212
Table 13.2.11.7-1: ANSI/VITA 65.1 Slot Profile for SLT3-PAY-1F1U1S1S1U1U1K- 14.6.14-n.....	215
Table 13.2.12.1-1: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY- 4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n.....	218
Table 13.2.12.1-2: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY- 4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n.....	218
Table 13.2.12.2-1: ANSI/VITA 65.1 Slot Profiles for SLT6-SWH-14F16U1U15U1J- 10.8.1-n.....	220
Table 13.2.12.4-1: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY- 4F2Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n.....	223
Table 13.3.2-1: ANS Example Using VITA 65 MOD3-PAY-1F1U1S1S1U1U4F1J- 16.6.13-n.....	228
Table 13.3.2-2: SOSA Protocol Summary	228
Table 13.3.3-1: AMPS Parameters	232
Table 13.3.3-2: Protocol Field Examples Where ANS Specifies One Fat Pipe	234
Table 13.3.3-3: Protocol Field Examples Where ANS Specifies Four Fat Pipes	234
Table 13.3.3-4: Protocol Field Examples Where ANS Specifies 8 Lanes.....	234
Table 13.3.3-5: Examples of Depth, Cooling, and Pitch	235
Table 13.3.3-6: Depth, Cooling, and Pitch Combination Supported in This Document	235
Table 13.3.4-1: Summary of 3U Payload Plug-In Card Profiles (PICPs).....	236
Table 13.3.4-2: Summary of 6U Payload Plug-In Card Profiles (PICPs).....	237
Table 13.3.4-3: Examples of Full AMPS Strings from PICPs of Table 13.3.4-1 and Table 13.3.4-2.....	237

Table 13.3.5-1: Summary of Switch Plug-In Card Profiles (PICPs)	239
Table 13.3.5-2: Examples of Full AMPS Strings from SOSA PICPs	239
Table 13.3.6-1: Examples of Protocol Fields for VITA 66 Connectors	240
Table 13.3.7.2-1: Protocol Support Levels for SLE1 and SLE2	245
Table 13.3.8.1-1: Terminology, Signal Definitions, and MORA Mapping	246
Table 13.3.8.3-1: ANSI/VITA 67.3 10_SMPM_contacts-6.4.5.6.3 Coaxial Pin Designations.....	248
Table 13.3.8.4-1: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Coaxial Pin Designations.....	249
Table 13.4.1-1: Glossary	253
Table 13.4.3.1-1: 19mm VNX Connector and Aperture Fills	254
Table 13.4.3.2-2: 39mm VNX+ Connector and Aperture Configurations	255
Table 13.4.7-1: Heat Transfer Mechanisms	257
Table 13.5.1-1: Turreted SOSA Sensor Electrical Classes.....	265
Table 13.5.1.1-1: Acceptable Input Power Specifications.....	266
Table 13.5.2.1-1: Class 1 & 2 Sensor Connectors	268
Table 13.5.2.2-1: J1-DC Power Connector Pin Allocation	270
Table 13.5.2.3-1: J2-Signal Connector Pin Allocation	272
Table 13.5.2.4-1: J3-Video Connector Pin Allocation	281
Table 13.5.2.5-1: J4-Fiber Optics Connector Pin Allocation	283
Table 13.5.2.6-1: J5-GPS Connector Pin Allocation.....	285
Table 13.5.2.7-1: J6-DC Auxiliary Power Connector	286
Table 13.5.2.8-1: J7-High Speed Electrical Pin Allocations	288
Table 13.5.2.9-1: J8 RF Pin Allocations	293
Table 13.5.2.10-1: VSWR and Frequency Range	294
Table 13.5.2.11-1: J9 RF Pin Allocation	295
Table 13.5.2.11.1-1: Size 8 Connector VSWR Requirements.....	297
Table 13.5.2.12-1: Auxiliary RF Connections.....	297
Table 13.5.2.13-1: J10-AC Power Pin Allocations	298
Table 13.5.2.14-1: J11 High Voltage DC Power Pin Allocations	299
Table 13.5.2.15-1: J12 Key Fill Connector Pin Out Details.....	300
Table 13.5.2.16-1: J13 Key Fill Connector Pin Out Details when used with the TIA 232 Protocol.....	302
Table 13.5.2.16-2: J13 Key Fill Connector Pin Out Details when used with the TIA 485 Protocol.....	303
Table 13.5.2.17.1-1: High Density MT Connector MT Pin Allocation.....	304
Table 13.5.2.19-1: J16 External Battery Connector Pin Allocation	308
Table 13.5.3.1-1: Class 3 Sensor Connectors	311
Table 13.5.3.2-1: J1-DC Power Connector Pin Allocation	313
Table 13.5.3.3-1: J2-Signal Connector Pin Allocation.....	315
Table 13.5.3.4-1: J3-Video Connector Pin Allocation	323
Table 13.5.3.5-1: J4-Fiber Optics Connector Pin Allocation	325
Table 13.5.3.6-1: J5-GPS Connector Pin Allocation.....	326
Table 13.5.3.7-1: J6-DC Auxiliary Power Connector Pin Allocation	327
Table 13.5.3.8-1: J7-High Speed Electrical Pin Allocations	329
Table 13.5.3.9-1: J8-RF Connector Pin Allocations.....	334
Table 13.5.3.9.1-1: Size 12 Connector Frequency Range and VSWR Requirements	335
Table 13.5.3.10-1: J9-Low Loss RF Connector Pin Allocation	336
Table 13.5.3.10.1-1: Size 8 Connector Frequency Range and VSWR Requirements	337
Table 13.5.3.11-1: Auxiliary RF Connections.....	338
Table 13.5.3.12-1: J11 High Voltage DC Power Pin Allocations	338
Table 13.5.3.13-1: J12 Key Fill Connector Pin Out Details.....	340
Table 13.5.3.14-1: J13 Key Fill Connector Pin Arrangement	341
Table 13.5.3.17-1: J16 External Connector Pin Arrangement.....	344

Table 13.5.4.2-1: Class 3 J1 Pin Locations	345
Table 13.5.4.3-1: J2 GPS Connector Pin Allocation	350
Table 13.5.5.1-1: SOSA Sensor Mechanical Classes	351
Table 13.5.5.1-2: SOSA Sensor Mechanical Classes	352
Table 14.1-1: SOSA Run-Time Environment Profiles	356
Table 14.5-1: Virtual Machine Types.....	364
Table 15.1-1: Interaction Types	369
Table 15.3-1: SOSA QoS Attribute Units and Ranges	373
Table 15.4.2-1: Interaction Bindings and Interaction Types on the SOSA Message Interconnect	375
Table 15.6.2-1: Interaction Roles, Endpoints, and Symbols	380
Table 13.5.3.3.3-1: AV-2 Integrated Dictionary (Master Glossary of SOSA Terminology)	384

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 870 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

This Document

This is a Snapshot document of what is intended to become the Technical Standard for SOSA™ (Sensor Open Systems Architecture) Reference Architecture, Edition 2.0. This document is developed and maintained by The Open Group SOSA Consortium.

Executive Summary

This document is a Snapshot document of the Technical Standard for SOSA™ Reference Architecture, Edition 2.0 in support of United States Department of Defense (DoD) C5ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance) development.

The goal of The Open Group SOSA Consortium is to develop open architecture at the right level for Communications (Comms), Electro-Optical/Infra-Red (EO/IR), Electronic Warfare (EW), Radar, and Signals Intelligence (SIGINT) systems. The open architecture supports airborne, subsurface, surface, ground, and space. The SOSA Consortium strives to develop an ecosystem

that allows interoperability, reuse, and faster delivery of products to market through vertical integration from cables, mechanical interfaces, hardware, software, and system designs.

Background

Today's development of sensor systems typically entails a unique set of requirements and a single vendor. This form of development has served the military sensor community well; however, this stovepipe development process has had a great deal of undesired side-effects including long lead times, cumbersome improvement processes, lack of hardware, software, and system reuse between various sensors and platforms that result in platform-unique designs that are locked to a single deployed platform.

As the complexity of sensor and mission equipment has increased, this has resulted in increased cost and development times, and impeded the ability to integrate new hardware, software, or entire payloads into deployable platform systems. This – combined with the extensive testing and airworthiness/ground/sea/space qualification requirements – has begun to affect the ability of the military sensor community to rapidly deploy new capabilities across the military fleet.

The current sensor community procurement system does not promote the process of hardware, software, and payload reuse. Furthermore, the sensors development community has not created standards that facilitate the reuse of components.

Part of the reason for this is the relatively small size of the military market. Another contributing factor is the difficulty of developing qualified sensor payloads. An additional problem is the inability to use current commercial standards because they do not adhere to the stringent safety requirements intended to reduce risk and the likelihood of loss of host platform, reduced mission capability, and ultimately loss of life.

To counter these trends, the United States Air Force, Army, and Navy, in partnership with the Defense Industry are promoting a new approach.

Approach

The SOSA initiative, formed as a Consortium of The Open Group, addresses the challenges of rapid, affordable capability evolution for today's military community. Part of the SOSA approach is to develop an Open Systems Architecture (OSA), captured in the SOSA Technical Standard, that addresses software, hardware, and interfaces. This OSA is designed to promote software, hardware, and interface portability and create product families across the Communications, EO/IR, EW, Radar, and SIGINT community. The SOSA Technical Standard is intended to promote the development of reusable sensor components applicable to a broad class of sensors and host platforms.

Additionally, there is a need to develop an Open Business Model that addresses the needs of the acquisition community and ensures a strong (and responsive) industrial base. It includes business processes to adapt the procurement to a Modular Open Systems Approach (MOSA) reality, protect industry Intellectual Property (IP), and incentivize industry to invest in broadly applicable technologies that can be applied to a wide variety of sensors.

The SOSA approach allows “capabilities” to be developed as components that are exposed to other components through well-defined interfaces. It also provides for the reuse of SOSA module functionality across different environments. A SOSA module will have a core set of mandatory functionalities, but different variants could be developed over time and different

systems could have different additional characteristics (e.g., special environmental conditions, higher throughput, higher reliability, etc.). These variants will be considered for incorporation into a future version of this document. The SOSA Technical Standard does not guarantee compliance with any safety certification standard, but instead provides all the necessary capabilities to achieve that in the implementation phase by the vendors.

Ultimately, the key objectives of the SOSA Consortium are to:

- Reduce tech refresh cycles and the time it takes to field new or updated sensor capabilities
- Reduce the time it takes to integrate any new or updated capabilities through the use of well-defined and key interfaces
- Maximize the reuse of all new and updated sensor capabilities across application classes

Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo are trademarks of The Open Group.

Data Distribution Service and DDS are trademarks of Object Management Group, Inc. in the United States and/or other countries.

Google is a registered trademark of Google LLC.

Java is a registered trademark of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

NVM Express is a registered trademark of NVM Express, Inc.

OpenVPX, VITA, and VNX+ are trademarks of VITA in the United States and other countries.

POSIX is a trademark of the Institute of Electrical and Electronic Engineers, Inc.

Python is a trademark of the Python Software Foundation.

SAE is a trademark of SAE International.

SAE ITC is a registered trademark of the SAE Industry Technologies Consortia.

Solaris is a registered trademark of Oracle and/or its affiliates in the United States and other countries.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Acknowledgements

(Please note affiliations were current at the time of approval.)

The Open Group gratefully acknowledges the contribution of the following people in the development of this document:

Principal Authors

- Darren Abbott, AFLCMC, Inter-Module Interactions SC
- Gerry Bezenek, Sierra Nevada, Hardware SC
- Nick Borton, SRC, Vice Chair Steering Committee
- Matt Brasher, AREA-I, Electrical Mechanical SC
- Ken Braund, Meritec, Electrical Mechanical SC
- Tim Brett, MITRE, Inter-Module Interactions SC
- Jeffrey Bryant, BAE Systems, Co-Lead Data Model SC
- Jonathan Cain, Raytheon, Electrical Mechanical SC
- Michael Clark, Riverside Research, Co-Lead Security SC
- Paul Clarke, Northrop Grumman., Co-Lead Data Model SC
- Charles Patrick Collier, C5ISR Center, Co-Lead Hardware SC, & Chair Conformance SC
- George Dalton, KeyW, Vice Chair Business WG
- Steven Davidson, Raytheon, Former Vice-Chair SOSA Steering Committee
- Steven Devore, Leonardo DRS, Hardware SC
- Jason Dirner, US Army, Chair TWG
- Steve Edwards, Curtiss Wright, Co-Lead Security SC
- Nathan Franz, Inter-Module Interactions SC
- David Gash, Behlman Electronics, Hardware SC
- Jay Grandin, Annapolis Micro Systems, Hardware SC
- Matthew Hannah, GTRI, Inter-Module Interactions SC
- CW Hinkle, Ascendant Engineering Solutions, Electrical Mechanical SC
- Tom Hoch, Collins Aerospace, Electrical Mechanical SC
- Tim Ibrahim, L3Harris, Electrical Mechanical SC
- Steve Jones, Meritec, Electrical Mechanical SC
- Chris Kellow, US Army, Vice-Chair TWG

- Grant Lawton, Gore, Electrical Mechanical SC
- Mark Littlefield, Kontron, Member of Hardware SC, Vice-Chair Conformance SC, & Co-Lead Small Form Factor SC
- Domenic LoPresti, SV Microwave, Electrical Mechanical SC
- Michael Majors, DCS Corp, Co-Lead Software Environment SC
- Paul Mesibov, Pentek, Co-Lead Hardware SC
- Michael Scott Moore, US Army, Co-Lead Inter-Module Interactions SC
- Scott Newland, L3Harris, Hardware SC
- Michael Orlovsky, L3Harris, Chair Business WG
- Greg Powers, Gore, Co-Lead Electrical Mechanical SC
- Shawn Reese, General Dynamics – MS, Chair Architecture SC & Co-Lead Sensor Management SC
- Greg Rocco, AFLCMC, Hardware SC
- Rick Ross, Raytheon Company, Architecture SC
- Joel Schlesselman, Inter-Module Interactions SC
- William Shih, Raytheon, Chair Architecture SC
- Trent Styrcula, US Army, Hardware WG
- Christal Sumner, Raytheon, Hardware SC
- Dan Toohey, Mercury, Co-Lead Sensor Management SC
- Herb Van Deusen, Gore, Co-Lead Electrical Mechanical SC
- David Vos, Lockheed Martin, Hardware SC
- Mike Walmsley, TE Connectivity, Electrical Mechanical SC
- Malcolm Weir, Ampex, Electrical Mechanical SC
- Leqi (Ken) Zhang, L3Harris, Security SC

Additional Contributors

- John Bowling, USAF, Former Chair Business WG
- Ilya Lipkin, USAF, Chair Steering Committee

Funding for the SOSA Consortium and its work products comes from its member organizations, which are listed at www.opengroup.org/sosa/members, and Naval Air System Command (NAVAIR). The US not withstanding any copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Naval Air Warfare Center Aircraft Division or the US Government.

Referenced Documents

Order of Precedence

In the event of a conflict between the text of this document and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

Normative References

See Section 1.4.

Informative References

The following documents are referenced in this Technical Standard.

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

- ANSI/VITA 17.3-2018: Serial Front Panel Data Port (sFPDP) Gen 3.0; refer to: www.vita.com/Standards
- ANSI/VITA 42.0-2021: Switched Mezzanine Card (XMC) Auxiliary Standard; refer to: www.vita.com/Standards
- ANSI/VITA 46.0-2019: VPX Baseline Standard; refer to: www.vita.com/Standards
- ANSI/VITA 46.9-2018: VPX: PMC/XMC Rear I/O Fabric Signal Mapping on 3U and 6U VPX Modules Standard; refer to: www.vita.com/Standards
- ANSI/VITA 46.11-2022: System Management for VPX; refer to: www.vita.com/Standards
- ANSI/VITA 46.30-2020: Higher Data Rate VPX; refer to: www.vita.com/Standards
- ANSI/VITA 46.31-2020: Higher Data Rate VPX, Solder Tail; refer to: www.vita.com/Standards
- ANSI/VITA 48.0-2020: Mechanical Standard for VPX Ruggedized Enhanced Design Implementation (REDI); refer to: www.vita.com/Standards
- ANSI/VITA 48.2-2020: Mechanical Standard for VPX REDI Conduction Cooling; refer to: www.vita.com/Standards
- ANSI/VITA 48.4-2018: Mechanical Standard for VPX REDI Liquid Flow Through Cooling; refer to: www.vita.com/Standards
- ANSI/VITA 48.8-2017: Mechanical Standard for VPX REDI Air Flow Through Cooling, 1.0” to 1.5” Pitches; refer to: www.vita.com/Standards

- ANSI/VITA 49.2-2017: VITA Radio Transport (VRT) Standard for Electromagnetic Spectrum: Signals and Applications; refer to: www.vita.com/Standards
- ANSI/VITA 62.0-2016: Modular Power Supply Standard; refer to: www.vita.com/Standards
- ANSI/VITA 65.0-2021: OpenVPX™ System Standard; refer to: www.vita.com/Standards
- ANSI/VITA 65.1-2021: OpenVPX™ System Standard – Profile Tables; refer to: www.vita.com/Standards
- ANSI/VITA 66.0-2016: Optical Interconnect on VPX – Base Standard; refer to: www.vita.com/Standards
- ANSI/VITA 67.0-2019: Coaxial Interconnect on VPX – Base Standard; refer to: www.vita.com/Standards
- ANSI/VITA 67.3-2020: Coaxial Interconnect on VPX, Spring-Loaded Contact on Backplane; refer to: www.vita.com/Standards
- ANSI/VITA 76.0-2016: High Performance Cable – Ruggedized 10 Gbaud Bulkhead Connector for Cu and AOC Cables; refer to: www.vita.com/Standards
- Anti-Tamper (AT) Technical Implementation Guide (TIG), Version 1.0, November 2016; available from the US DoD Anti-Tamper Executive Agent to US Government authorized personnel
- ARINC Specification 653: Avionics Application Software Standard Interface, December 2019, published by the SAE Industry Technologies Consortia (SAE ITC®)
- ARINC Specification 802-3: Fiber Optic Cables, August 2018, published by the SAE Industry Technologies Consortia (SAE ITC®)
- AS6070/6: Interface Standard, Cable, High Performance, 4 Pair, Shielded, 100 OHM, 200°C, Ethernet 10G Base T, April 2016, published by SAE International; refer to: www.sae.org/standards/content/as6070/6/
- AS6129: Interface Standard, Airborne EO/IR Systems, Electrical, December 2012, published by SAE International; refer to: www.sae.org/standards/content/as6129/
- AS6169: Interface Standard, Airborne EO/IR Systems, Mechanical, February 2013, published by SAE International; refer to: www.sae.org/standards/content/as6169/
- AS22759/70 (WIP): Wire, Electrical, Polytetrafluoroethylene Insulated, Low Fluoride, Smooth Surface, Normal Weight, Silver-Coated Copper, 200 °C, 600 VOLT, ROHS, SAE International; refer to: <https://www.sae.org/standards/content/as22759/70/>
- AS22759/75 (WIP): Wire, Electrical, Polytetrafluoroethylene Insulated, Low Fluoride, Smooth Surface, Normal Weight, Nickel-Coated Extra High Strength Copper, 200 °C, 600 VOLT, ROHS, SAE International; refer to: <https://www.sae.org/standards/content/as22759/75/>
- AS39029/28: Contacts, Electrical Connector, Pin, Crimp Removable, Shielded, Size 12 (for MIL-C-38999 Series I, II, III, and IV Connectors), July 2000, published by SAE International; refer to: www.sae.org/standards/content/as39029/28/

- AS39029/56: Contacts, Electrical Connector, Socket, Crimp Removable (for MIL-C-38999 Series I, III, and IV Connectors), July 2000, published by SAE International; refer to: www.sae.org/standards/content/as39029/56/
- AS39029/58: Contacts, Electrical Connector, Pin, Crimp Removable (for MIL-C-24308, MIL-C-38999 Series I, II, III, and IV, and MIL-C-55302/69 and MIL-C-83733 Connectors), July 2000, published by SAE International; refer to: www.sae.org/standards/content/as39029/58/
- AS39029/59: Contacts, Electrical Connector, Socket, Crimp Removable, Shielded, Size 8 (for MIL-C-38999 Series I, III, and IV Connectors), July 2000, published by SAE International; refer to: www.sae.org/standards/content/as39029/59/
- AS39029/75: Contacts, Electrical Connector, Socket, Crimp Removable, Shielded, Size 12 (for MIL-C-38999 Series I, III, and IV Connectors), July 2000, published by SAE International; refer to: www.sae.org/standards/content/as39029/75/
- AS39029/90: Contact, Electrical Connector, Concentric Twinax, Pin, Size 8, March 2001, published by SAE International; refer to: www.sae.org/standards/content/as39029/90/
- AS39029/91: Contact, Electrical Connector, Concentric Twinax, Socket, Shielded, Size 8, March 2001, published by SAE International; refer to: www.sae.org/standards/content/as39029/91/
- Aurora 64B/66B Protocol Specification, Xilinx; refer to: <https://www.xilinx.com/products/intellectual-property/aurora64b66b.html>
- Cyber Survivability Endorsement Implementation Guide, Version 1.01, Joint Chiefs of Staff, 2016; available to US Government authorized personnel at: <https://go.intelink.gov/my.policy>
- DoDAF: Department of Defense Architecture Framework, Version 2.02, August 2010; published by the US Department of Defense; refer to: <http://dodcio.defense.gov/Library/DoD-Architecture-Framework/>
- Electronic Key Management Standard (EKMS) – 308 Data Tagging and Delivery Standard, Revision F, April 16, 2008
- FACE™ Technical Standard, Edition 3.1, The Open Group Standard (C207), July 2020, published by The Open Group; refer to: www.opengroup.org/library/c207
- FIPS 140-2: Security Requirements for Cryptographic Modules, May 2001; published by National Institute of Standards and Technology (NIST); refer to: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- I²C Bus Specification, Version 2.1, January 2000, published by Philips Semiconductors; refer to: www.csd.uoc.gr/~hy428/reading/i2c_spec.pdf
- ICD-GPS-060B: GPS User Equipment (Phase III) Interface Control Document (ICD) for the Precise Time and Time Interval (PTTI) Interface, February 2002; refer to: <https://navcen.uscg.gov/pdf/gps/ICD-GPS-060B.pdf>
- IEC 61754-5:2005: Fibre Optic Connector Interfaces – Part 5: Type MT Connector Family; refer to: <https://webstore.iec.ch/publication/5844>

- IEEE 802.3-2008: IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, December 2008, published by the Institute of Electrical and Electronics Engineers (IEEE), Inc.; refer to: https://standards.ieee.org/standard/802_3-2008.html
- IEEE 802.3-2018: Standard for Ethernet (Revision of IEEE Std 802.3-2015), August 31, 2018, published by the Institute of Electrical and Electronics Engineers (IEEE), Inc.; refer to: https://standards.ieee.org/standard/802_3-2018.html
- IEEE 802.3an-2006: IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN – Specific Requirements, Part 3: CSMA/CD Access Method and Physical Layer Specifications – Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T, September 2006, published by the Institute of Electrical and Electronics Engineers (IEEE), Inc.; refer to: https://standards.ieee.org/standard/802_3an-2006.html
- IETF RFC 768: User Datagram Protocol (UDP), August 1980, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc768>
- IETF RFC 791: Internet Protocol, September 1981, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc791>
- IETF RFC 2224: NFS URL Scheme, October 1997, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc2224>
- IETF RFC 2236: Internet Group Management Protocol (IGMP), Version 2, November 1997, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc2236>
- IETF RFC 4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Delivery (MLD) Snooping Switches, May 2006, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc4541>
- IETF RFC 5227: IPv4 Address Conflict Detection, July 2008, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc5227>
- IETF RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, August 2008, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc5246>
- IETF RFC 5424: The Syslog Protocol, March 2009, published by the Internet Engineering Task Force (IETF); refer to: <https://datatracker.ietf.org/doc/html/rfc5424>
- IETF RFC 6347: Datagram Transport Layer Security (DTLS), Version 1.2, January 2012, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc6347>
- IETF RFC 7230: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, June 2014, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc7230>

- IETF RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, June 2014, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc7231>
- IETF RFC 8446: The Transport Layer Security (TLS) Protocol, Version 1.3, August 2018, published by the Internet Engineering Task Force (IETF); refer to: <https://tools.ietf.org/html/rfc8446>
- Intelligent Platform Management Interface (IPMI) Specification, Second Generation, Version 2.0, October 2013
- ISO/IEC 11801:2002: Information Technology – Generic Cabling for Customer Premises; September 2002; refer to: www.iso.org/standard/36491.html
- MIL-DTL-38999: Detail Specification: Advanced Connectors for Military and Aerospace
- MIL-DTL-55116: Detail Specification: Military Audio Connectors
- MIL-DTL-83513: Detail Specification: Connectors, Electrical, Rectangular, Microminiature, Polarized Shell, General Specification
- MIL-HDBK-516C: Department of Defense Handbook: Airworthiness Certification Criteria, December 2014
- MIL-HDBK-704-8: Department of Defense Handbook: Guidance for Test Procedures for Demonstration of Utilization Equipment Compliance to Aircraft Electrical Power Characteristics 28 VDC, April 2004
- MIL-PRF-29504/4: Performance Specification: Termini, Fiber Optic, Connector, Removable, Environment Resisting, Pin Terminus, Size 16, Rear Release, MIL-DTL-38999 Series III, December 2006
- MIL-PRF-29504/5: Performance Specification: Termini, Fiber Optic, Connector, Removable, Environment Resisting, Socket Terminus, Size 16, Rear Release, MIL-DTL-38999 Series III, December 2006
- MIL-PRF-39012: Performance Specification: Connectors, Coaxial, Radio Frequency, General Specification for MIL-STD-464, April 2005
- MIL-STD-188-148B: Department of Defense Interface Standard: Anti-Jam (AJ) Communications in the High Frequency (2-30 MHz) Band (U), March 1999
- MIL-STD-348B: Department of Defense Interface Standard: Performance Specification for Radio Frequency Coaxial, Triaxial, and Twinaxial Connectors and Interfaces, February 2009
- MIL-STD-464: Department of Defense Interface Standard: Electromagnetic Environmental Effects Requirements for Systems, December 2010
- MIL-STD-704F: Department of Defense Interface Standard: Aircraft Electric Power Characteristics, March 2004
- MIL-STD-1275E: Characteristics of 28-Volt DC Electrical Systems in Military Vehicles, March 2013

- MIL-STD-1310H: Shipboard Bonding, Grounding, and Other Techniques for Electromagnetic Compatibility, Electromagnetic Pulse (EMP) Mitigation, and Safety, September 2009
- MIL-STD-1399/300-1: Department of Defense Interface Standard, §300, Part 1: Low Voltage Electric Power, Alternating Current, September 2018
- MIL-STD 1553B: Department of Defense Military Standard: Aircraft Internal Time Division Command/Response Multiplex Data Bus, September 1978
- Modular Open Radio Frequency Architecture (MORA) Specification, Version 2.4, March 2021
- NIST Special Publication (SP) 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations, Joint Task Force Transformation Initiative, April 2013, published by the National Institute of Standards and Technology (NIST); refer to: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST Special Publication (SP) 800-57, Revision 5: Recommendation for Key Management, May 2020; refer to: <https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>
- NIST Special Publication (SP) 800-125, Guide to Security for Full Virtualization Technologies, January 2011; refer to: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf>
- NIST Special Publication (SP) 800-190: Application Container Security Guide, September 2017; refer to: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf>
- NVM Express[®], Revision 1.2, November 3, 2014; refer to: www.nvmexpress.org/developers/nvme-specification
- OpenAPI Specification, Version 3.0.3, February 2020; refer to: <https://spec.openapis.org/oas/v3.0.3>
- Open Container Initiative (OCI) Run-Time Specification, Version 1.0.2, March 2020, published by The Linux[®] Foundation; refer to: <https://opencontainers.org/release-notices/v1-0-2-runtime-spec/>
- Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products: Part 1: Requirements and Recommendations, Version 1.1.1 (technically equivalent to ISO/IEC 20243-1:2018), The Open Group Standard (C185-1), September 2018, published by The Open Group; refer to: www.opengroup.org/library/c185-1
- Open Universal Domain Description Language (Open UDDL), Edition 1.0 (C198), July 2019, published by The Open Group; refer to: www.opengroup.org/library/c198
- Open Virtualization Format (OVF), Version 2.1.1, August 2015, published by the Distributed Management Task Force (DMTF); refer to: https://www.dmtf.org/sites/default/files/standards/documents/DSP0243_2.1.1.pdf

- PCIe Version 3.0: Peripheral Computer Interface Express – Base Specification, November 2010, published by PCI-SIG; refer to: <https://pcisig.com/specifications>
- REDHAWK Framework and Tactical Open Architecture (TOA), February 2018; refer to: <http://redhawksdr.github.io/Documentation/index.html>
- Risk Management Framework (RMF) for DoD Information Technology (IT), Department of Defense Instruction 8510.01, July 2017
- RS-170: Electrical Performance Standards – Monochrome Television Studio Facilities, November, 1957, published by the Electronic Industries Alliance (EIA)
- RTCA/DO-160: Environmental Conditions and Test Procedures for Airborne Equipment, December 8, 2010
- RTCA/DO-160 Chg 1: Environmental Conditions and Test Procedures for Airborne Equipment Change 1, December 16, 2014
- SOSA Business Guide, Version 0.8, The Open Group Guide (G177), October 2017, published by The Open Group; refer to: www.opengroup.org/library/g177
- ST 292-1:2018 SMPTE Standard – 1.5 Gb/s Signal/Data Serial Interface, April 2018, published by SMPTE
- ST 297:2015: SMPTE Standard – Serial Digital Fiber Transmission System for SMPTE ST 259, SMPTE ST 344, SMPTE ST 292-1/2, SMPTE ST 424, SMPTE ST 2081-1, and SMPTE ST 2082-1 Signals, March 2015, published by SMPTE
- ST 424:2012: SMPTE Standard – 3 Gb/S Signal/Data Serial Interface, October 2012, published by SMPTE
- STANAG 4586, NATO Standardization Agreement: Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability, November 2007, published by the NATO Standardization Agreement (NSA)
- TIA 232: Telecommunications Industry Association (TIA) Standard: Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange, October 1997
- TIA 422 (TIA/EIA-422): Telecommunications Industry Association (TIA) Standard: Electrical Characteristics of Balanced Voltage Digital Interface Circuits, January 2000
- TIA 485 (TIA/EIA RS-485): Telecommunications Industry Association (TIA) Standard: Differential Data Transmission System Basics
- Universal Serial Bus (USB) 2.0 Specification, April 2000; refer to: www.usb.org
- Universal Serial Bus (USB) 3.0 Specification, November 2008; refer to: www.usb.org
- Universal Serial Bus (USB) 3.1 Specification, July 2013; refer to: www.usb.org
- Universal Serial Bus (USB) 3.2 Specification, September 2017; refer to: www.usb.org
- VICTORY: Vehicular Integration for C4ISR/EW Interoperability Standard Specifications, Version 1.9, April 2021; refer to: <https://victory-standards.org/>

- VITA 66.5: VPX: Optical Interconnect on VPX – Hybrid Variant; refer to: www.vita.com/Standards
- VITA 87.0: MT Circular Connector; refer to: www.vita.com/Standards
- VITA 90.0 (Draft): VNX+ Base Standard; refer to: www.vita.com/Standards
- VITA 90.2 (Draft): VNX+ Optical and Coaxial Connector Modules; refer to: www.vita.com/Standards

1 Introduction

Long lead times, cumbersome improvement processes, lack of reuse, platform-unique design, and extensive testing requirements characterize the current Department of Defense (DoD) C5ISR (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance) capability. This results in higher costs and the inability to deliver capabilities to the war fighter in a timely manner. To counter these trends, the United States Air Force (USAF) Air Force Life Cycle Management Center (AFLCMC), Naval Air System Command (NAVAIR), US Army C5ISR Center, and Program Executive Office (PEO)-Aviation program offices, enabled by the expertise and experience of the DoD's industrial base, are adopting a revolutionary approach. The Sensor Open Systems Architecture Technical Standard (also known as the SOSA™ Technical Standard) will enable rapid, affordable, cross-platform capability advancements based upon fundamentals of system, software, hardware, and electrical and mechanical engineering best practices and Modular Open Systems Approach (MOSA) principles to develop a solution that addresses DoD needs for a cohesive unified set of sensor capabilities.

The goal of The Open Group SOSA Consortium is to reduce development and integration costs and reduce time to field new sensor capabilities.

1.1 Objective

The subject of this Snapshot document is the specification of the SOSA Technical Standard.

This Snapshot document is intended to make public the direction and thinking about the path we are taking in the development of the SOSA Technical Standard. We invite your feedback and guidance. To provide feedback on this Snapshot document, please send comments by email to ogsosa-admin@opengroup.us no later than March 1, 2023.

This document defines an architecture and standards for modular entities for composing sensors with Electro-Optical/Infrared (EO/IR), Electronic Warfare (EW), Radar, and Signals Intelligence (SIGINT) modalities. This document defines a set of logical modules that group functions, behaviors, and interfaces, and which together define the logical architecture of a sensor. The scope of coverage also includes relevant business and conformance approaches and supporting guidance documents. The vision statement for the SOSA Consortium is:

Business/acquisition practices and a technical environment for sensors and sensor payloads that foster innovation, industry engagement, competition, and allow for rapid fielding of cost-effective capabilities and platform mission reconfiguration while minimizing logistical requirements.

The specifics of the SOSA Consortium's efforts are reflected in the Capability View – 1 (CV-1), shown in Figure 1.1-1.

As an example, the goals from the SOSA CV-1 are:

- **Open:** vendor and platform-agnostic open modular reference architecture and business model

- **Standardized:** software component, hardware element, and electrical and mechanical interface standards
- **Harmonized:** leverage existing and emerging open standards scope
- **Aligned:** consistent with DoD acquisition policy guidance
- **Cost-effective:** affordable C5ISR systems including lifecycle costs
- **Adaptable:** rapidly responsive to changing user requirements

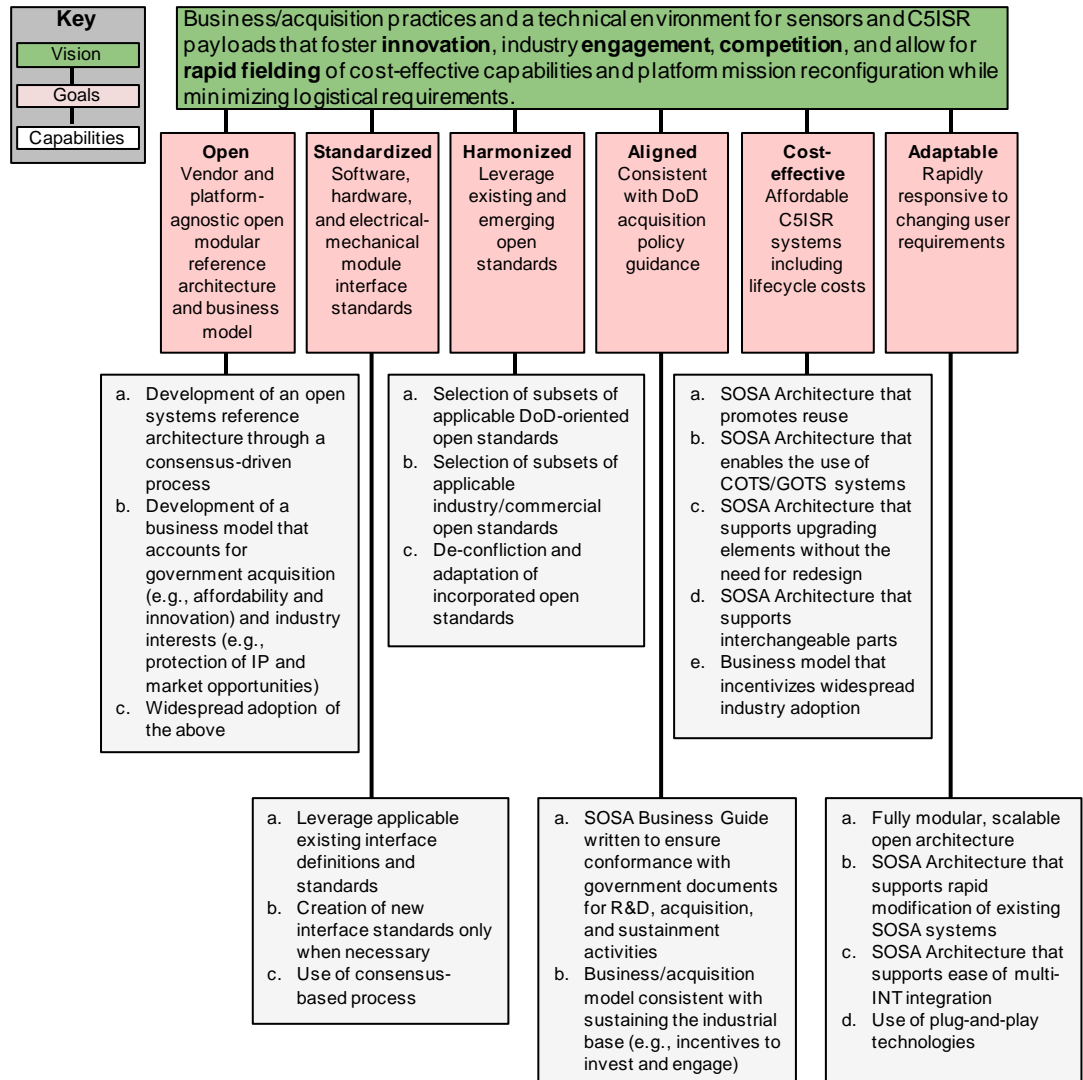


Figure 1.1-1: SOSA CV-1

1.2 Overview

This document defines a reference/objective architecture with software, hardware, electrical, and mechanical aspects that support real-time sensing solutions. The SOSA Technical Standard as indicated via its Mission Statement and Objectives (shown above) will leverage (either fully or partially (with augmentation)) Industry Standards for software (e.g., APIs), hardware (e.g.,

hardware building blocks such as VITA 65 Slot Profiles), electrical (e.g., SAE AS6129), and mechanical (e.g., SAE AS6169) sensor payload specifications. The intent of the SOSA Consortium is to provide regular releases of the SOSA Technical Standard alongside a set of published Business Strategy and Acquisition guidance documents, a set of Conformance Guidance and Policy documents, and a Reference Implementation Guide (RIG) to assist all interested entities in the development and certification of SOSA conformant items.

1.2.1 Reference Architecture Description

The foundations of the SOSA Reference Architecture are:

- **Quality Attributes:** characteristics of a system that collectively influence the overall quality of the system and will drive many of the architectural decisions (often referred to as “-ilities”) (see Chapter 3) – these are the measures for “goodness” of harmonization
- **Architecture Principles:** general rules and guidelines, intended to be enduring and seldom amended, that inform and serve as drivers for defining the architecture; a framework for decision-making (evaluation criteria) as a means to weed out approaches that are inconsistent with intent, and serve as a foundation for adjudication (see Section 3.2)
- **Capability View – 1 (CV-1):** the overall vision, goals, and enablers that support the goals of the architecture that are captured in the CV-1 DoDAF artifact (see Section 1.1)

These products provide the foundation for the architecture definition contained in this document. Another foundational element is the Integrated Dictionary (AV-2) which establishes the baseline terminology used throughout to ensure clarity and reduces (if not eliminates) ambiguity. All essential terms in the SOSA Technical Standard are captured in the AV-2.

The fundamental building blocks of the SOSA Architecture are the SOSA modules (“an element of a system that has individually distinct boundaries that are well-defined interfaces”) and the SOSA interfaces (“the region, physical or logical, where two systems or elements meet and interact”). Modules perform functions (physical and/or logical) and exhibit behaviors.

The SOSA Architecture was captured using the DoDAF, Version 2.02 Viewpoint Models, chosen because the primary target audience is the US DoD, and DoDAF is (as of this writing) the prescribed framework.

1.2.2 Modular Open System Approach (MOSA) Fundamentals

The SOSA ecosystem is an umbrella based on the convergence of domains of knowledge for business logic (market and government-driven forces) and technical specifications (software, hardware, electrical, and mechanical interfaces). To that end, a sensor aligned with the SOSA ecosystem will be defined by a conformance-driven architecture. A sensor could include SOSA conformant parts and by necessity parts which are not SOSA conformant. The SOSA mandate is driven by the idea of fielded sensors with only SOSA conformant parts. The foundation of the SOSA ecosystem is defined by a set of modules (parts) with conformant interfaces. This document provides a description of each SOSA module and its interfaces (physical, logical, mechanical, electrical, etc.) which will be required to create SOSA sensor designs/implementations based on unique customer needs.

This document is being developed using a mature architecture methodology that derives the technical details from overarching business and operational needs (see Figure 1.2.2-1).

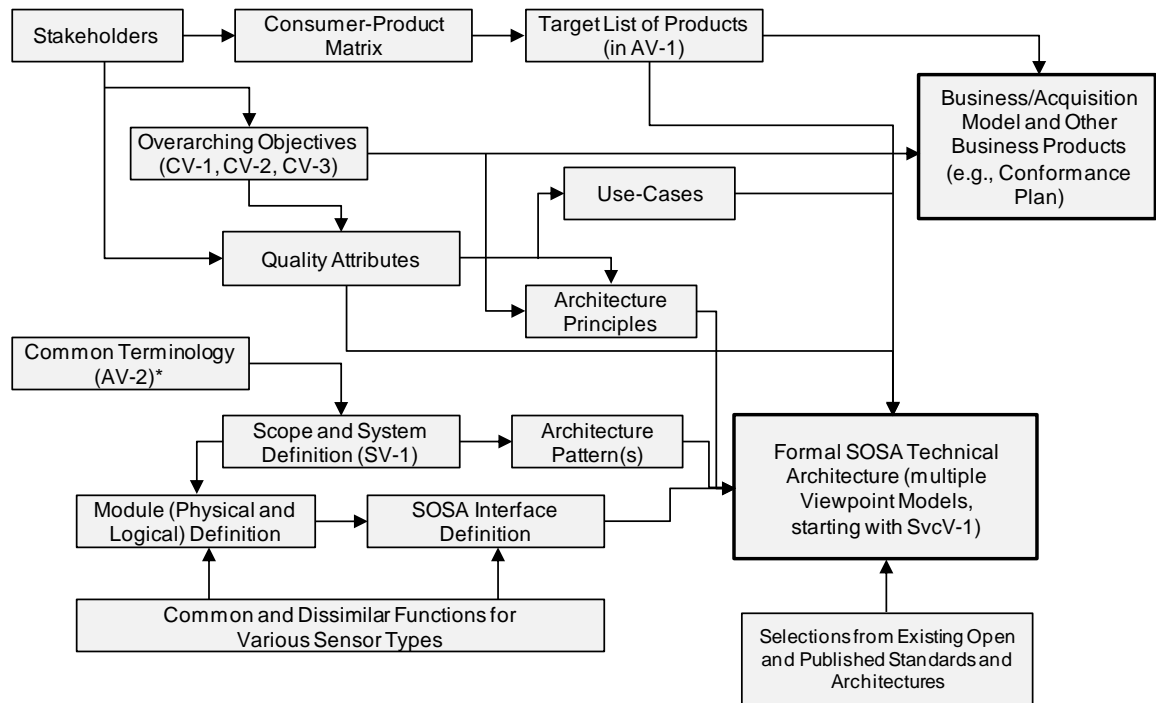


Figure 1.2.2-1: SOSA Architectural Development Process

This document describes the SOSA Technical Architecture, including the SOSA module specifications (functions, behaviors, and interfaces), and the hardware elements and software components from which they are synthesized.

1.2.3 Business Alignment

The overview of alignment between technical and business focus areas for the SOSA Technical Standard and the SOSA Open Business Model is available through a companion document – the SOSA Business Guide (see [Referenced Documents](#)). A detailed presentation of the SOSA Open Business Model can be found in the SOSA Business Guide. Examples of SOSA Open Business Model incorporation into the acquisition process can be found in the SOSA Contracting Guide. Policies guiding the development and conduct of the SOSA Conformance Certification Program can be found in the SOSA Conformance Certification Policy.

The SOSA Business Guide explains the objectives and organization of The Open Group SOSA Consortium and describes the SOSA Technical Standard and SOSA Open Business Model. It is intended for use by all stakeholders in the development, acquisition, deployment, modernization, and sustainment of sensor systems that support a broad array of sensors, including C5ISR. The primary stakeholder groups are government organizations, Aerospace and Defense contractors, and commercial businesses. Within each of these broad groups there are business and technical communities, acquisition and contracting communities, users, and operational communities. All of them have a stake in the SOSA ecosystem and should become familiar with the SOSA Business Guide.

The SOSA Contracting Guide provides procurement language examples for organizations that acquire sensor components and systems, as well as for those who provide them. This Guide is necessarily abstract to relay essential concepts without getting bogged down in details which could change as the SOSA Technical Standard and conformance processes mature. While the US

Government is the most common procurer of C5ISR systems, and contractors within the defense industrial base are the most common providers of those systems, it should be noted that the same concerns and general procedures are also applicable to procurements led by industry and to products and services provided by commercial enterprises.

1.2.4 Reference Implementation Guide Description

Whereas the SOSA Technical Standard provides specific language in the form of requirements to convey the intent and context of the SOSA Reference Architecture, the SOSA Reference Implementation Guide (RIG) is a document in which a greater amount of detail and explanation are afforded to help guide a reader of the SOSA Technical Standard on how to use the document.

The RIG outline and the subsequent content are developed and delivered in such a way to connect the reader to all necessary content based on the decision of the reader. It is worth noting that each section, and subsection, of the RIG are useful as self-contained units of information. But the real intent of the RIG is to demonstrate to the reader through guidance and examples how to design a “sensor system” using the SOSA Technical Standard.

Three sensor system-level examples of the various building blocks of the SOSA Technical Standard are used in the development of a system. The examples are hypothetical, but they do provide very good context and exemplify the principles of the SOSA Architecture.

1.3 Conformance Certification

Even though the SOSA Conformance Certification Program is tied to the production of a SOSA Technical Standard, there is a delay between the publication of the Technical Standard and the beginning of an operational program that can verify and certify potential industry products developed against that version of the Technical Standard. Until the Conformance Program is operational, the following phrase is used:

- Products in alignment with the SOSA Technical Standard

Defining conformance processes and creating an effective, affordable method for certifying software, hardware, electrical, and mechanical interfaces is vital to establishing an effective standard. Certification provides formal recognition of conformance to an industry standard, which allows the following:

- Suppliers and practitioners can make verified claims of conformance to an open standard
- Buyers can specify and successfully procure modular capability from vendors who provide solutions which conform to that open standard
- Buyers have assurance that each certified sensor component has been independently verified for conformance

The SOSA Consortium has developed a SOSA Conformance Certification Policy and will be developing a Conformance Certification Program for the SOSA Technical Standard. The SOSA Conformance Certification Program will provide the associated conformance criteria and processes necessary to assure that sensor components have been developed and conform to this document. The entity seeking certification is called the supplier. The item that is to be certified is called a sensor component. The sensor component is comprised of one or more SOSA modules and/or SOSA infrastructure elements. Each SOSA module and hardware element defined within

this document will have a set of conformance requirements called a Conformance Product Set. A sensor component can certify to one or more Conformance Product Sets. The SOSA Conformance Certification Program will consist of Preparation, Verification, and Certification phases.

The **SOSA Preparation phase** is the process in which a supplier familiarizes itself with this document and the SOSA Conformance Certification Program, as well as performing in-house testing before commencing the Verification phase.

The **SOSA Verification phase** is the act of independently assessing the conformance of the implementation of the sensor component to the applicable SOSA Technical Standard requirements. The independent assessment will be done by an accredited SOSA Verification Authority that is listed on the Verification Authority Register housed on The Open Group website.

The **SOSA Certification phase** is the process of applying for SOSA Conformance Certification once the Verification Authority declares the sensor component has successfully completed verification. Once the supplier has been notified of a successful certification, the certified sensor component will be listed in the SOSA Certification Register on The Open Group website.

Successful completion of the SOSA Conformance Certification Program results in a SOSA Conformance Certificate and the right to use the SOSA Conformance Certification Trademark in marketing.

Each phase and process is described in the SOSA Conformance Certification Policy, as well as what information is made public on the SOSA Certification Register.

Given the complexity of the SOSA effort and the variety of potential SOSA products, the SOSA Conformance Certification Program will execute in phases (in time). Each phase of the Program is based on those products deemed mature and of need to the end-user community at large. The phases are also aligned and subject to supplier developmental schedules.

1.4 Normative References

None.

1.5 Terminology

See Chapter 2.

1.6 Future Directions

The SOSA Hardware Subcommittee created a space segment for this document to extend its domain-specific architecture to a variety of applications and platforms. The new effort will leverage existing space standards against the tenets of this document.

The Small Form Factor Subcommittee (SFFSC) is working to extend the SOSA Architecture to form factors used in Small Satellites (e.g., Cube Satellites).

The Mission Operations Subcommittee (MOSC) is working on the detailed specification of many SOSA modules. A future edition of this document will have enough SOSA modules defined to build fully functional sensors with only SOSA modules.

Not all SOSA modules are defined in this version of the Technical Standard. For SOSA modules where rules are not yet defined, descriptive information is provided for reference and to show future direction of the Technical Standard.

2 Definitions

For the purposes of this document, all terms that are not specifically defined in the SOSA AV-2 Integrated Dictionary provided in Appendix 13.5.3.3.3 will be interpreted as defined in the Merriam-Webster's Collegiate Dictionary.

2.1.1 System Requirements

For the purposes of the SOSA Technical Standard, Edition 1.0, the following terminology definitions apply:

- | | |
|--------|--|
| Shall | Describes a feature or behavior that is mandatory for an implementation that conforms to this document. A hardware element or software component relies on the existence of the feature or behavior. |
| Should | Describes a feature or behavior that is strongly recommended for an implementation that conforms to this document. A hardware element or software component cannot rely on the existence of the feature or behavior. |

2.1.2 Specification Keywords

To avoid confusion and to make very clear what the requirements for conformance are, many of the paragraphs in this document are labeled with keywords that indicate the type of information they contain. Any text not labeled with one of these keywords is to be interpreted as descriptive in nature. These will be written in either a descriptive or a narrative style.

Keywords are reserved for specific use as follows:

Rule <section>-<number>

Conformance with Rules is mandatory. Rules always include the term “shall”. Rules are expressed in some combination of text, figures, tables, or drawings. All Rules will be followed to ensure compatibility between board and backplane designs. All Rules use the “shall” or “shall not” words to emphasize the importance of the Rule. The “shall” or “shall not” words are reserved exclusively for stating Rules in this document and are not used for any other purpose. In addition, each rule has one or more corresponding Conformance Methodology(ies), to indicate whether adherence to the rule is demonstrated via Test (T), Inspection (I), Demonstration (D), and/or Analysis (A).

Recommendation <section>-<number>

Conformance to a Recommendation is conditional upon its execution. When an implementation chooses to use a Recommendation as part of a product's Verification Matrix then conformance is required. Recommendations always include the term “should”. As such, the term “should” is reserved exclusively for stating Recommendations in this document and are not used for any other purpose.

Recommendations are used to convey implementation advice based on the community's collective knowledge base. Wherever a Recommendation appears, designers would be wise to take the advice given. Doing otherwise might result in poor performance or awkward problems. All Recommendations use the "should" or "should not" words to emphasize the importance of the Recommendation.

Suggestion <section>-<number>

A Suggestion contains advice, which is helpful but not vital. The reader is encouraged to consider the advice before discarding it. Some design decisions that need to be made are difficult until experience has been gained. Suggestions are included to help a designer who has not yet gained this experience.

Permission <section>-<number>

Conformance with Permissions is optional. Permissions always include the term "may". In some cases, a Rule does not specifically prohibit a certain design approach, but the reader might be left wondering whether that approach might violate the spirit of the Rule or whether it might lead to some subtle problem. Permissions reassure the reader that a certain approach is acceptable and will cause no problems. All Permissions use the "may" words to emphasize the importance of the Permission. The lower-case "may" words are reserved exclusively for stating Permissions in this document and are not used for any other purpose.

Observation <section>-<number>

Observations do not offer any specific advice. They usually follow naturally from what has just been discussed. They spell out the implications of certain Rules and bring attention to things that might otherwise be overlooked. They also give the rationale behind certain Rules so that the reader understands why the Rule must be followed.

3 Architectural Drivers

3.1 Quality Attributes

The quality attributes outlined in Table 3.1-1 inform the SOSA Technical and Business Architecture design decisions.

Table 3.1-1: SOSA Quality Attributes (in order of decreasing precedence)

Name	Description
Interoperability	<p>The ability of the system to provide data/information to – and accept the same from – other systems, and to use the data/information so exchanged to enable them to operate effectively together.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of SOSA systems to be able to exchange information during operation, and (possibly with adaptation) be able to interoperate with other systems not designed to align with the SOSA Reference Architecture.</p>
Securability	<p>The property of a system such that its design renders it largely protected/inviolable against acts designed to alter functionality or capabilities, or reverse-engineer capabilities and/or critical program information, or impair its effectiveness, and prevent unauthorized persons or systems from having access to data/information contained within.</p> <p>In the context of the SOSA Architecture, this quality attribute ensures that the fundamental architecture is one that has minimal attack surfaces and effective authentication enforcement, and SOSA systems can be designed so that they can adapt to an evolving threat environment.</p>
Modularity	<p>The degree to which a system or element is composed of individually distinct physical and functional units that are loosely coupled with well-defined interface boundaries.</p> <p>In the context of the SOSA Architecture, this quality attribute enforces the establishment of well-defined, well-understood, standardized system modules that can be created and tested individually for function and conformance.</p>
Compatibility	<p>The ability of a system to coexist with other systems without conflict or impairment or be integrated or used with another system of its type.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of SOSA systems to be used or integrated with systems not designed to align with the SOSA Reference Architecture, or with systems designed with earlier versions of the SOSA Technical Standard (backwards compatible).</p>

Name	Description
Portability	<p>An attribute that describes the reuse of existing hardware or software elements (as opposed to the creation of new) when moving hardware or software elements from one environment (physical or computing) to another.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of SOSA based hardware and software to be used, without modification, in other SOSA based environments (e.g., different operational domains, different systems, and different sensor modalities), but does not necessarily imply the porting to vastly different physical environments (e.g., operating temperature, shock, vibration – which are design, not architectural, features).</p>
Plug-and-Playability	<p>The capability of a system to recognize that a hardware component has been introduced or replaced – and subsequently use it without the need for manual device configuration or operator intervention.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of a SOSA conformant system to recognize the introduction or replacement of SOSA modules, and through an information exchange, to understand and use the capabilities and services that the module offers – thereby reducing the cost and schedule impact of adding a new SOSA module – but does not eliminate the need for integration and test.</p>
Upgradeability	<p>The ability of a system to be improved, enhanced, or evolved without fundamental physical, logical, or architectural changes.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of a SOSA system to have specific hardware elements or software components replaced with more modern or more capable equivalents, while maintaining SOSA conformance, and without (significant) change to the rest of the system.</p>
Scalability: Sensor Multiplicity	<p>The capability of a system to cope and perform well under an increased or expanding workload or increased demands, and to function well when there is a change in scope or environment – and still meet the mission needs.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of the SOSA Architecture to accommodate a multiplicity of sensors, constrained only by design-specific limitations.</p>
Scalability: Platform Size	<p>The capability of a system to cope and perform well under an increased or expanding workload, increased demands, and to function well when there is a change in scope of environment and still meet the mission needs.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of the SOSA Architecture to be applied to platforms that range from the small (e.g., Class I UAS) to large surveillance aircraft – and possibly even spacecraft.</p>
Resiliency	<p>The ability of a system to continue or return to normal operations in the event of some disruption or over-capacity (system saturation), natural or man-made, inadvertent or deliberate, and to be effective with graceful and detectable degradation of function.</p> <p>In the context of the SOSA Architecture, this quality attribute refers to the ability of SOSA systems to be able to maintain operations while under “duress” caused by physical damage, electronic interference, or cybersecurity attack.</p>

3.2 Architecture Principles

The following architecture principles were created to guide the development and maturation of SOSA Technical and Business Architectures.

Important Note: The list of principles below is not in any order and the numerical value does *not* indicate precedence.

3.2.1 Business-Oriented Architecture Principles

#1	The SOSA Technical and Business Architecture is vendor-agnostic.
Statement	The modules and interfaces that make up the SOSA Technical Standard and Reference Architecture, and the processes and practices that make up the SOSA business/procurement architecture, are equally beneficial to all vendors, offering no inherent advantage or disadvantage to any one company or business sector.
Rationale	The first goal of the SOSA Architecture is “Open: vendor and platform-agnostic open modular reference architecture and business model”, and as such the SOSA Technical and Business Architecture supports a “level playing field” to ensure business fairness, and that the best technical solution, regardless of vendor source, can be incorporated into systems based on the SOSA Technical Architecture.
Implications	The SOSA Business Architecture ensures that there are no barriers for stakeholder participation in the development or use of the SOSA Architecture. This includes making material available and eliminating financial barriers (or ensuring that they are minimal). The acquisition model is one that enables all qualified vendors to participate. The Technical Architecture incorporates standards that favor no vendor by ensuring that it incorporates widely available standards for which all qualified vendors have equivalent opportunity.

#2	SOSA Consortium products are provided royalty-free.
Statement	There is no cost to obtaining SOSA Consortium materials required to develop, procure, or implement systems (or subsystems or modules) that are aligned to the SOSA Technical Standard.
Rationale	Achieving the vision and goals of the SOSA Consortium requires that there is widespread adoption, implying the minimization of barriers to access and use the products of the SOSA Consortium. High royalties or fees to access these materials would run counter to the goals of the open business objectives, and therefore are to be avoided.
Implications	The means of publication of the SOSA Technical Standard is low-to-no cost, such as non-physical distribution via the World Wide Web, file servers, or other electronic means – subject to national security considerations (e.g., the need to authenticate that recipients are US persons who understand their responsibilities to safeguard the material). In addition, and by implication, tools (testing methodology, SDKs, etc.) required to develop and verify hardware and software conformance are widely available at no-to-little cost. Third-party products that are derived from SOSA Consortium products could be made commercially available (for additional cost).

#3	SOSA products and processes protect the IP of vendors.
Statement	Participation in the development and use of SOSA Consortium products does not jeopardize the IP of vendors. The SOSA Consortium respects IP and the SOSA Consortium products do not expose IP.
Rationale	A financially healthy Intelligence, Surveillance, and Reconnaissance (ISR) ecosystem is in the best interest of the nation. Businesses must be incentivized to invest in technology and other innovative solutions. IP protection is the cornerstone of that process that ensures that there is a return on the investment. Therefore, it is imperative that SOSA processes and products retain protections for IP rights within the module boundary.
Implications	The SOSA Architecture takes a “gray box” approach: modules are defined with properties of functions and behaviors, and interfaces are defined with properties that include their physical characteristics, protocols for exchange of signals and data, and the signal and data content. How the functions and behaviors of the modules (“inside the box”) are realized is completely up to the vendor to determine. It is “inside the box” where the IP resides. In addition, the SOSA Architecture does not include company-specific IP unless that IP has been consensually released to the SOSA Consortium for open use through the SOSA Technical Standard – per the membership agreement.

3.2.2 Technically-Oriented Architecture Principles

#4	The SOSA Technical Standard is extensible and evolvable.
Statement	The SOSA Technical Standard, and associated Reference Architecture, can continue to mature beyond the existing goals and expectations, to be able to incorporate technological and architectural improvements, and be able to maintain relevance as stakeholder needs change (e.g., new sensor types and new mission areas).
Rationale	Technologies, markets, and requirements evolve over time. To preserve the considerable time and funds invested in creating the SOSA Architecture – embodied in the SOSA Technical Standard – consideration is given to “future proof” it. For the SOSA Technical Standard to be relevant in the future, it is important that it can be extended in scope.
Implications	Architecture decisions, trades, etc. favor options that enable growth and do not “lock out” expansion. Interfaces are defined to include growth paths (extra capacity, for example). Module definitions are not so narrow as to preclude additional functionality. The architecture developers and maintainers are mindful that the current version will not necessarily be the last one.

#5	The SOSA Architecture maximally leverages/incorporates existing industry and government standards.
Statement	The SOSA Architecture takes advantage of existing industry and government standards and OSAs whenever possible and practical and consistent with achieving the goals of the SOSA Consortium.

#5	The SOSA Architecture maximally leverages/incorporates existing industry and government standards.
Rationale	Crafting well-instituted standards is both time and resource-consuming, and the community does not benefit from having multiple, overlapping, or redundant standards. Therefore, the SOSA Architecture incorporates other standards and approaches when appropriate.
Implications	Systems that already are compliant or conformant with other OSAs are likely to require minimal (or no) modifications to achieve consistency with the SOSA Technical Standard. Adoption is more efficient for the SOSA team, helping to develop and evolve the SOSA Technical Standard, though the team ensures that said adoption does not undermine the quality attributes, goals, or other guiding principles upon which the SOSA Architecture is based, and is consistent with the entirety of the SOSA Architecture more rapidly.

#6	Resilience (including cybersecurity) is enabled by the SOSA Architecture.
Statement	Physical and logical aspects of SOSA Architectures can maintain a reasonable level of operation in situations where system degradation or attack is possible.
Rationale	A SOSA conformant system is not viable if it is unable to respond accordingly to either a localized degradation event, a system-wide degradation, or a cyber-attack by maintaining a reasonable level of operational viability.
Implications	The SOSA Architecture incorporates functions that permit monitoring for health and status and facilitate the design of a system that incorporates safeguards, redundancy, and the ability to be upgraded considering new threats. A SOSA conformant system can respond to physical or logical degradation or a localized failure. Maximizing the ability of a SOSA system to effectively manage these possibilities ensures operation at an acceptable level of performance in a variety of situations.

#7	The SOSA Architecture is agnostic with respect to host platform.
Statement	The SOSA Technical Standard, and associated Reference Architecture, applies to a wide range of host platforms (e.g., aircraft, ground vehicle, ship), and makes no assumption regarding the type of vehicle or installation in or upon which it is resident.
Rationale	Conformance and adherence to this principle engenders hardware and software interoperability and reuse across multiple platforms and multiple mission types. Enabling and maximizing reuse lowers overall development costs and operational costs over the lifetime of any program.
Implications	The development of the SOSA Technical Standard considers a wide range of physical and environmental conditions, and so it specifies, for example, a range of standards-based connector types appropriate for the variety of environments. This could have implications on plug-and-playability, and so it is important that one type of interface (for one environment) easily be adapted (through interface conversion and/or software shim) to another. This enables, for example, a small-vehicle sensor to be leveraged for a large platform.

#8	The SOSA Architecture is agnostic with respect to processing environment.
Statement	SOSA modules and SOSA interfaces are not dependent upon the physical processing and operating system environments.
Rationale	SOSA modules represent the codified logic of the sensor system. Physical realization of processing environments will continue to evolve with processors, operating systems, network protocols, backplanes, memory architectures, and communication circuits. The desire is for the physical realizations to be changed as technology continues to evolve. Adherence to this principle enables hardware and software interoperability and reuse across multiple platforms and multiple mission types. Isolating SOSA modules from the processing environment allows rapid technology refreshment, system scaling, and module reuse.
Implications	The SOSA Technical Standard needs to consider a wide range of processing environments as realized by the selection of processors – Central Processing Unit (CPU), Graphical Processing Unit (GPU), Field Programmable Gate Array (FPGA), and custom – operating systems, network protocols, backplanes, memory architectures, and communication circuits. This means that the interfaces are independent from the processing environment through abstraction.

#9	Every SOSA module has defined logical interfaces.
Statement	All SOSA sensors have well-defined logical interfaces for each of their SOSA defined modules. Logical interfaces describe the information content or signaling between modules for the interchange of control and data. The logical interface is a point that encapsulates control and data along with the syntax/semantics as described by the SOSA Architecture. Information exchange, including transmission type, interchange protocols, and routing are part of the interface definition.
Rationale	An interface is a shared boundary for interaction between architectural modules. SOSA module logical interfaces enable replacement for modernization and upgrade, support plug-and-playability, interoperability, operational flexibility, and will likely result in cost savings over the lifetime of an operational program.
Implications	The SOSA Technical Standard addresses a wide range of logical interfaces realized in SOSA environments. SOSA logical interfaces mandate that a set of interface standards is needed to span the types, protocols, addressing, service types, and operational environments.

#10	Every SOSA hardware element has defined physical interfaces.
Statement	All SOSA sensors have well-defined physical interfaces for each of their hardware elements. Physical interfaces describe the physical or mechanical connection between SOSA hardware elements, providing structural attachment, electrical/electronic connectors, backplanes, or other inter-module associations that are physically manifested.

#10	Every SOSA hardware element has defined physical interfaces.
Rationale	Well-defined SOSA hardware element physical interfaces enable replacement for modernization and upgrade, support plug-and-playability, interoperability, operational flexibility, and will likely result in cost savings over the lifetime of an operational program.
Implications	The SOSA Technical Standard addresses a wide range of physical interfaces realized in SOSA environments. SOSA physical interfaces mandate that a set of interface standards is needed to span the types, physical sizes, connector types, electrical signaling (including physical and data link layers), and operational environments.

#11	The SOSA Architecture accommodates simple through complicated systems.
Statement	The SOSA Architecture provides the building blocks for deriving multiple sensor types that scale within a design, increasing or decreasing complexity relative to processing and Size, Weight, and Power (SWaP) constraints for a system.
Rationale	<p>There are many aspects of complexity that the SOSA Architecture addresses, such as number of sensors to manage, diversity of sensors, and algorithm complexity/parallel processing requirements.</p> <p>The management functions of sensor systems become more complex as the number of entities increase. Having patterns that allow the management functions to scale with (at most) minor changes is crucial.</p> <p>The ability to support algorithm scaling (e.g., instances of the same process working in parallel) and increasing or reducing the corresponding hardware as needed with only configuration changes is an important attribute of a SOSA system.</p>
Implications	<p>SOSA systems accommodating a range of complexity require well-defined functional decomposition, use-cases, and interface definitions. The functional decomposition needs to create the right layer(s) of abstraction for a variety of hardware and software entities to coexist in different configurations. The use-cases need to cover all required system functionality, from specific mode processing to state/mode control to heartbeats. Integrating different software or hardware into a system should minimally affect the management functions of a SOSA derived system.</p> <p>The interface definitions need to be firm for system management, but flexible for a variety of sensor type processing. Patterns are used extensively to manage the complexity.</p>

#12	The SOSA Architecture accommodates small through large platforms.
Statement	The SOSA Architecture is flexible enough so that designs derived from it can be tailored to large as well as small platforms, with the flexibility to be used to design simple, lightweight systems (suitable for a small UAS) as well as large complex systems (e.g., suitable for a wide-body jet, warship, or ground-based installation).

#12	The SOSA Architecture accommodates small through large platforms.
Rationale	Applicability is dependent upon the ability of a solution to provide a standard suite of interfaces across a multiplicity of host structures. Not limiting the scope of the SOSA Technical Standard to one class of hosts or another ensures broad applicability and utility.
Implications	The SOSA Architecture is a superset architecture; complete in that it can be used to design a complex, fully functional system, and at the same time does not mandate/require the presence of all (or many/most) modules for systems with more modest SWaP resources. The SOSA Architecture incorporates hardware and physical standards that allow the use of small as well as large form factors.

#13	Modularity is fundamental to the SOSA Architecture – physical and logical.
Statement	The SOSA Architecture is an OSA, and as such is composed of physical and logical units (“building blocks”) that have individually distinct boundaries that are well-defined interfaces. The units or elements that make up a SOSA Architecture (or resulting system) are known as SOSA modules.
Rationale	The goals for the SOSA Architecture include openness, standardization, and adaptivity that allow for replacement/upgrade of parts of a sensor and reuse in a vendor-neutral manner. Modules (physical and logical units with well-defined boundaries) are the means of achieving these goals.
Implications	<p>The SOSA Architecture is described in terms of modules (functions and behaviors) and interfaces (information or signals to be exchanged by these modules, and how they are exchanged, such as protocols or electrical specs). The modules are defined in a way that ensures independence and low coupling (so that changes in one do not impact others). Criteria used:</p> <ul style="list-style-type: none"> • Severable (can be separated and used elsewhere) – based on business needs, timing requirements, or other drivers • Has minimal complexity interfaces (minimum interdependencies) • Can operate as stand-alone or be operated via function/process/system manager • Is independently testable • Does not expose IP • Facilitates competitive procurement • Encapsulates rapid change

#14	Interchangeability is fundamental to the SOSA Architecture.
Statement	Modules making up SOSA systems can be replaced by equivalent modules regardless of the source. Moreover, it would be possible to interchange one (entire) SOSA system with another SOSA system (provided it does not violate physical/environmental requirements).

#14	Interchangeability is fundamental to the SOSA Architecture.
Rationale	The goals of the SOSA Consortium include openness (platform and vendor-agnostic) and rapid response. The quality attributes include modularity and upgradability. Essential to these objectives is the need to be able to interchange SOSA modules to achieve goals, such as using module replacement to upgrade a sensor or modify it because of a changing mission need. This will result in a more robust marketplace where subsystem upgrades become more commonplace as the ease of modular upgrades becomes apparent.
Implications	Interfaces are very well-defined and yet contain a high degree of flexibility. Module-unique interface technologies should be avoided in favor of those that are broadly applicable. Interface definitions are superset definitions; they include all the functionality/capability that a SOSA module or system is anticipated to include. The architecture defines a default behavior for situations where all functions supported in the interface are not implemented.

#15	Reuse is fundamental to the SOSA Architecture.
Statement	SOSA systems and modules that are developed for one program, host vehicle, or environment will be employable, with minimal modification, for other programs, with other host vehicles and in other operational environments.
Rationale	The ability to reuse SOSA sensors and modules across various vehicles allows the DoD to reduce parallel investment to develop the same type of payload assembly multiple times to fly on various vehicles. The ability for a sensor subsystem to operate inside various SOSA sensors and modules reduces the integration costs for creating a new payload assembly.
Implications	Modules should be reusable across the range of host platforms, consistent with SWaP limitations (embodied in their specific design/instantiation). It is imperative that standard SOSA interfaces are well-defined, to include physical, logical/protocol, and data content and format. A standardization of electrical connector interfaces and aperture mounting interfaces is required. Multi-platform integration architectures are used to allow modules to communicate with an embedded computer or the host platform, and/or both. The intent is to minimize (or eliminate) the cost and schedule impact of adding or replacing a new SOSA module, not to eliminate the need for integration and test.

4 SOSA Architecture Overview

4.1 SV-1 (System Interface Description and Context)

The System View 1 (SV-1) system interface description presented below identifies and describes the physical/hardware systems and the nature of the interconnections for the SOSA sensor system. The SOSA SV-1 depicts all system resource flows between systems that are of interest to the SOSA Consortium (see Figure 4.1-1 and Figure 4.1-2).

The SV-1 is an abstract representation showing key top-level SOSA actors and their physical relationships. Logical relationships (e.g., messaging) will be shown in other SOSA viewpoint models. This document addresses two categories of interface:

- **SOSA External Interfaces** cross the orange SOSA sensor boundary and consist of aperture(s) sensing the electromagnetic environment and interfaces to connect to a SOSA host
- **SOSA Internal Interfaces** are contained entirely within the orange boundary – the SOSA Consortium will choose a subset of the many possible internal interfaces to address in this document

The SV-1 only shows a few instances of SOSA elements as exemplary cases; the number of SOSA elements depends on the specific SOSA sensor. A SOSA sensor is mounted on a SOSA host, which can be a pod or a platform, or both. This is the Nominal Case, shown in Figure 4.1-1. A SOSA sensor can also contain its own pod (a “SOSA sensor pod”), which is the special case shown in Figure 4.1-2. Multiple SOSA sensors could be mounted on the same SOSA host. Relationships between SOSA sensors are logical (e.g., via messaging), not physical, and therefore not shown in the SV-1.

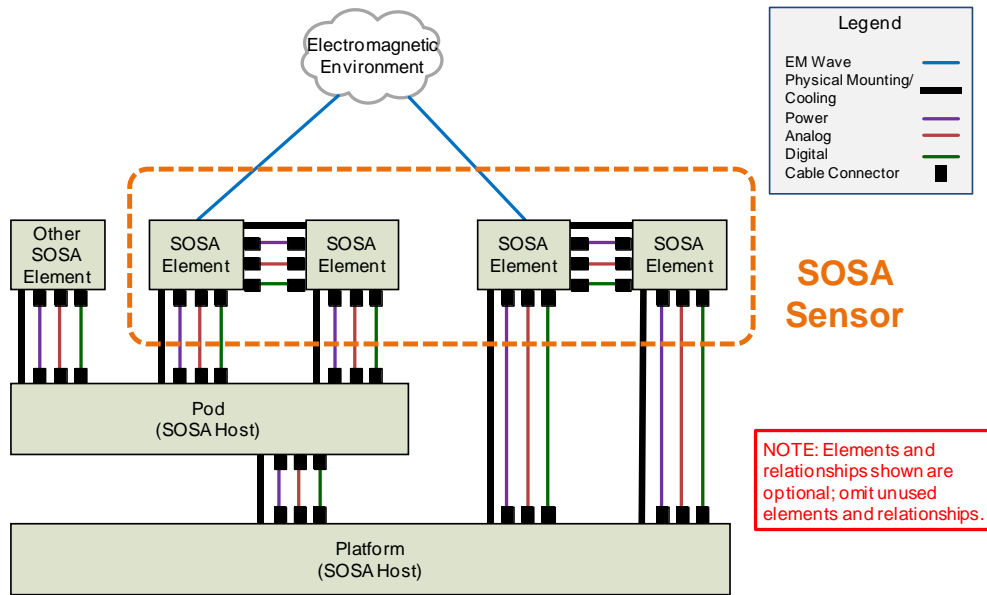


Figure 4.1-1: SV-1 for Nominal Case

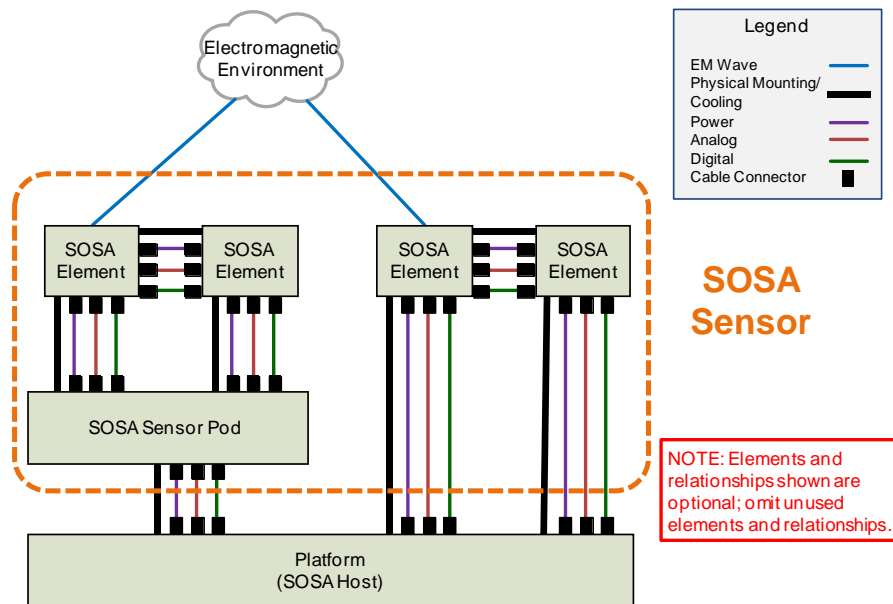


Figure 4.1-2: SV-1 for Sensor Pod Special Case

4.1.1 SOSA Physical Context

4.1.1.1 SOSA Sensor

The main subject of this document is the SOSA sensor, which consists of a set of one or more SOSA sensor hardware elements (some of which host software components). Each SOSA sensor is either one of the five “sensor” types (Communications, EO/IR, EW, Radar, and SIGINT), or any combination of the five sensor types (e.g., they could be multi-INT). Any interface crossing the SOSA sensor’s boundary is a SOSA external interface.

4.1.1.2 *SOSA Hardware Element*

A SOSA sensor consists of a set of one or more SOSA hardware elements mounted within or on the same host platform. Hardware elements could be grouped together and/or distributed in different locations on/in the SOSA host platform. In the context of the SV-1, it is a physical component of a SOSA sensor which could contain software and firmware and could support more than one sensor type (it has other “non-physical” interpretations in other viewpoint models). It consists of but is not limited to:

- Aperture (antenna, packaged antenna array, packaged imaging array, or imaging turret)
- Hardware enclosure (e.g., chassis)

SOSA hardware elements could optionally contain SOSA Plug-In Cards (PICs) connected to its backplane.

4.1.1.3 *SOSA Host Platform*

A SOSA host platform is the physical entity to which the SOSA sensor is mounted. Normally, it is a vehicle or structure (such as an aircraft, surface craft, a building, or a pod) or a combination of one or more pods within a vehicle/structure. It nominally provides to the sensor:

- Power
- Cooling
- Platform navigation information (position, velocity, etc.)
- Reference signals (e.g., 1 PPS, 10MHz, etc.)
- Network connections
- Connections for any other needed analog or digital interfaces

The SOSA host platform could contain external (to the SOSA sensor) processing capability that could use the data products of the SOSA sensor, and external communications. It will provide the SOSA sensor with its tasking. It is assumed that the host platform provides any User Interface (UI) that could be required; while the SOSA system could provide data and information to be used by a UI, the UI is outside the scope of the SOSA system.

4.1.1.4 *SOSA Sensor Pod*

A SOSA sensor pod is a pod that is delivered as an integral part of a SOSA sensor and has elements from one or more SOSA sensors mounted in/on it.

4.2 **SvcV-1 (Services Context Description)**

The Service View 1 (SvcV-1) documents the SOSA modules and their top-level relationships to one another. Not all modules need to be instantiated in a design to be conformant. A future version of this document will define the core functionality for each type of sensor. In the case of multiple integrated sensors, the sensor integrator would need to determine how to instantiate the modules necessary to incorporate the SOSA core functionality. The details of their relationships are documented in the SvcV-4: Services Functionality Description.

Figure 4.2-1 identifies the SOSA modules and their relationships (enumerated in the dotted decimal numerical identifications, by color-code, and grouping/proximity). It also shows some of the resulting interfaces that are being determined for the SOSA Technical Architecture. It should be noted that Figure 4.2-1 does not represent “*The SOSA Architecture*”. This artifact is one among the many that, taken together, constitute the SOSA Technical Architecture.

Descriptions (explaining the encapsulated functionality and behaviors) of each of the SOSA modules is documented in Table 4.2-1. All SOSA sensor functionality must be contained within the encapsulating SOSA module. In practice, a SOSA sensor could implement a subset of these modules.

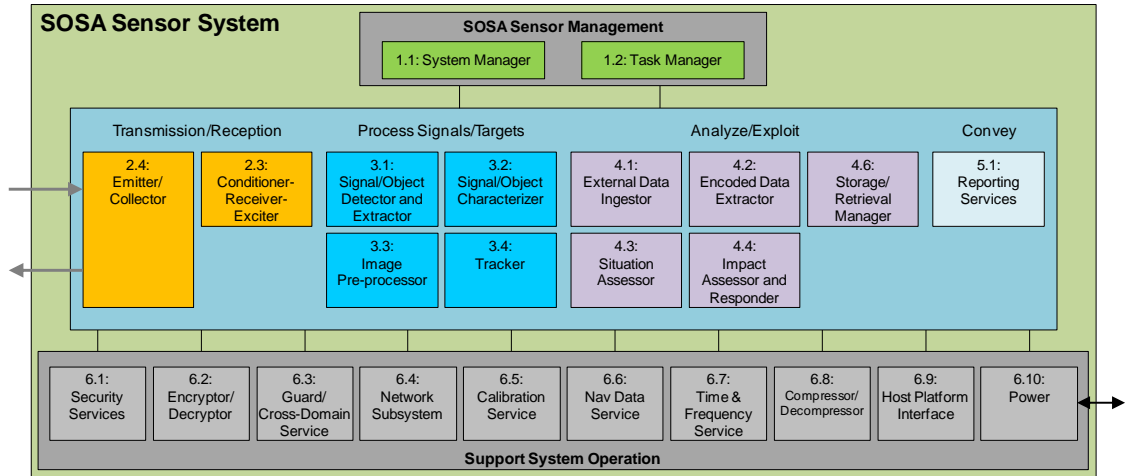


Figure 4.2-1: SvcV-1 Top-Level SOSA Services Context Description

Table 4.2-1: SvcV-1 Module Descriptions

Module Name	Description
SOSA Sensor Management	
1.1 System Manager	The System Manager module is responsible for implementing functions necessary to manage the overall SOSA sensor system, its hardware and software infrastructure, and the security controls applied to it. System management functions include Discovery (identifying and obtaining information required to communicate with the SOSA sensor and its sensor components), Configuration (obtaining a detailed description of the sensor, its sensor components, and the security controls applied, reading and setting configuration parameters, and updating software packages), Control (monitoring and setting control parameters for the sensor and its modules, such as mode and state, and performing control actions such as reset or BIT), and Health Management (publishing periodic health reports, notifying occurrence of configuration, control, and health events, and logging health reports and events), and Security Management (monitoring of the system to detect and counter cybersecurity anomalies and threats). The System Manager applies these functions to the SOSA sensor, to its modules, its hardware and software infrastructure, its security controls, and its interface to the sensor host. The System Manager does not manage or control the mission, tasking, or operational aspects of the SOSA sensor, but instead takes care of the SOSA sensor itself so it can implement the mission.

Module Name	Description
1.2 Task Manager	The Task Manager module is responsible for coordinating all mission operations. External sensor tasking is accepted in the form of a request that contains information detailing when and where to collect data, the type of processing to be performed, and the required output products to be generated. Information in the request is used by the Task Manager to optimize, manage, and prioritize resources to support various competing tasks in a SOSA sensor. Any externally invoked changes to tasking are handled by the Task Manager, which in turn propagates the mission changes into relevant mode and state changes for the other SOSA modules. Lastly, the Task Manager is responsible for invoking routine calibration as needed to support the mission tasking.
Transmission/Reception	
2.1	Reserved
2.2	Reserved
2.3 Conditioner-Receiver-Exciter	The Conditioner-Receiver-Exciter module performs receive tasking, transmit tasking, or both. Receive tasking could include calibration, channelization, image formation, tagging with metadata, data framing, and data cube formation. Transmit tasking could include waveform generation, calibration, and adaptation to spectrum use. The signal could be amplified, filtered, frequency translated, distributed, and signal domain converted – Analog to Digital Conversion (ADC) and Digital to Analog Conversion (DAC).
2.4 Emitter/Collector	The Emitter/Collector module is responsible for converting between Electromagnetic (EM) energy and electric signals, performing receive functions, transmit functions, or both. This module could include mechanical and electronic steering, beam forming, focus control, and preparing analog/digital raw data products for processing. The signal could be stabilized and calibrated. The signal could be amplified, filtered, frequency translated, distributed, and signal domain converted (ADC and DAC).
Process Signals/Targets	
3.1 Signal/Object Detector & Extractor	The Signal/Target Detector & Extractor module is responsible for detecting EM signals or physical objects among the noise and other signals and objects in the environment (e.g., clutter or interference). This module extracts a detected signal, detected object, or image chip for downstream processing. Techniques to perform this could include clutter suppression and extraction of scintillation/de-correlation information, interference suppression, the use of constant false alarm rate techniques, coherent and non-coherent integration, Space-Time Adaptive Processing (STAP), image enhancement (including edge detection and sharpening), and employment of gating logic to manage and balance search volume returns with existing object tracks.
3.2 Signal/Object Characterizer	The Signal/Object Characterizer module is designed to make measurements on images, signals, and physical objects to determine attributes, properties, categories, classes, types, or identification – all with confidence estimates.

Module Name	Description
3.3 Image Pre-processor	The Image Pre-processor module forms the image and/or prepares it for final use by processing sensed data. This could include enhancing images, reformatting into standard formats (e.g., NITF, MISB), or registering/correlating images to geographical coordinates and/or other images.
3.4 Tracker	The Tracker module correlates detections and tracks over time, forming new or updated tracks. It is responsible for all track management functions and producing track reports. The core functionality of the Tracker is data association, track initiation, track drop, track update, state and covariance estimation, and split track handling. Estimation of relative position or location (geolocation), when feasible, is also included in this function.
Analyze/Exploit	
4.1 External Data Ingestor	The External Data Ingestor module is responsible for ingesting data from other SOSA sensors, as well as sensors that don't conform to the SOSA Technical Standard (converting from non-conformant format to conformant format as needed) and distributes ingested data to other SOSA modules.
4.2 Encoded Data Extractor	The Encoded Data Extractor module is applicable to Communications, EW, and SIGINT. It is responsible for demodulating and extracting message content (Communications and EW), extracting internals (EW and SIGINT), and human language processing (SIGINT).
4.3 Situation Assessor	The Situation Assessor module determines current relationships among objects and events in the context of their environment. The distribution of individual signals and objects is examined to aggregate them into operationally meaningful groups. In addition, this module focuses on relational information (e.g., physical proximity, communications, causal, temporal, and other relations) to determine the meanings of groups of entities. This analysis is performed in the context of environmental information about terrain, surrounding media, hydrology, weather, and other factors.
4.4 Impact Assessor & Responder	The Impact Assessor & Responder module interprets the current situation to draw inferences about enemy threats, friendly and enemy vulnerabilities, and it could project those into the future. Impact assessment could involve estimating possible outcomes and assessing an enemy's intent based on knowledge about enemy doctrine, level of training, political environment, and the current situation. This module could develop alternate hypotheses about an enemy's strategies, given the effect of uncertain knowledge about enemy units, tactics, and the environment. This module could also initiate a response to a threat; for example, by notification to an internal capability (e.g., electronic attack) or an external system to act (e.g., countermeasures or evasive maneuvering).
4.5	Reserved

Module Name	Description
4.6 Storage/Retrieval Manager	The Storage/Retrieval Manager module provides the capability of storing a variety of data types in a persistent medium and allows it to be retrieved in bulk by authorized client entities. The Storage/Retrieval Manager can be used for short-term (in-mission) data as well as long-term (or archival) purposes. Data that can be stored includes health reports, heartbeats, notifications (health, configuration, and control notifications), streaming data, and metadata.
Convey	
5.1 Reporting Services	The Reporting Services module generates and disseminates reports. Specifically, the Reporting Services module is responsible for formatting, processing (as required by sensor type), packaging data for reporting, structuring data to match a selected format, and dissemination of data to intended recipients. Such data can include RF signal, image/video streams, demodulated signal, metadata for streams, detections, characterized targets, associated and non-associated targets/threats, assessed behaviors, alerts, sensor cues/tips, complex data (data between raw and fully processed), logging or test information, and responsible reporting commands. The module is responsible for accepting/rejecting requests for existing data in storage, retrieving requested data, aggregating data, and selecting data to be reported. The module also selects header/packet structure for streaming data. The Reporting Services module must be capable of storing report templates germane to the sensor type; and accept updates to those templates (e.g., metadata updates to format types).
Support System Operation	
6.1 Security Services	The Security Services module is responsible for controlling all sensor protection functionality. This includes software/data integrity checks, control access, zeroizing sensitive data, managing keys, auditing, root of security, environmental checks, and response actions.
6.2 Encryptor/Decryptor	The Encryptor/Decryptor module is responsible for all cryptographic services such as encryption, and decryption with authentication. In addition, it communicates with the Security Services module for key interchange and to report status (successful/failed result).
6.3 Guard/Cross-Domain Service	The Guard/Cross-Domain Service module is responsible for transferring data between separate security enclaves of the same or differing security levels and preventing data leakage between enclaves.

Module Name	Description
6.4 Network Subsystem	The Network Subsystem module is the infrastructure responsible for enumerating network elements, monitoring the health of network elements, detecting and isolating degraded network elements, transferring data with the requested Quality of Service (QoS), and detecting intrusion. Data users could request data from data sources that have requirements for update rate, latency, and priority, and the Network Subsystem module ensures that these requests are met and can report when they are not met. The Network Subsystem module can be configured to alert on thresholds such as network bandwidth exceeded. The Networking Subsystem module provides the services to request network status such as throughput, up/down status, and configuration at any time, and will collect metrics to support this reporting. Intrusion detection can be configured by a network manager to alert on security breaches and to isolate the breached network channel.
6.5 Calibration Service	The Calibration Service module is responsible for ingesting and injecting the test signal and disabling SOSA modules not under test.
6.6 Nav Data Service	The Nav Data Service module translates platform 3D position, 3D velocity, time, and 3D platform orientation into a generic format compliant with SOSA interface standards. It is common across all sensor types. The service distributes this nav data to subscribers. It will report accuracy, integrity, and source information so that subscribers to this data could decide if the data is suitable for use. The service will select, smooth, blend, or exclude data as necessary to create the best solution. The service accepts requests for data configuration such as specific data elements, update rates, and formats. Subscribers could perform individual one-time requests for nav data or could request a repetitive update at a selected interval.
6.7 Time & Frequency Service	The Time & Frequency Service module is responsible for providing time information and providing Local Oscillator (LO)/frequency references. The time information is a high precision time signal that is a higher precision than that typically provided by GPS although it could be synchronized with GPS. Discrete time output signals are provided and could be used by any other module without a request. Time information quality status is provided by a communications channel. The LO/frequency references provide highly accurate and stable output signals suitable for GHz range RF systems to any other module without a request. Signal quality status is provided by a message via the Network Subsystem module. Other modules could send a request to the Time & Frequency Service module to be notified if time or frequency signal quality thresholds are not met. A time and frequency management capability allows the time and frequency output signals to be enabled or disabled.
6.8 Compressor/Decompressor	The Compressor/Decompressor module is responsible for reducing the volume of data for storage or transport/restoring the compressed data to its original format. These functions are performed by executing codec functions.
6.9 Host Platform Interface	The Host Platform Interface module is responsible for all communication with the host platform. Its primary function is data translation to/from formats and messages required by the host platform.

Module Name	Description
6.10 Power	<p>The Power module could be responsible for power conversion, conditioning, storage, protection, distribution, and management. It applies to all sensor types. The Power module could receive host platform power (via the Host Platform Interface module) and could convert it to the conditioned power needed by SOSA modules. It could also include the routing and distribution of power to SOSA modules that use it, which can include chassis, switches, relays, transformers, etc. The Power module could provide status such as to indicate whether power is within specification and an alert to impending power loss. It could also provide a management interface that allows configuration, control, and status.</p> <p>Note that some modules could be designed with integrated power supplies. That type of module should have its own power management interface which could be aligned with the power management interface of the Power module.</p>

4.3 SvcV-2: Services Resource Flow Description

The Service View 2 (SvcV-2) provides a high-level view of the information passing to give the user an initial understanding of the SOSA module roles in the context of their processing relationships. It does this by documenting the flow of information between SOSA modules. Documenting this flow is useful given SOSA modules in service and the information exchanged can vary as sensor system modalities and required functionality are composed for a specific SOSA sensor solution.

Figure 4.3-1 identifies the subset of SOSA modules defined for use in the SOSA Technical Standard, Edition 1.0, and a high-level description of the information flows between them. Currently, these flows are a combination of functional requirements for SOSA sensor thread processing in the SOSA Technical Standard, Edition 1.0 only. Additional flows will be added in a future version of this document. A complete detailed description of each flow can be found in each SOSA module section of this document, each SOSA module SvcV-4 table, and the corresponding details.

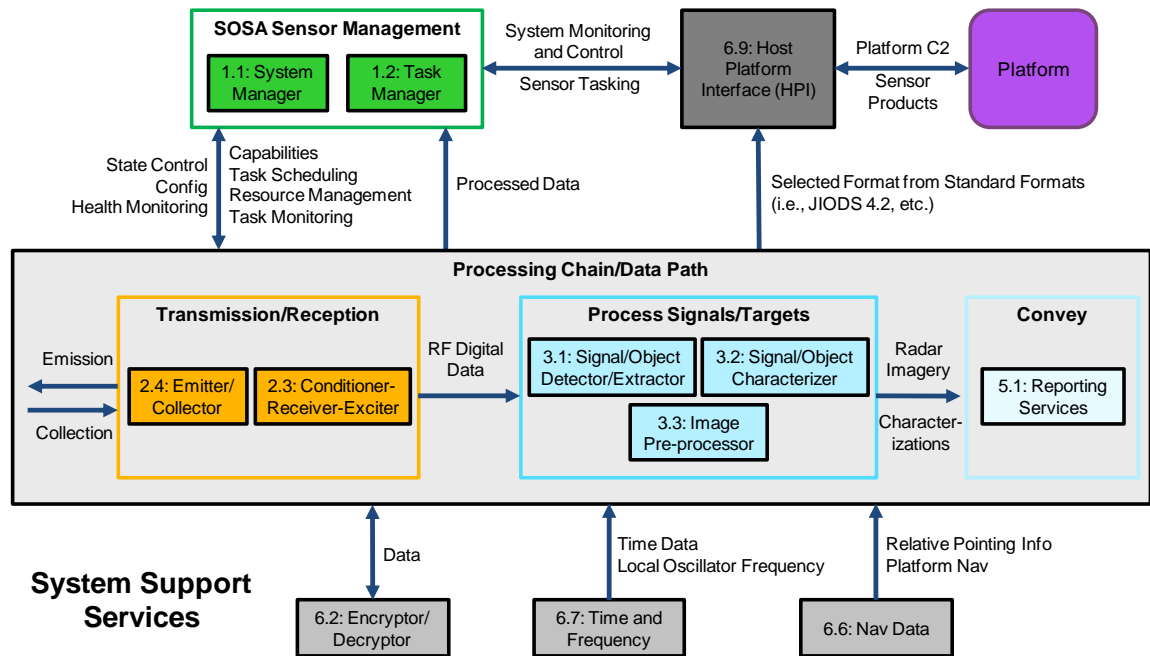


Figure 4.3-1: SvcV-2: Top-Level SOSA Service Resource Flow Description for Edition 1.0

SvcV-2s for each SOSA sensor thread defined for SOSA module integration are included in the RIG document. These SOSA sensor threads describe at a high level:

- Synthetic Aperture Radar (SAR)
- Electronic Warfare (EW)/Electronic Attack (EA)
- Signals Intelligence (SIGINT) processing using a SOSA sensor construct

SOSA sensor threads for EO/IR and Communications processing SvcV-2 diagrams will be created as they are defined and supported in a future version of this document.

5 Technical Concepts and Overview

5.1 Taxonomy

The SOSA ecosystem addresses the sensing domains of Communications (Comms), Electro-Optical/Infra-Red (EO/IR), Electronic Warfare (EW), and Radar from signal transmission, signal acquisition, through signal to data (in both directions), to information processing with a set of sensor components realizing the principles of the Modular Open Systems Approach (MOSA). For the purposes of this Technical Standard, a sensor is comprised of a set of sensor components, which can be instantiated in hardware, firmware, or software. Hardware examples include PICs, chassis, apertures, Application-Specific Integrated Circuits (ASICs), FPGAs, analog and digital discrete logic. Firmware examples include executable programs typically developed in a low-level language. Software examples include executable programs typically developed in a high-level language and software Run-Time Environments (RTEs). A sensor aligned with the SOSA ecosystem employs one or more sensor components conformant to the SOSA Technical Standard, called SOSA sensor components.

The taxonomy for SOSA sensor components is illustrated in Figure 5.1-1. This document describes two types of SOSA sensor component:

- Logical building blocks implementing specific functions and interfaces, called SOSA modules
- Infrastructure building blocks providing a platform for SOSA modules to execute, called SOSA infrastructure

A sensor can incorporate a set of SOSA sensor components provided by any combination of SOSA modules in the SOSA Architecture. A sensor will also incorporate various hardware elements, software RTEs, and interaction infrastructure needed to communicate between SOSA modules.

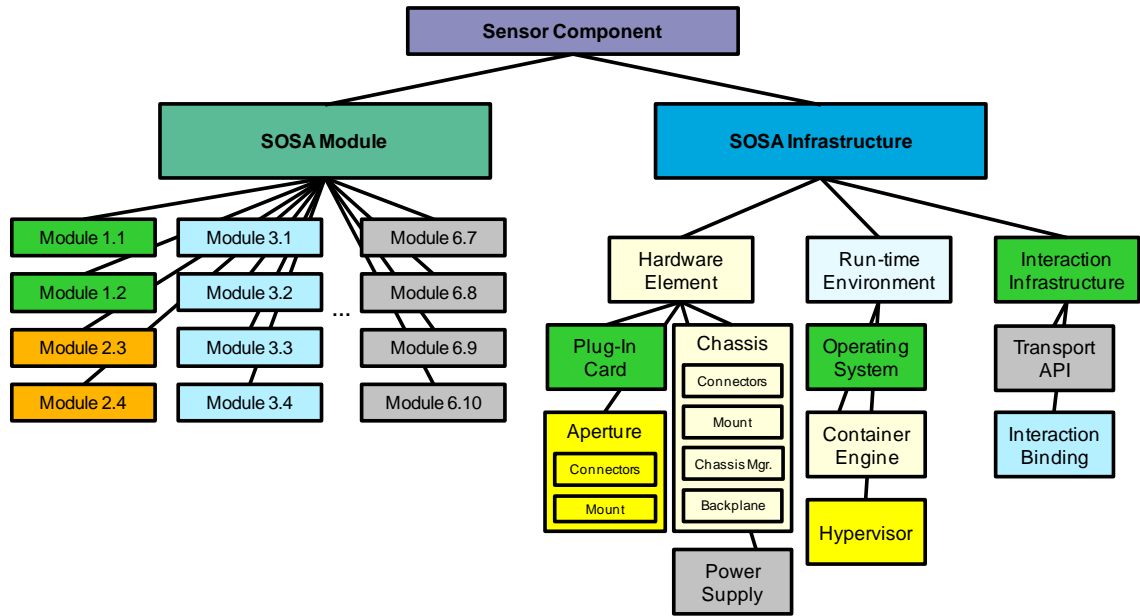


Figure 5.1-1: SOSA Taxonomy

The SOSA Architecture’s modular decomposition is further described in Section 5.2. The specific rules for each SOSA module are described in later sections of this document.

The SOSA infrastructure provides the sensor components required for SOSA modules to perform its functions. The SOSA Architecture standardizes these infrastructure components as hardware elements, RTE, and interaction infrastructure. Hardware elements are categorized as PICs, apertures, chassis, and power supplies. PICs employ Plug-In Card Profiles (PICPs) described in Section 13.2 that allow for standardization of connector and pin definitions (physical, electrical, and protocol). Similarly, Section 13.5.13.5.5 and Section 13.5.5 describe the connector, mounts, and other requirements for apertures and chassis. There is also a separately conformant hardware element called a Chassis Manager that manages the PICs within the chassis, further described in Section 6.3 and Section 6.4. Power supplies are independently managed – via the Intelligent Platform Management Interface/Bus (IPMI/IPMB) with an Intelligent Platform Management Client (IPMC) – conformant hardware element responsible for delivering specified voltages to PICs within a chassis.

The SOSA Architecture defines a standard RTE to host software. This promotes software portability and allows for native software applications executing on top of an operating system, applications within a virtual machine managed by a hypervisor, or containerized applications orchestrated by a container engine. The RTE is further described in Chapter 14.

Finally, the SOSA Architecture defines a standard interaction infrastructure that allows SOSA modules to communicate with each other via a standardized interaction infrastructure. This document defines a set of Application Programming Interfaces (APIs) that software components could employ to perform inter-module communications. Inter-module communications, either via API or otherwise, will be performed with an approved set of interaction bindings to promote modularity and upgradeability via on-the-wire interface compatibility (on-the-wire). This interaction infrastructure is described in Chapter 15.

Suppliers offering sensor components conformant to the SOSA Technical Standard are required to have a conformance certification certificate based on testing by an approved SOSA

Verification Authority and issued by the SOSA Conformance Authority. Details on the Conformance Program are described in the SOSA Conformance Certification Policy available from The Open Group (<https://www.opengroup.org/sosa>).

5.2 Modular Decomposition Approach

There are a great many functions that must be performed within a Communications, EO/IR, EW, Radar, and SIGINT system. These have been logically combined into what have become the SOSA modules, the aggregation process based on these seven criteria:

1. Is severable (can be separated and used elsewhere) – based on business needs, timing requirements, or other drivers.
2. Has minimal complexity interfaces (minimum interdependencies).
3. Can operate stand-alone or independent of the rest of the SOSA sensor.
4. Is independently testable.
5. Does not expose IP.
6. Facilitates competitive procurement.
7. Encapsulates rapid change.

For each of the SOSA modules, the inputs required to support these functions have been determined (leading to the definition of each SOSA module's inputs), and the products of each of the functions have been defined (leading to the definition of each SOSA module's outputs). A top-level enumeration of the SOSA modules is documented in the SOSA Service View 1 (see Section 4.2), and the details of their interactions are documented in the SOSA Service View 4 (see subsequent sections of this document for SvcV-4 details).

It should be noted that this document specifies what the SOSA modules do, but not how they do it (IP and innovation are preserved).

5.3 Applying the Taxonomy to SOSA Procurable Units

This document does not define implementation approaches or design patterns, but defines the architectural elements, their interfaces and behaviors, and requirements to be applied to those architectural elements. Although a particular implementation approach is not mandated, this document takes into consideration the potential design patterns when determining key interfaces to be standardized and the suitability of potential specifications.

The taxonomy provides a naming convention and hierarchical decomposition of the types of modular elements that can be composed into a sensor. It stops short of defining or implying implementation and procurement-related concepts.

Procurable units – implementations combining one or more items in the SOSA taxonomy in varying design patterns – are evaluated by the Conformance Certification Program. Some combinations are more likely than others, and some portions of the taxonomy require others to be implemented.

SOSA modules, as pure logical entities, do not imply implementation technologies. Modules are implemented by instances of the SOSA infrastructure. Some elements of the SOSA infrastructure can be procurable units on their own. A SOSA procurable unit could implement any number of SOSA modules and infrastructure elements if the interfaces at the conformance boundaries are well-defined and testable.

Below are a few illustrative examples of how the taxonomy elements can be composed into SOSA procurable units. Note that this list is not exhaustive but points out likely implementation patterns for SOSA modules.

- **SOSA Module Portable Software Implementation**
A SOSA module implemented in software which uses standardized APIs to access operating system resources and communication resources. This promotes portability of software. Conformance with the SOSA module is evaluated at the API.
- **SOSA Module Container Implementation**
A SOSA module implemented by software running in a container engine. Conformance with the SOSA module is evaluated at the API to the container engine and at interaction bindings on network interfaces outside of the container engine.
- **SOSA Module Virtual Machine Implementation**
A SOSA module implemented by software running in a hypervisor. Conformance with the SOSA module is evaluated at the API to the hypervisor and at the interaction bindings on network interfaces outside of the container engine.
- **SOSA Module PIC Implementation**
One or more SOSA modules implemented by a SOSA PIC, and which conforms with the PIC interfaces and interactions of each SOSA module it implements by evaluating the card-slot interface and the interaction bindings at the card edge network interfaces.
- **SOSA Module Hardware Element Implementation**
A SOSA module implemented by a SOSA hardware element that does not plug into an OpenVPX™ backplane, and which conforms with the interactions of each SOSA module it implements by evaluating the interaction bindings at its external network interfaces.

5.4 System Management Approach

The SOSA Architecture defines a set of modular elements including processing modules, multi-computer hardware, and distributed software/firmware components, as well as network and runtime infrastructure that will be implemented with varying patterns of hardware, firmware, and software components. To reduce the cost of integration, maintenance, repurposing, and extension of complex sensor and sensor component implementations it is necessary to standardize modules and interfaces to support “housekeeping” functions, which fall in the system management category.

The concept of system management lies largely outside of the mission or operational space. System management functions are not about directly performing the mission, but are about taking care of the system, so it can perform the mission. Thus, system management does not address mission-level tasking or execution and control of the tasks, but ensuring the underlying hardware, software, and firmware can support the task. The System Manager module is

responsible for the system management functions. The Task Manager module supports the tasking and control functions but is not ready for publication in this version of the standard.

General system management functions include discovering, determining capacities, configuring, controlling, monitoring and logging health, handling faults, executing Built-In Tests (BITs), and diagnosing a sensor system and its sensor components.

Hardware system management requires functions including setting-up, managing the configuration, handling faults, and diagnosing the hardware assemblies and elements.

5.5 Airworthiness Concepts and Approach

Airborne ISR systems built from SOSA modules could need airworthiness certification by a government or civilian regulatory agency. This applies if a failure of the system could result in a hazard to the aircraft. This could be because the ISR system has:

- Mechanical or electrical effects such as air loads on an external mounting, electrical loads, crash safety, Electromagnetic Compatibility (EMC), etc.
- Interfaces with flight safety equipment
- Has a dual purpose serving both mission and flight safety functions
- Controls weapons release, Radio Frequency (RF) emissions, etc.

This section provides guidance on developing SOSA modules, including hardware and software, to enable and promote products that can achieve airworthiness certification as part of a system.

This applies to manned and unmanned aircraft systems. This document cannot provide complete instruction on how to perform a safety assessment or correctly use regulatory guidance. It can provide direction on where to find information and some recommendations on best practices. Specific safety practices are outside the scope of this document.

There are differences in military and civilian airworthiness certification, so it is important to know your customer and certification authority, and to be aware of differences. Military programs sometimes use civilian guidance.

SOSA objectives include reducing cost and increasing reusability and portability, which should include airworthiness aspects. SOSA module developers with airworthiness considerations should remember these objectives:

- Design SOSA modules that can be part of a system that can achieve an airworthiness certification, and thus avoid developing a product that will have to be redesigned to adapt to other platforms/systems or have to produce artifacts long after the original work is complete
- SOSA module developers should be aware of airworthiness issues so that even if the short-term use is not safety-critical, it could be more easily adapted in the future to safety-critical applications – this will lead to products where:
 - Appropriate data exists
 - Appropriate verification and qualification were accomplished

- There is partitioning
- Failure cases are identified
- Upgrades can be applied with minimal impact
- Promote reuse of software and artifacts, which helps lower cost of certification when adapted to other systems/platforms

5.5.1 Types of Equipment

Aircraft equipment can be classified in two categories: flight equipment and mission equipment. Flight equipment is pieces of equipment that contribute directly to the safe operation of the aircraft, including communication systems, navigation systems, surveillance systems, safety systems, propulsion systems, control systems, and others. Mission systems are those systems used to accomplish a particular task in-flight, but the failure of which does not affect flight safety (for example, an intelligence collection system would be mission equipment).

Because many sensor systems in the SOSA application domain are anticipated to be mission equipment, the SOSA Technical Standard, Edition 1.0 has addressed mission equipment first. However, there are expected to be cases where a SOSA sensor is dual-use, meaning that sensors could act as part of the mission equipment functions. For that reason, the SOSA Technical Standard is likely to address dual-use (including flight equipment) requirements in the future. Single-purpose flight equipment (e.g., a flight management system) is outside of the scope of this document.

While this document is intended for sensor systems, there is potential for using the SOSA Technical Standard to develop a system of SOSA modules that perform a safety-critical function not related to flight safety of the host aircraft. For example, it is possible to construct a SOSA sensor system that also contains an application for directing the release of and flight control of munitions. Another example is a system that follows the SOSA Technical Standard for hardware and software design but is used to autonomously and/or remotely control Unmanned Aerial Vehicle (UAVs).

5.5.2 Airworthiness of Mission Equipment

The function of mission equipment is often not necessary for safe aircraft operation. Airworthiness of mission equipment includes structural considerations (e.g., crash loads), electrical considerations (e.g., electrical loads analysis), fire risk, and others. These considerations are important to the integrator and are covered under airworthiness certification guidance such as MIL-HDBK-516C for military systems.

Airworthiness aspects of mission equipment directly applicable to the SOSA Architecture are interfaces where SOSA modules directly interface to flight equipment. For example, if a SOSA sensor system directly interfaced via Ethernet to a safety-critical bus, the SOSA module would be required to show that the SOSA module would not affect the safety-critical functions of the bus. However, typical aircraft design would not have mission equipment directly interfaced to safety-critical equipment.

5.5.3 Qualification *versus* Airworthiness

Airworthiness is concerned with the safe operation of the aircraft in flight. Qualification of aircraft systems supports airworthiness but is more specifically the assurance that a particular

system will function as intended in a specific environment such as altitude, temperature, EMC, etc. The SOSA promise is that disparate software/hardware SOSA modules can be easily changed and even that SOSA compatible cards can easily be swapped within a SOSA compatible chassis. However, these changes could affect qualification of the system even if they do not affect the airworthiness of the system. For example, swapping cards between vendors even for the same function could affect power consumption (e.g., cause the system to exceed available power), thermal loads, and vibration tolerances. Therefore, SOSA module vendors should consider what future environments their equipment could encounter and consider what additional qualification would improve their adaptability and utility across platforms.

5.6 Security Concepts and Approach

The security aspects of the SOSA Technical Architecture are an active area of development. The SOSA overall approach is to treat the security aspects of the architecture in a holistic fashion, as opposed to treating the various security disciplines (e.g., anti-tamper, cybersecurity, supply chain risk mitigations, software assurance, etc.) as separate, segregated concerns. The guiding principles for security are consistent with the SOSA Architecture Principles – that the standard leverages/incorporates existing industry and government standards and that the architecture enables resilience and cybersecurity.

The approach to security began with a review of existing DoD and commercial security standards, such as the Anti-Tamper (AT) Technical Implementation Guide (TIG), the DoD Risk Management Framework (RMF), security-related Open Mission System (OMS) Interface Control Documents (ICDs), the Cyber Survivability Endorsement Implementation Guide, and The Open Group Open Trusted Technology Provider™ Standard (O-TTPS), which is technically equivalent to ISO/IEC 20243-1:2018. The approach is also informed by industry best practices, collecting inputs from the various members of the SOSA Consortium. These standards and best practices are being reviewed for their applicability to a SOSA system and the interfaces between SOSA modules, software components, and/or hardware elements, as appropriate. As the SOSA Technical Architecture is refined, the architecture will be reviewed based on these and other standards to ensure that security is built in and to maintain alignment with security requirements from various other open architecture standards.

The security aspects of the SOSA Technical Architecture are implemented in the functions (and behaviors) of the SOSA modules and their interfaces. Security best practices for how SOSA products are developed are intentionally not included in this document. The primary functions and behaviors are implemented in SOSA modules 1.1 (System Manager), 6.1 (Security Services), 6.2 (Encryptor/Decryptor), and 6.3 (Guard/Cross-Domain Service). All SOSA modules are shown in Table 4.2-1 of Section 4.2. The System Manager will manage the start-up of the system (including the secure loading of software), maintain a secure configuration, manage keys used in the system, and authorize/authenticate requests to publish/subscribe messages or access privileged resources and services. Security Services will implement the security functions needed by the System Manager, including verification of software integrity, key management, access control, audit, and other security controls. The Encryptor/Decryptor provides cryptographic services to the System Manager and other applications to ensure that data-at-rest and data-in-transit are protected to the level required by the classification of the data. The Guard/Cross-Domain Service provides applications with the ability to send/receive data across security domains.

5.6.1 Security Manager

In a SOSA sensor, where all components, hardware, software, or firmware are intended to be easily swappable and interoperable, a capability is required to ensure the security posture of the system. Such entity is referred to as the Security Manager, which is a function of the System Manager. Upon system start-up, the Security Manager facilitates the authentication of the hardware and software components of the system which determines the security states of the system. Details on security state transitions are described in Chapter 12.

5.7 SOSA Data Model

The SOSA Data Model is a normalized representation of entities, their associations and views of those entities, and associations to unambiguously document the meaning and structure of the data that occurs in the interfaces defined by the SOSA Technical Standard; for example, in the messages being communicated between SOSA modules. This single set of semantically defined and organized concepts become the building blocks by which all SOSA messages are defined and constructed.

5.7.1 Data Model Structure

The SOSA Data Model structure leverages the rules of construction found in the Open Universal Domain Description Language (Open UDDL), Edition 1.0 to provide a standardized language for formally describing, querying, and communicating concepts within a data model. This allows the SOSA Data Model to follow a top-down architectural approach, based on DoDAF best practices:

- A Conceptual Data Model (DIV-1) documents the domain concepts in terms of FACE conformant Shared Data Model (SDM) observables, as well as in terms of other DIV-1 concepts

The DIV-1 describes the conceptual types, relationships, semantics, and nature of the data to be exchanged while being independent of any specific data representation in terms of units, measurements, or reference frames.

- A Logical Data Model (DIV-2) builds upon DIV-1 content by providing details such as units, measurements, and coordinate systems for the data items in the DIV-1

The DIV-2 is independent of any specific platform data representations.

- A Physical Data Model (DIV-3) documents the physical manifestation of the data (exact format, bits per field, formats, schemas, structures); for example, using JavaScript Object Notation (JSON), eXtensible Markup Language (XML), OMG Interface Definition Language (IDL) or another physical representation definition approach

The transports used to carry the data are defined separately from the data itself; this decoupling ensures that the same data (in the same format) can be carried between source and destination by different means (and as necessary).

5.7.2 DIV-1: Conceptual Data Model

The SOSA Conceptual Data Model (DIV-1) documents the nature of, and relationships among, the many “pieces” of information required for the operation and upkeep of the SOSA sensor ecosystem. The DIV-1 is constructed of entities and entity associations related to one another in

such a way as to provide a semantic framework by which all SOSA concepts can be semantically specified unambiguously. Entities and associations are constructed with attributes typed as either SDM observables or typed as other DIV-1 entities or associations and are minimally composed to precisely represent the nature of the entity or association itself. Connections between entities and associations are constructed to accurately represent how each of the entities and associations relate to one another. The Conceptual Data Model is self-describing and should not require any additional information to understand its meaning.

5.7.3 DIV-2: Logical Data Model

The SOSA Logical Data Model (DIV-2) further specifies the conceptual entities in the DIV-1 to a lower level of abstraction by including logical details such as units, measurements, measurement systems, coordinate systems, and reference points (e.g., a position is broken down into its constituent three-dimensional parts, a speed is provided for its unit of measure, an enumeration is given its respective possibilities of literals). It should be noted that the DIV-2 does not define the physical representation (e.g., number of digits, precision, etc.) so that the same data item can be represented differently depending on the need.

DIV-1 entities are realized in the DIV-2 with their DIV-1 observable types substituted with DIV-2 measurements. This substitution allows for the same DIV-1 concept to be realized in the DIV-2 in various ways to satisfy the needs of SOSA interfaces.

5.7.4 DIV-3: Physical Data Model

The SOSA Physical Data Model (DIV-3) further specifies the logical representation of SOSA entities with the addition of platform-specific specification such as primitive types.

As part of the DIV-3 specification, views of the data model are constructed to represent the payloads of SOSA messages. These views use queries and templates as defined in the Open UDDL Standard to specify both the semantic meaning of the data along with the structure of the data as needed by a SOSA interface message.

5.7.5 Data Model Formats and Usage

As mentioned, the SOSA Data Model follows the rules of construction as defined by the Open UDDL Standard. Following these rules of construction, the SOSA Data Model is defined in a FACE conformant format, which is then used to generate the various formats defined by the SOSA Technical Standard. The format needed for FACE Transport Services Segment (TSS) interfaces is generated directly. The FACE Conformance Test Suite (CTS) is used to generate OMG IDL 4.0 files representing the templated views of the SOSA interfaces, which can then, in turn, be used to generate other message formats such as Google[®] Protocol Buffer files or Open API Specification (OAS) files.

The FACE version of the data model is importable into Enterprise Architect, MagicDraw/Cameo, or Rhapsody using Vanderbilt University's freely available tools.¹

¹ Refer to: <https://www.vanderbilt.edu/cdr/module1/other-interactive-tools/>.

5.8 Inter-Module Interaction Approach

5.8.1 Inter-Module Interactions

The SOSA Architecture is composed of a set of loosely-coupled modular entities that interact with each other via well-defined logical interfaces implemented by the underlying SOSA infrastructure. Interoperability between modular entities is described in terms of interactions, which are realized as messages on network interconnects. The network implementation of the interactions (encoding, encapsulation, transport, etc.) is identical whether implemented in hardware, software, or firmware. In portable software, SOSA modules leverage APIs to the interaction infrastructure, which realizes the interactions as network messages.

5.8.2 SOSA Sensor Interconnects

A SOSA sensor interconnect is a communication mechanism via which sensor components interoperate by engaging in interactions. SOSA sensor interconnects should be considered types of communication mechanism, not instances. The example shown in Figure 5.8.2-1 has exactly one instance of each SOSA sensor interconnect type; a SOSA sensor could have more than one instance of any of the interconnect types.

Figure 5.8.2-1 illustrates some of the interconnects this document defines to support interoperability between SOSA modules and hardware elements. The SOSA Message Interconnect and the SOSA Wideband Low-Latency Interconnect are Ethernet-based networks. The difference is that the former is a general-purpose network, while the latter supports more demanding Quality of Service (QoS) metrics, including higher data rates and lower, more consistent delivery latency.

Note that these are not the only interconnects supported by the SOSA Technical Architecture. SOSA sensors could include well-defined interconnects in addition to those shown in Figure 5.8.2-1, to meet performance and other requirements – and these will be specified in a future version of this document.

SOSA modules interoperate in various ways, and at different timescales, but generally interoperate via well-defined non-proprietary interfaces implementing standard interactions supported by SOSA sensor interconnects.

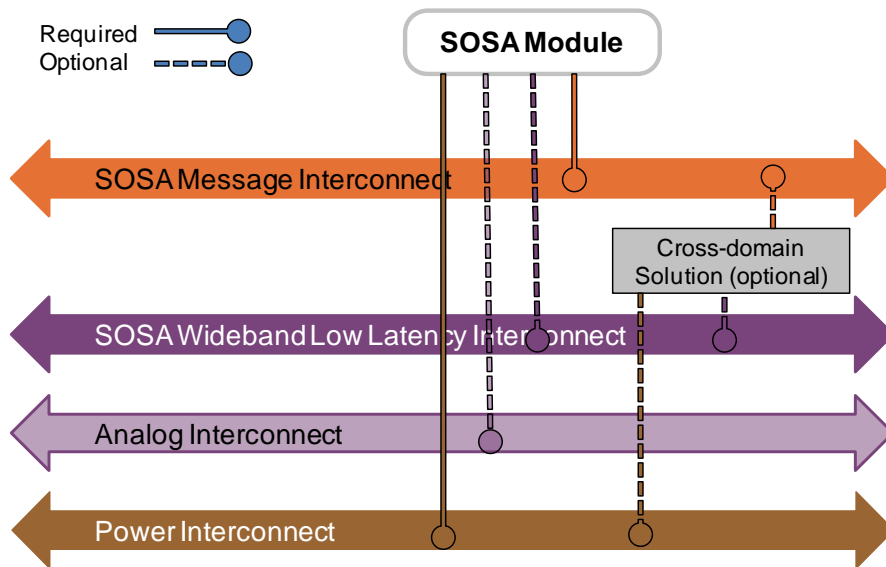


Figure 5.8.2-1: Default SOSA Sensor Interconnects

6 System Management

The SOSA Architecture applies a holistic approach to system management of the sensor and its individual sensor components (e.g., modules, hardware elements). The overall system management concepts are defined in Section 6.1.

Sensor components can be *managed* or *unmanaged*. Managed sensor components are SOSA conformant entities of the sensor that can be supervised via the capabilities and interfaces defined by the SOSA system management architecture. Unmanaged sensor components are those SOSA conformant entities of the sensor that are not capable of being supervised via the capabilities and interfaces defined by the SOSA system management architecture. Conformant managed SOSA sensor components can be implemented with the system management interfaces and capabilities *built* into the component itself to enable *direct* management of the component. Alternately, responsibility for the implementation of the system management interfaces and capabilities to manage one component can be *affixed* or *assigned* to a second SOSA component that then represents and enables management of the first component in an *indirect* but still conformant manner.

6.1 System Management Architecture

Figure 6.1-1 shows the SOSA system management architectural approach. The System Manager is the SOSA module responsible for providing system management functionality to and for managed SOSA modules, PICs, and other hardware elements (e.g., power supplies, network switches). Functionality is provided via a set of system management services. The ability to manage and interact with these system management services is enabled through well-defined sets of APIs and sensor component messages.

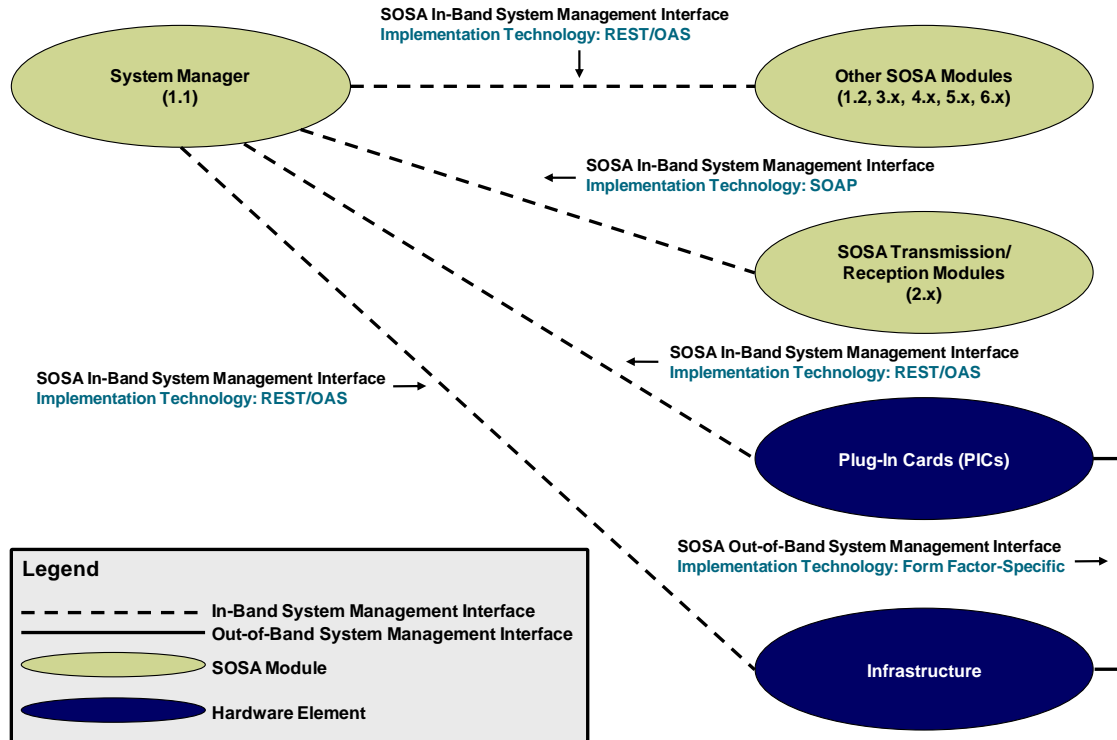


Figure 6.1-1: SOSA System Management Architectural Approach

The SOSA system management architecture provides both in-band and out-of-band management functionality. In-band system management refers to management functionality that is enabled via the System Manager over the SOSA Message Interconnect network. Its operation requires that the network is online, configured correctly, and operating as expected such that messaging between nodes on the network is possible. In-band system management capabilities are directly supported between the System Manager and managed PICs, SOSA modules, and infrastructure items, such as power supplies and network switches that are conformant with the SOSA Technical Standard. In-band system management is the primary mechanism for SOSA system management and is form factor-independent in its implementation.

Out-of-band system management refers to management functionality that is present and available even when the SOSA Message Interconnect is offline, configured incorrectly, and/or not operating as expected such that messages between the System Manager and one or more networked nodes are not possible. Situations in which this condition might occur include but are not limited to initial start-up and shutdown conditions, faulted hardware, software faults, improper configuration, over/under provisioned network, infrastructure faults, and/or malicious events such as cyber-based attacks. In some implementations, out-of-band system management might also be available in *lights-out* situations, which is when primary power is disabled and/or inhibited to the platform and only auxiliary or stand-by power is available. Out-of-band system management is a secondary mechanism for SOSA system management. It is also form factor-dependent in its implementation as it leverages pre-existing capabilities of the underlying electro-mechanical form factor standards for the hardware elements (i.e., the PICs and infrastructure). Figure 6.1-2 shows how the out-of-band system management architecture is realized for SOSA conformant VPX-based PICs and infrastructure.

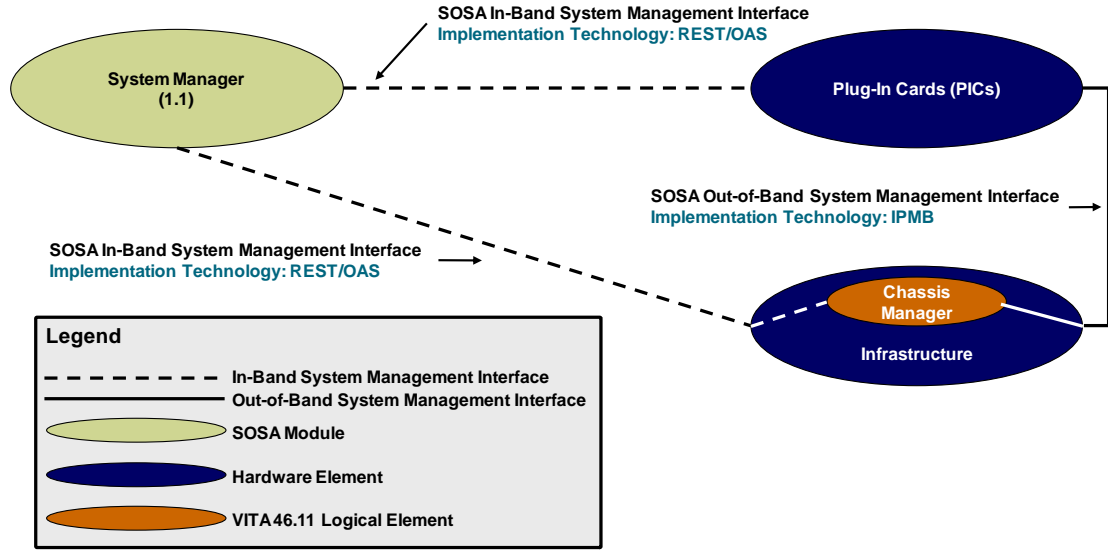


Figure 6.1-2: SOSA Out-of-Band System Management Architectural Realization: VPX Form Factor

6.1.1 System Manager Functionality

As shown in Figure 6.1.1-1, the functionality of the System Manager is decomposed and organized into two primary functional groups called Manage Sensor and Manage Sensor Security. The former functional group is associated with all non-security-related system management functionality and the latter functional group is associated with only security-related system management functionality. This distinction was made in the system management architecture to preserve clear separation in the security-related system management functions to allow for them to potentially be spun out into their own module in a future version of this document.

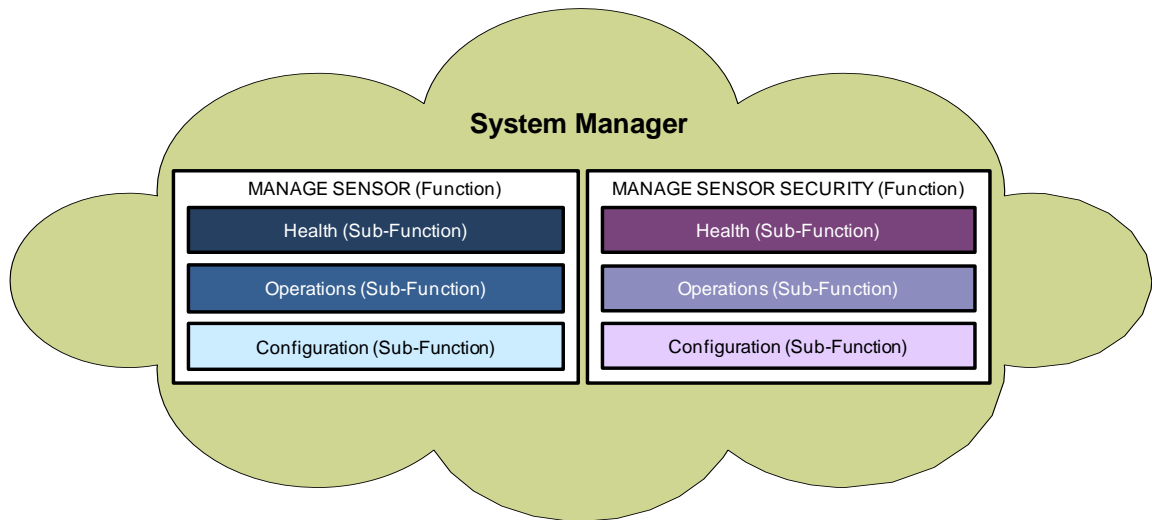


Figure 6.1.1-1: System Manager Functional Decomposition

The second level of System Manager functional decomposition shown in Figure 6.1.1-1 organizes functionality into three secondary functional groups: Health, Operations, and Configuration. The Health secondary functional group contains the system management

capabilities and features needed to determine, control, and report on the condition of the sensor and its underlying sensor components. The Operations secondary functional group contains the system management capabilities and features to determine, control, and report on the state and mode of the sensor and its underlying sensor components from the System Manager’s viewpoint. The Configuration secondary functional group contains the system management capabilities and features to determine, control, and report on the sensor inventory, composition, and parameterization at the level of the sensor and its individual underlying sensor components.

The complete functionality of the System Manager module is defined in the Service View 4 (SvcV-4: Services Functionality Description) shown in Table 6.1.1-1. The first three columns in Table 6.1.1-1 define the functional groups that form a hierarchical decomposition of the in-band system management functions. Column 1 shows the primary, or Functional Group 1, decomposition. Column 2 shows the secondary, or Functional Group 2, decomposition. The third and fourth columns introduce a tertiary, or Functional Group 3, decomposition, and their associated definitions. The Functional Group 3 decomposition lists functional capabilities of the System Manager with the expectation that further decomposition defines distinct features that enable the capability.

Table 6.1.1-1: SOSA System Manager Functions (SvcV-4)

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Sensor	Manage Sensor Health	Monitor Sensor Health	Keep track of and report on the current and/or projected condition and well-being of the sensor and/or the underlying sensor components that comprise the sensor.
Manage Sensor	Manage Sensor Health	Manage Sensor Diagnostics	Coordinate and/or perform the execution of test sequences to determine the operational status of the sensor and/or the individual sensor components that comprise the sensor and/or report the findings of such actions.
Manage Sensor	Manage Sensor Health	Manage Sensor Health Logging	Administer records that keep track of and/or report on the past, current, and/or projected condition and well-being of the sensor and the underlying sensor components that comprise the sensor.
Manage Sensor	Manage Sensor Operations	Manage Sensor State	Monitor, report, control, and/or perform state and/or state changes for the sensor and/or the sensor components that comprise the sensor.
Manage Sensor	Manage Sensor Operations	Manage Sensor Mode	Monitor, report, control, and/or perform mode and/or mode changes for the sensor and/or the sensor components that comprise the sensor.
Manage Sensor	Manage Sensor Configuration	Manage Sensor Inventory	Discover, aggregate, verify, and/or report on the procurable unit contents (i.e., sensor components) contained within the sensor and/or the sensor components that comprise the sensor.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Sensor	Manage Sensor Configuration	Manage Sensor Composition	Monitor, verify, aggregate, report, and/or control the make-up and/or arrangement of the resources identified by the sensor inventory (i.e., sensor components) to address the needs of a particular sensor realization.
Manage Sensor	Manage Sensor Configuration	Manage Sensor Parameterization	Monitor, verify, aggregate, report, and/or control the state of user-controllable features/settings of a composed sensor realization.
Manage Sensor Security	Manage Sensor Security Health	Monitor Sensor Security	Collect and/or analyze available indicators to identify anomalies associated with, but not limited to, intrusions, exfiltration, and/or unintended and/or unexpected malicious actions.
Manage Sensor Security	Manage Sensor Security Health	Manage Sensor Security Diagnostics	Coordinate and/or perform the execution of test sequences to determine the operational status of the modules and other protection features of the sensor and/or the individual sensor components that comprise the sensor to ensure the integrity of the system on a routine basis and/or as a reaction to an event, and/or report the findings of such actions.
Manage Sensor Security	Manage Sensor Security Health	Manage Sensor Security Logging	Administer records that keep track of and/or report on the past, current, and/or projected sensor security condition and/or the underlying sensor components security condition that comprise the sensor security condition.
Manage Sensor Security	Manage Sensor Security Operations	Manage Sensor Security Mode	Monitor, report, supply, and/or control security mode and/or security mode changes of the sensor security operation and/or of the sensor components security operation that comprise the sensor security operation.
Manage Sensor Security	Manage Sensor Security Configuration	Manage Sensor Security Parameterization	Monitor, verify, aggregate, report, and/or control the settings of user-controllable features realized via composed sensor security capabilities and/or the composed sensor components' security capabilities that comprise the sensor security capabilities.

6.1.2 In-Band System Management Interactions

SOSA in-band system management functionality is implemented through a combination of request-response and event-notification interaction types. The request-response interactions can support set and get operations on the system management parameter(s). The event-notification interactions are one-to-many relationships where one endpoint monitors the occurrence of an event, or change of state, and then sends notification messages to a pre-established set of endpoints when an event occurs.

All in-band system management interactions follow a client/server pattern in which the managing entity (System Manager module) provides management clients, managers, and the managed entities provide management agents. Managers and agents exchange messages to implement interactions and realize a particular system management functional capability and/or its underlying feature(s). Figure 6.1.2-1 shows this client/server paradigm and introduces the terminology of managers and agents, where the former are the clients, and the latter are the servers in the paradigm. Additionally, Figure 6.1.2-1 assigns the manager/agent relationship to the secondary functional decomposition level. Thus, applying the terminology and methodology introduced in Figure 6.1.2-1 to the Functional Group 2 decomposition content from the second row in Table 6.1.1-1, a health manager/health agent pair can be derived and leveraged to describe the one or more interactions needed to satisfy the Monitor Sensor Health capability listed in the associated Functional Group 3 cell. This ultimately creates becomes the basis of the master/agent interactions paradigm for SOSA in-band system management.

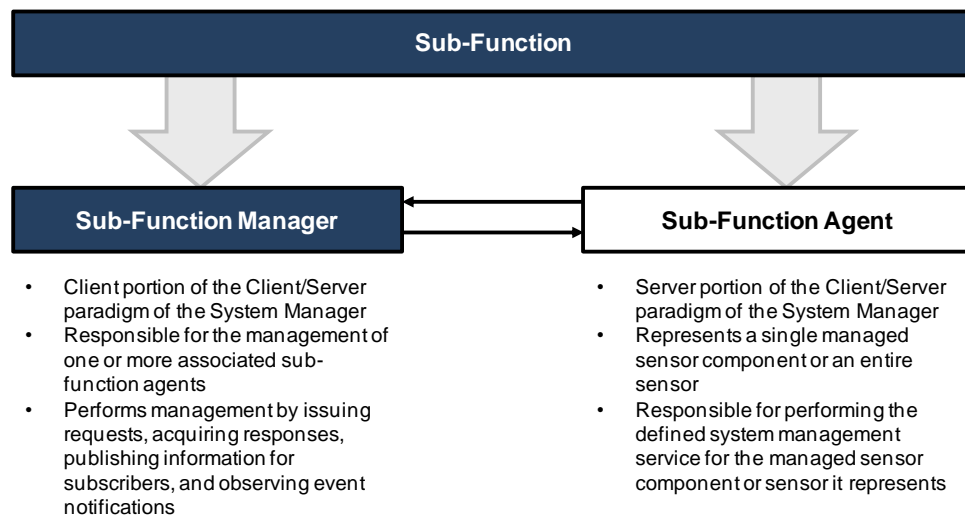


Figure 6.1.2-1: SOSA System Management Client/Server Interactions Paradigm

Figure 6.1.2-1 shows a graphical representation of the extension of the previous master/agent paradigm example to include the complete set of functionalities captured in Table 6.1.1-1. Looking at Figure 6.1.2-1, a few observations can be made. First, the System Manager includes both a master and an agent for each secondary functional decomposition entity. This is necessary because the System Manager needs to both manage and provide interfaces to manage each of the sensor components within the sensor and the entire sensor as its own entity. Second, the roll up of system management functionality is only possible when a path of agents and managers exists from the requesting entity all the way to the entity being managed, and that some of these agents and managers will exist outside of the System Manager direct responsibilities. Managed sensor components need to provide the necessary conformant agent and/or manager interfaces to participate in the system management architecture. Sensor component suppliers and/or integrators need to integrate the SOSA conformant system management interfaces and adapt them to any proprietary or alternate standards implementations that exist, as required, within the agents and/or managers they implement to perform the intended SOSA system management functionality in a conformant manner.

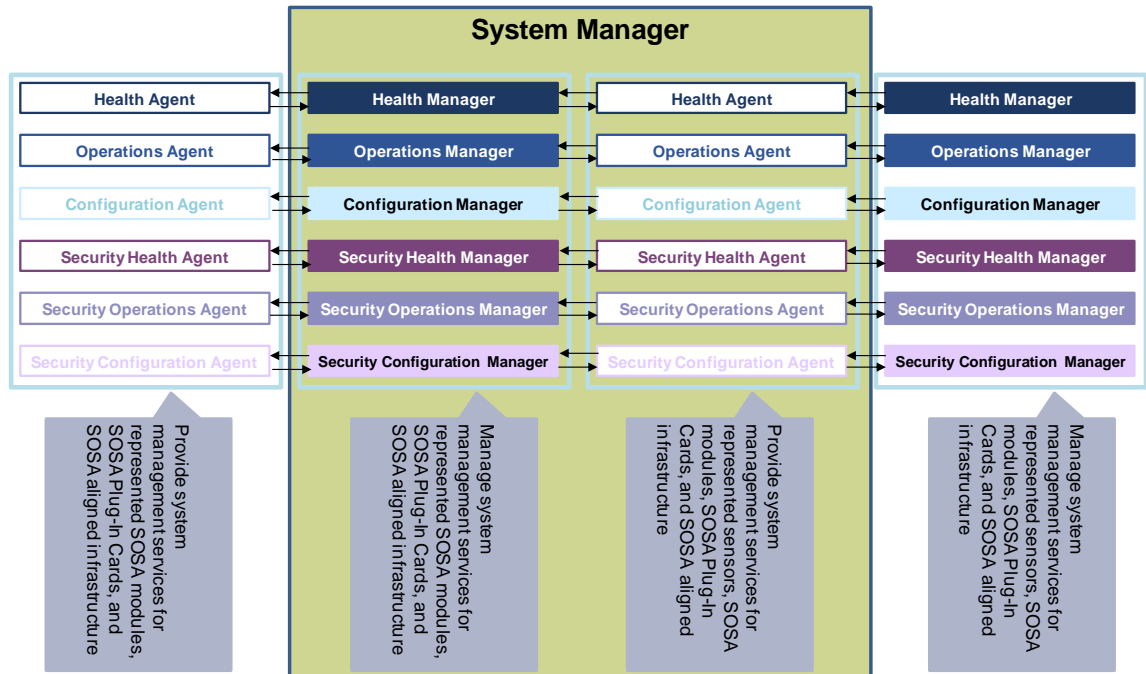


Figure 6.1.2-2: SOSA In-Band System Management Manager/Agent Paradigm

6.2 In-Band System Management Definitions

This section defines the specific requirements of the in-band system management interfaces to the various types of sensor components defined by this document.

6.2.1 In-Band System Management General Profile Technology Bindings

The following rules apply to the technology bindings for the in-band system management interfaces defined in this section.

Observation 6.2.1-1: This document employs the concept of “profiles” for technology bindings. The General Profile is the default profile. In the case that the technology bindings associated with the General Profile are inappropriate due to safety and/or security requirements, this document will support additional profiles with technology stacks to meet those requirements. Additional profiles will be documented in future change proposals.

Rule 6.2.1-1: Where a SOSA sensor component provides an in-band system management interface, that SOSA sensor component shall implement an Internet Protocol (IP)-based interface for in-band system management interactions with other SOSA sensor components. Conformance Methodology (D)

Rule 6.2.1-2: In the General Profile, when a SOSA sensor component provides an in-band system management interface, and when the in-band system management interface to that SOSA sensor component is not specified otherwise, that SOSA sensor component shall implement in-band system management request-response interactions with other SOSA sensor components with a JSON encoding over HTTP as defined at <http://spec.openapis.org/oas/v3.0.3>. Conformance Methodology (D) (evaluate the protocol and format of the messages only).

Rule 6.2.1-3: In the General Profile, when a SOSA sensor component provides an in-band system management interface, and when the in-band system management interface to that SOSA sensor component is not specified otherwise, that SOSA sensor component shall implement in-band system management event notification interactions with other SOSA sensor components with a JSON encoding over HTTP as defined at <http://spec.openapis.org/oas/v3.0.3#callback-object>. Conformance approach: Demonstrate (evaluate the protocol and format of the messages only)

Observation 6.2.1-2: Sensor components with in-band system management interfaces that are specified otherwise include the 2.x modules.

Observation 6.2.1-3: Request-response and event notification interactions between SOSA sensor components are documented using Version 3.0.3 of the OpenAPI Specification format as defined at <http://spec.openapis.org/oas/v3.0.3#format>.

6.2.2 In-Band System Management Definition Structure

Each of the in-band system management definition sections that follow consists of a table of functions, a table of interactions, a set of rules, and an OpenAPI Specification definition. The OpenAPI definitions are attached in Appendix B.

The function and interaction tables include a column titled “Support”. A value of “V1.0” indicates that this version of the standard defines OpenAPI endpoints to implement the function or interaction. A value of “Future” indicates that the SOSA Technical Working Group plans to define OpenAPI endpoints to implement the function or interaction in a future version of this document.

6.2.3 System Manager Module In-Band System Management Definitions

This section defines the interactions provided by the System Manager module, which allows the sensor system to be managed from the outside, and provides functionality needed by the Task Manager.

6.2.3.1 System Manager In-Band System Management Functions

Table 6.2.3.1-1 provides the detailed list of in-band system management functions to be provided by SOSA modules by default.

Note that the content of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.3.1-1: SOSA System Manager Module In-Band System Management Functions

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Health	Notify Sensor Health Alerts	Supply data that indicates a change in health information for the sensor.	V1.0
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Built-In Test Parameter Settings	Supply data that describes the current parameter settings for a BIT for a sensor.	Future
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Parameter Settings	Solicit data that describes the current parameter settings for a BIT for a sensor component.	Future

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Diagnostics	Execute Update Sensor Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Update Sensor Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Action Start Sensor Built-In Test	Initiate a BIT for a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Execute Action Start Sensor Component Built-In Test	Initiate a BIT for a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor component.	V1.0
Manage Sensor Health Logging	Provide Sensor Health Log Data	Supply data that describes the past, current, and/or projected condition and well-being of a sensor.	V1.0
Manage Sensor Health Logging	Provide Sensor Health Logging Configuration	Supply data that describes the current configuration settings for sensor logging for a sensor.	V1.0
Manage Sensor Health Logging	Execute Update Sensor Health Logging Configuration	Modify the configuration settings for sensor logging for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Health Logging	Provide Sensor Health Logging Parameter Settings	Supply data that describes the current parameter settings for sensor health logging for a sensor.	V1.0
Manage Sensor Health Logging	Execute Update Sensor Health Logging Parameter Settings	Modify the parameter settings for sensor health logging for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Health Logging	Provide Sensor Health Logging Health	Supply data that describes the health of the sensor health logging function of a sensor.	V1.0
Manage Sensor Health Logging	Notify Sensor Health Logging Health Alerts	Supply data that indicates a change in health of the health logging function of a sensor.	V1.0

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Health Logging	Provide Sensor Health Logging Health Alert Parameter Settings	Supply data that describes the current parameter settings for health alerts for the health logging function of a sensor.	V1.0
Manage Sensor Health Logging	Execute Update Sensor Health Logging Health Alert Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Health Logging	Execute Action Delete Health Log Data	Delete the portion(s) of the sensor health log for a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Health Logging	Execute Action Sanitize Health Log	Sanitize the portion(s) of the sensor health log for a sensor as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Provide Sensor State	Supply data that describes the current state for the sensor.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor State Events	Supply data that indicates a change in state status, or state transition, for a sensor.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor State	Perform a state transition on a sensor as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Request Action Restart Sensor	Initiate a <i>Restart</i> function on a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor	Receive and act upon a request to shut down the sensor. This will include different types of shutdowns, indicated by a parameter, including Gracefully and Instantly.	V1.0

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Mode	Supply data that describes the current mode for the sensor.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0
Manage Sensor Mode	Notify Sensor Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor.	V1.0
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Mode	Perform a mode transition on a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Zeroize Sensor	Initiate a <i>Zeroize</i> function on a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor	Initiate a <i>Sanitize</i> function on a sensor as solicited by the <i>Request Action</i> function.	V1.0

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Inventory	Provide Sensor Inventory Information	Supply data that identifies the aggregate list current procurable entities contained within the sensor.	Future
Manage Sensor Inventory	Execute Action Register Sensor Component Inventory Information	Initiate the registration of sensor component inventory information in the sensor inventory information representation as solicited by the <i>Register Sensor Component Inventory Information</i> function.	Future
Manage Sensor Composition	Provide Sensor Firmware Package Info	Supply data that identifies the firmware package running on a component in the sensor.	V1.0
Manage Sensor Composition	Execute Update Sensor Firmware Package	Perform a replacement of one or more firmware and/or software elements on the sensor as solicited by the <i>Request Update Sensor Firmware Package</i> function.	V1.0
Manage Sensor Composition	Execute Action Verify Sensor Firmware Package	Perform verification of the sensor firmware package as solicited by the <i>Verify Sensor Firmware Package</i> function. Verification of authenticity will be provided by the Security Services module.	Future
Manage Sensor Composition	Provide Resources	Provide list of resources on a hardware element, module, or RTE, including current reservation status.	Future

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Composition	Execute Action Reserve Resource	Provide reservation of resources requested or deny request.	Future
Manage Sensor Composition	Execute Action Release Resource Reservation	Release reservation made earlier.	Future
Manage Sensor Composition	Provide Cryptographic Resources	Provide list of cryptographic resources.	Future
Manage Sensor Parameterization	Provide Sensor Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor.	V1.0
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0
Manage Sensor Parameterization	Notify Sensor Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor.	V1.0
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor as solicited by the <i>Request Update Sensor Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Configuration	Perform verification of the sensor configuration as solicited by the <i>Verify Sensor Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor.	V1.0
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Parameterization	Execute Update Sensor Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Monitor Sensor Security	Provide Sensor Security Status	Supply data that describes the current security status of a sensor.	Future
Monitor Sensor Security	Provide Sensor Component Security Status	Supply data that describes the security-relevant status of a sensor component.	Future
Monitor Sensor Security	Provide Sensor Security Status Parameter Settings	Solicit data that describes the current parameter settings for the security status reporting functions for a sensor.	Future
Monitor Sensor Security	Provide Sensor Component Security Status Parameter Settings	Supply data that describes the current parameter settings for the security status reporting functions for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Security Status Parameter Settings	Modify the parameter settings for the security monitoring and reporting functions for a sensor as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Status Parameter Settings	Modify the parameter settings for the security status reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Notify Sensor Security Alerts	Supply data that indicates a security event for the sensor.	Future
Monitor Sensor Security	Notify Sensor Component Security Alerts	Supply data that indicates a security event for a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Alerts Parameter Settings	Supply data that describes the current parameter settings for security alerts for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Alerts Parameter Settings	Modify the parameter settings for security alerts for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Security Mode	Provide Sensor Security Mode	Supply data that describes the current security mode for the sensor.	Future

SOSA Functional Group 3	System Manager Module Function Name	Definition	Support
Manage Sensor Security Mode	Notify Sensor Security Mode Events	Supply data that indicates a change in security mode status, or security mode transition, for a sensor.	Future
Manage Sensor Security Mode	Execute Action Sensor Security Mode	Perform a security mode transition on a sensor as solicited by the <i>Request Action</i> function.	Future
Manage Sensor Security Mode	Execute Action Attest Sensor Component Trust	Execute the attestation of component trust to determine granting of privileged access per policy.	Future
Manage Sensor Security Parameterization	Provide Sensor Security Configuration	Provide a report of the overall sensor security configuration upon request. Note that the sensor configuration information is obtained through interactions with the various sensor components to obtain their configuration information.	Future
Manage Sensor Security Parameterization	Notify Sensor Security Configuration Change	Send notifications of changes in the security configuration of the sensor.	Future
Manage Sensor Security Parameterization	Verify Sensor Security Configuration	Determine whether the current sensor security configuration is acceptable based on current context/configuration mode. This determination could be specific to a particular sensor or mission. Common action is to indicate whether the configuration is verified by sending a notification and reporting status.	Future
Manage Sensor Security Parameterization	Execute Update Sensor Security Configuration	Receive and act upon a request to update the security configuration of the sensor.	Future

6.2.3.2 System Manager In-Band System Management Interactions

In-band system management interactions provided by the System Manager (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.3.2-1.

Note that each interaction in Table 6.2.3.2-1 can be mapped back to a function in the in-band system management functions table (Table 6.2.3.1-1) for this interface. To make the table fit into the document format, the mapping to the System Manager Function Name was not included in the table. The information is tracked in the source material for these tables.

Table 6.2.3.2-1: System Manager Module In-Band System Management Interactions

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getSensorHealth	Request Response		SensorHealth	V1.0
getSensorFaults	Request Response		FILTEREDLIST Fault	V1.0
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getSensorHealthParameters	Request Response		DICTIONARY SensorComponent ComponentHealthParameters	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateSensorHealthParameters	Request Response	ComponentHealthParameters, ComponentId		Future
updateHealthParameters	Request Response	ComponentHealthParameters		Future
notifySensorHealthCallback	Event Notification	HealthNotification		V1.0
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getSensorHealthCallbacks	Request Response		LIST Callback	V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createSensorHealthCallback	Request Response	Callback	Callback	V1.0
deleteSensorHealthCallback	Request Response	CallbackId		V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getSensorBitConfig	Request Response		DICTIONARY SensorComponent BITConfig	Future
getBitConfig	Request Response		BITConfig	Future
updateSensorBitConfig	Request Response	BITConfig, ComponentId		Future
updateBitConfig	Request Response	BITConfig		Future
executeSensorBIT	Request Response	ComponentId		V1.0
executeBIT	Request Response			V1.0
getSensorBITResults	Request Response		DICTIONARY SensorComponent BITResults	V1.0
getBITResults	Request Response		BITResults	V1.0
getLoggerData	Request Response		FILTEREDLIST LogEvent	V1.0
getLoggerConfiguration	Request Response		LoggerConfiguration	V1.0
updateLoggerConfiguration	Request Response	LoggerConfiguration		V1.0
getLoggerHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateLoggerHealthParameters	Request Response	ComponentHealthParameters		V1.0
getLoggerHealth	Request Response		ComponentHealth	V1.0
getLoggerFaults	Request Response		LIST Fault	V1.0
notifyLoggerHealthCallback	Event Notification	HealthNotification		V1.0
getLoggerHealthCallbacks	Request Response		LIST Callback	V1.0

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
createLoggerHealthCallback	Request Response		Callback	V1.0
deleteLoggerHealthCallback	Request Response	CallbackId		V1.0
deleteLoggerData	Request Response	DeleteLogEventRequest		V1.0
getSensorState	Request Response		DICTIONARY SensorComponent ComponentState	V1.0
getState	Request Response		ComponentState	V1.0
notifySensorStateCallback	Event Notification	StateNotification		V1.0
notifyStateCallback	Event Notification	StateNotification		V1.0
restartSensor	Request Response			V1.0
restartSensorComponent	Request Response			V1.0
shutdownSensor	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getSensorStateCallbacks	Request Response		LIST Callback	V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createSensorStateCallback	Request Response	Callback	Callback	V1.0
deleteSensorStateCallback	Request Response	CallbackId		V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getSensorMode	Request Response		DICTIONARY SensorComponent ComponentMode	V1.0
getMode	Request Response		ComponentMode	V1.0
notifySensorModeCallback	Event Notification	ModeNotification		V1.0
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateSensorMode	Request Response	ComponentMode, ComponentId		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroizeSensor	Request Response	ZeroizeConfig		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitizeSensor	Request Response	SanitizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getSensorModeCallbacks	Request Response		LIST Callback	V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createSensorModeCallback	Request Response	Callback	Callback	V1.0
deleteSensorModeCallback	Request Response	CallbackId		V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getSensorInventory	Request Response		DICTIONARY SensorComponent ComponentInventory	Future
getSensorFirmwareInfo	Request Response	ComponentId	FirmwarePackageInfo	V1.0
updateSensorFirmware	Request Response	FirmwarePackage, ComponentId		V1.0
verifySensorFirmware	Request Response	VerifyFirmwareRequest, ComponentId		Future
getResources	Request Response		HardwareResources	Future
reserveResources	Request Response	ResourceReservationRequest	ResourceReservation	Future
releaseResources	Request Response	ReservationId		Future
getSensorConfig	Request Response		SensorConfig	V1.0
getSystemManagerConfig	Request Response		SystemManagerConfig	V1.0
notifySensorConfigCallback	Event Notification	SensorConfigNotification		V1.0
notifySystemManagerConfigCa llback	Event Notification	SystemManagerConfigNotific ation		V1.0
updateSensorConfig	Request Response	SensorConfig		Future
updateConfig	Request Response	SystemManagerConfig		Future
verifySensorConfig	Request Response	VerifyConfigRequest, ComponentId		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getSensorConfigCallbacks	Request Response		LIST Callback	V1.0
getConfigCallbacks	Request Response		LIST Callback	V1.0

System Manager Module Interaction Name	Interaction Type	Input Object	Output Object	Support
createSensorConfigCallback	Request Response	Callback	Callback	V1.0
deleteSensorConfigCallback	Request Response	CallbackId		V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0
deleteConfigCallback	Request Response	CallbackId		V1.0
getSensorSecurityStatus	Request Response		SensorSecurityStatus	Future
getSecurityStatus	Request Response		SecurityStatus	Future
getSensorSecurityStatusParameters	Request Response		DICTIONARY SensorComponent SecurityStatusParameters	Future
getSecurityStatusParameters	Request Response		SecurityStatusParameters	Future
updateSensorSecurityStatusParameters	Request Response	SecurityStatusParameters, ComponentId		Future
updateSecurityStatusParameters	Request Response	SecurityStatusParameters		Future
notifySecurityCallback	Event Notification	SecurityNotification		Future
getSecurityCallbacks	Request Response		LIST Callback	Future
createSecurityCallback	Request Response	Callback	Callback	Future
deleteSecurityCallback	Request Response	CallbackId		Future

6.2.3.3 System Manager In-Band System Management Interface Rules

Rule 6.2.3.3-1: In the General Profile, when the SOSA System Manager module is not implemented as a SOSA module implemented by software using the operating system API to access operating system resources and the transport API to access communication resources, the SOSA System Manager module shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.3.3-2: In the General Profile, when the SOSA System Manager module is not implemented as a SOSA module implemented by software using the operating system API to access operating system resources and the transport API to access communication resources, the SOSA System Manager module shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T)

Rule 6.2.3.3-3: In the General Profile, when the SOSA System Manager module is implemented as a SOSA module implemented by software using the operating system API to access operating system resources and the transport API to access communication resources, the SOSA interaction infrastructure shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.3.3-4: In the General Profile, when the SOSA System Manager module is implemented as a SOSA module implemented by software using the operating system API to access operating system resources and the transport API to access communication resources, the SOSA System Manager module shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T)

6.2.4 Generic SOSA Module In-Band System Management Definitions

This section defines the in-band system management interactions provided by the SOSA modules by default, if they are not otherwise specified in this document. For example, Section 6.2.3.2 defines the interactions for the System Manager module, so the definitions in this section do not apply to the System Manager module.

6.2.4.1 Generic SOSA Module In-Band System Management Functions

Table 6.2.4.1-1 provides the detailed list of in-band system management functions to be provided by SOSA modules by default.

Note that the content of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.4.1-1: Generic SOSA Module In-Band System Management Functions

SOSA Functional Group 3	Generic SOSA Module Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future

SOSA Functional Group 3	Generic SOSA Module Function Name	Definition	Support
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0

SOSA Functional Group 3	Generic SOSA Module Function Name	Definition	Support
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0

6.2.4.2 Generic SOSA Module In-Band System Management Interactions

In-band system management interactions provided by the Generic SOSA module (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.4.2-1.

Note that each interaction in Table 6.2.4.2-1 can be mapped back to a function in the in-band system management functions table (Table 6.2.4.1-1) for this interface. To make the table fit into

the document format, the mapping to the Generic SOSA Module Function Name was not included in the table. The information is tracked in the source material for these tables.

Table 6.2.4.2-1: Generic SOSA Module In-Band System Management Interactions

Generic SOSA Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateHealthParameters	Request Response	ComponentHealthParameters		Future
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0
getState	Request Response		ComponentState	V1.0
notifyStateCallback	Event Notification	StateNotification		V1.0
restartSensorComponent	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0

Generic SOSA Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getMode	Request Response		ComponentMode	V1.0
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0
getModuleConfig	Request Response		ModuleConfig	V1.0
notifyModuleConfigCallback	Event Notification	ModuleConfigNotification		V1.0
updateConfig	Request Response	ModuleConfig		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getConfigCallbacks	Request Response		LIST Callback	V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0
deleteConfigCallback	Request Response	CallbackId		V1.0

6.2.4.3 Generic SOSA Module In-Band System Management Interface Rules

Rule 6.2.4.3-1: In the General Profile, SOSA modules shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.4.3-2: In the General Profile, SOSA modules for which interactions are not otherwise specified, shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T) (Interact with the Generic SOSA module in-band system management interface via network messages and evaluate whether it conforms to the rules.)

6.2.5 Security Services Module In-Band System Management Definitions

This section defines interactions provided by the Security Services module, which allows the security subsystems to be managed by the System Manager or other clients.

6.2.5.1 Security Services In-Band System Management Function

Table 6.2.5.1-1 provides the detailed list of in-band system management functions to be provided by the Security Services module.

Note that the content of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.5.1-1: Security Services Module In-Band System Management Functions

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Parameter Settings	Solicit data that describes the current parameter settings for a BIT for a sensor component.	Future

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Manage Sensor Diagnostics	Execute Update Sensor Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Action Start Sensor Component Built-In Test	Initiate a BIT for a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Composition	Execute Action Verify Sensor Firmware Package	Perform verification of the sensor firmware package as solicited by the <i>Verify Sensor Firmware Package</i> function. Verification of authenticity will be provided by the Security Services module.	Future
Manage Sensor Composition	Execute Action Verify HW Element Firmware Package	Perform verification of the hardware element firmware package as solicited by the <i>Verify Hardware Element Firmware Package</i> function. Verification of authenticity is provided by the Security Services module.	Future
Manage Sensor Composition	Execute Action Verify Run-time Environment Firmware Package	Perform verification of the RTE firmware package as solicited by the <i>Verify Run-time Environment Firmware Package</i> function. Verification of authenticity is provided by the Security Services module.	Future
Manage Sensor Composition	Provide Cryptographic Resources	Provide a list of cryptographic resources.	Future
Manage Sensor Composition	Execute Action Reserve Cryptographic Resource	Provide reservation of resources requested or deny request.	Future
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Monitor Sensor Security	Provide Sensor Component Security Status	Supply data that describes the security-relevant status of a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Status Parameter Settings	Supply data that describes the current parameter settings for the security status reporting functions for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Status Parameter Settings	Modify the parameter settings for the security status reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Notify Sensor Security Alerts	Supply data that indicates a security event for the sensor.	Future
Monitor Sensor Security	Notify Sensor Component Security Alerts	Supply data that indicates a security event for a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Alerts Parameter Settings	Supply data that describes the current parameter settings for security alerts for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Alerts Parameter Settings	Modify the parameter settings for security alerts for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Security Diagnostics	Provide Security Component Built-In Test Parameter Settings	Supply data that describes the current parameter settings for a BIT for a security component.	Future

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Manage Sensor Security Diagnostics	Execute Update Security Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a security component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Security Diagnostics	Execute Action Start Security Component Built-In Test	Initiate a BIT for a security component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor Security Diagnostics	Provide Security Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the security component.	Future
Manage Sensor Security Logging	Provide Sensor Security Log Data	Supply data that describes the past, current, and/or projected condition and well-being of the security of a sensor.	V1.0
Manage Sensor Security Logging	Provide Sensor Security Logging Parameter Settings	Supply data that describes the current parameter settings for sensor security logging for a sensor.	V1.0
Manage Sensor Security Logging	Execute Update Sensor Security Logging Parameter Settings	Modify the parameter settings for sensor security logging for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Security Logging	Provide Sensor Security Health Logging Parameter Settings	Supply data that describes the current parameter settings for sensor health logging for a sensor security function.	V1.0
Manage Sensor Security Logging	Execute Update Sensor Security Health Logging Parameter Settings	Modify the parameter settings for sensor security health logging function for a sensor as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Security Logging	Provide Sensor Security Logging Health	Solicit data that describes the health status for the sensor security logging function for a sensor.	V1.0
Manage Sensor Security Logging	Notify Sensor Security Logging Health Alerts	Supply data that indicates a change in health status for a sensor security logging function.	V1.0
Manage Sensor Security Logging	Provide Sensor Security Health Logging Health Alert Parameter Settings	Supply data that describes the current parameter settings for health alerts for the security health logging function of a sensor.	V1.0
Manage Sensor Security Logging	Execute Update Sensor Security Health Logging Health Alert Parameter Settings	Modify the parameter settings for health alerts for a sensor security health logger as solicited by the <i>Request Update</i> function.	V1.0

SOSA Functional Group 3	Security Services Module Function Name	Definition	Support
Manage Sensor Security Logging	Execute Action Delete Security Log Data	Delete the portion(s) of the sensor security log for a sensor as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Security Mode	Provide Sensor Security Component Mode	Supply data that describes the current mode for the sensor security component.	Future
Manage Sensor Security Mode	Notify Sensor Security Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor security component.	Future
Manage Sensor Security Mode	Execute Action Sensor Security Component Mode	Perform a mode transition on a sensor security component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor Security Parameterization	Provide Sensor Security Component Configuration	Provide a report of the sensor security component configuration upon request.	Future
Manage Sensor Security Parameterization	Notify Sensor Security Component Configuration Change	Send notifications of changes in the sensor security component configuration.	Future
Manage Sensor Security Parameterization	Verify Sensor Security Component Configuration	Determine whether the sensor security component configuration is acceptable based on current context/configuration mode. This determination could be specific to a particular sensor or mission. Common action is to indicate whether the configuration is verified by sending a notification and reporting status.	Future
Manage Sensor Security Parameterization	Execute Update Sensor Security Component Configuration	Send a request to update the configuration of a sensor security component.	Future
Manage Sensor Security Parameterization	Request Verification HW Element Software Package	Send a request to determine whether the current sensor software package is acceptable based on current context.	Future
Manage Sensor Security Parameterization	Execute Verification Software Package	Determine whether the software package for a sensor, a hardware element, or a RTE is acceptable based on current context. This determination could be specific to a particular sensor or mission. Common action is to indicate whether the software package is verified by sending a notification and reporting status.	Future

6.2.5.2 Security Services In-Band System Management Interactions

In-band system management interactions provided by the Security Services module (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.5.2-1.

Note that each interaction in Table 6.2.5.2-1 can be mapped back to a function in the in-band system management functions table (Table 6.2.5.1-1) for this interface. To make the table fit into the document format, the mapping to the Security Services Module Function Name was not included in the table. The information is tracked in the source material for these tables.

Table 6.2.5.2-1: Security Services Module In-Band System Management Interactions

Security Services Module Interaction Name	Interaction Type	Input Object	Output Object	Support
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateHealthParameters	Request Response	ComponentHealthParameters		Future
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0
getBitConfig	Request Response		BITConfig	Future
updateBitConfig	Request Response	BITConfig		Future
executeBIT	Request Response			V1.0
getBITResults	Request Response		BITResults	V1.0
getState	Request Response		ComponentState	V1.0

Security Services Module Interaction Name	Interaction Type	Input Object	Output Object	Support
notifyStateCallback	Event Notification	StateNotification		V1.0
restartSensorComponent	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0
getMode	Request Response		ComponentMode	V1.0
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0
verifySensorFirmware	Request Response	VerifyFirmwareRequest, ComponentId		Future
verifyFirmware	Request Response	VerifyFirmwareRequest		Future
getSecurityServicesConfig	Request Response		SecurityServicesConfig	V1.0

Security Services Module Interaction Name	Interaction Type	Input Object	Output Object	Support
notifySecurityServicesConfigCallback	Event Notification	SecurityServicesConfigNotification		V1.0
updateConfig	Request Response	SecurityServicesConfig		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getConfigCallbacks	Request Response		LIST Callback	V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0
deleteConfigCallback	Request Response	CallbackId		V1.0
getSecurityStatus	Request Response		SecurityStatus	Future
getSecurityStatusParameters	Request Response		SecurityStatusParameters	Future
updateSecurityStatusParameters	Request Response	SecurityStatusParameters		Future
notifySecurityCallback	Event Notification	SecurityNotification		Future
getSecurityCallbacks	Request Response		LIST Callback	Future
createSecurityCallback	Request Response	Callback	Callback	Future
deleteSecurityCallback	Request Response	CallbackId		Future
getLoggerData	Request Response		FILTEREDLIST LogEvent	V1.0
getLoggerConfiguration	Request Response		LoggerConfiguration	V1.0
updateLoggerConfiguration	Request Response	LoggerConfiguration	LoggerConfiguration	V1.0
getLoggerHealthParameters	Request Response		ComponentHealthParameters	V1.0

Security Services Module Interaction Name	Interaction Type	Input Object	Output Object	Support
updateLoggerHealthParameters	Request Response	ComponentHealthParameters		V1.0
getLoggerHealth	Request Response		ComponentHealth	V1.0
getLoggerFaults	Request Response		LIST Fault	V1.0
notifyLoggerHealthCallback	Event Notification	HealthNotification		V1.0
getLoggerHealthCallbacks	Request Response		LIST Callback	V1.0
createLoggerHealthCallback	Request Response		Callback	V1.0
deleteLoggerHealthCallback	Request Response	CallbackId		V1.0
deleteLoggerData	Request Response	DeleteLogEventRequest		V1.0

6.2.5.3 Security Services In-Band System Management Interface Rules

Rule 6.2.5.3-1: In the General Profile, the SOSA Security Services module shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.5.3-2: In the General Profile, the SOSA Security Services module shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T)

6.2.6 SOSA Chassis Manager In-Band System Management Definitions

This section defines the interactions provided by the Chassis Manager hardware element, which allows the chassis hardware to be managed by the System Manager.

6.2.6.1 SOSA Chassis Manager In-Band System Management Functions

Table 6.2.6.1-1 provides the detailed list of in-band system management functions to be provided by the Chassis Manager.

Note that the contents of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.6.1-1: Chassis Manager In-Band System Management Functions

SOSA Functional Group 3	Chassis Manager Module Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Parameter Settings	Solicit data that describes the current parameter settings for a BIT for a sensor component.	Future
Manage Sensor Diagnostics	Execute Update Sensor Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Action Start Sensor Component Built-In Test	Initiate a BIT for a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0

SOSA Functional Group 3	Chassis Manager Module Function Name	Definition	Support
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Execute Action low-level Command	Act upon a request for the Chassis Manager to execute a low-level command and return the result. Low-level commands and their responses follow the IPMI messaging standard implemented by the out-of-band hardware management interactions. This interaction allows interaction with the out-of-band hardware management interface from the in-band system management interface of the Chassis Manager. Access to this functionality could be restricted to specific conditions.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0

SOSA Functional Group 3	Chassis Manager Module Function Name	Definition	Support
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Inventory	Provide Sensor Component Inventory Information	Supply data that identifies the aggregate list current procurable entities contained within a sensor component.	Future
Manage Sensor Composition	Provide Field Replaceable Unit Info	Supply a description of a particular Field Replaceable Unit (FRU).	Future
Manage Sensor Composition	Provide Sensor Component Firmware Package Info	Supply data that identifies the firmware package running on the component.	V1.0
Manage Sensor Composition	Execute Update HW Element Firmware Package	Perform a replacement of one or more firmware and/or software elements on the sensor as solicited by the <i>Request Update Hardware Element Firmware Package</i> function.	V1.0
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0

SOSA Functional Group 3	Chassis Manager Module Function Name	Definition	Support
Monitor Sensor Security	Provide Sensor Component Security Status	Supply data that describes the security-relevant status of a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Status Parameter Settings	Supply data that describes the current parameter settings for the security status reporting functions for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Status Parameter Settings	Modify the parameter settings for the security status reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Notify Sensor Component Security Alerts	Supply data that indicates a security event for a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Alerts Parameter Settings	Supply data that describes the current parameter settings for security alerts for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Alerts Parameter Settings	Modify the parameter settings for security alerts for a sensor component as solicited by the <i>Request Update</i> function.	Future

6.2.6.2 SOSA Chassis Manager In-Band System Management Interactions

In-band system management interactions provided by the Chassis Manager hardware element (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.6.2-1.

Table 6.2.6.2-1: Chassis Manager In-Band System Management Interactions

Chassis Manager Interaction Name	Interaction Type	Input Object	Output Object	Support
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateHealthParameters	Request Response	ComponentHealthParameters		Future

Chassis Manager Interaction Name	Interaction Type	Input Object	Output Object	Support
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0
getBitConfig	Request Response		BITConfig	Future
updateBitConfig	Request Response	BITConfig		Future
executeBIT	Request Response			V1.0
getBITResults	Request Response		BITResults	V1.0
getState	Request Response		ComponentState	V1.0
notifyStateCallback	Event Notification	StateNotification		V1.0
restartSensorComponent	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0
executeCommand	Request Response	LowLevelCommand	LowLevelResult	V1.0
getMode	Request Response		ComponentMode	V1.0

Chassis Manager Interaction Name	Interaction Type	Input Object	Output Object	Support
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0
getChassisManagerInventory	Request Response		ChassisManagerInventory	Future
getFRU	Request Response	FruId	FieldReplaceableUnit	Future
getFirmwareInfo	Request Response		FirmwarePackageInfo	V1.0
updateFirmware	Request Response	FirmwarePackage		V1.0
getChassisManagerConfig	Request Response		ChassisManagerConfig	V1.0
notifyChassisManagerConfigCallback	Event Notification	ChassisManagerConfigNotification		V1.0
updateConfig	Request Response	ChassisManagerConfig		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getConfigCallbacks	Request Response		LIST Callback	V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0

Chassis Manager Interaction Name	Interaction Type	Input Object	Output Object	Support
deleteConfigCallback	Request Response	CallbackId		V1.0
getSecurityStatus	Request Response		SecurityStatus	Future
getSecurityStatusParameters	Request Response		SecurityStatusParameters	Future
updateSecurityStatusParameters	Request Response	SecurityStatusParameters		Future
notifySecurityCallback	Event Notification	SecurityNotification		Future
getSecurityCallbacks	Request Response		LIST Callback	Future
createSecurityCallback	Request Response	Callback	Callback	Future
deleteSecurityCallback	Request Response	CallbackId		Future

6.2.6.3 SOSA Chassis Manager In-Band System Management Interface Rules

Rule 6.2.6.3-1: In the General Profile, the Chassis Manager hardware element shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance approach (D)

Rule 6.2.6.3-2: In the General Profile, the Chassis Manager hardware element shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance approach (T)

6.2.7 SOSA PIC In-Band System Management Definitions

This section defines the in-band system management interactions for a SOSA PIC. This interface allows a set of PICs to be managed by the System Manager.

Not all PICs will implement the in-band system management interface, and those that do could not implement it on the PIC itself. Some could require the functions to be implemented on a separate PIC.

6.2.7.1 SOSA Plug-In Card In-Band System Management Functions

Table 6.2.7.1-1 provides the detailed list of in-band system management functions to be provided by SOSA PICs with in-band system management requirements.

The contents of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.7.1-1: SOSA Plug-In Card In-Band System Management Functions

SOSA Functional Group 3	Plug-In Card Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Parameter Settings	Solicit data that describes the current parameter settings for a BIT for a sensor component.	Future
Manage Sensor Diagnostics	Execute Update Sensor Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Action Start Sensor Component Built-In Test	Initiate a BIT for a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0

SOSA Functional Group 3	Plug-In Card Function Name	Definition	Support
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Execute Update Application State	Receive a request to modify an application's state. State update requests include; load, unload, start, stop, pause, resume, reset. Provide an application ID when the infrastructure component loads the application.	V1.0
Manage Sensor State	Provide Sensor Application Health	Provide a report of the current health (status, faults) of a sensor application.	Future
Manage Sensor State	Provide Application State	Provide a report of the current state of an application.	V1.0
Manage Sensor State	Provide Application Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor.	V1.0
Manage Sensor State	Execute Update Application Health Alerts Parameter Settings	Modify the parameter settings for health alerts for an application solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Notify Application State Change	Send notifications of changes in the state of an application running on an RTE or hardware element.	V1.0
Manage Sensor State	Notify Application Event	Send notifications of events (such as faults) in an application running on an RTE or hardware element.	Future
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0

SOSA Functional Group 3	Plug-In Card Function Name	Definition	Support
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Inventory	Provide Sensor Component Inventory Information	Supply data that identifies the aggregate list current procurable entities contained within a sensor component.	Future
Manage Sensor Composition	Provide Field Replaceable Unit Info	Supply a description of a particular FRU.	Future
Manage Sensor Composition	Provide Sensor Component Firmware Package Info	Supply data that identifies the firmware package running on the component.	V1.0
Manage Sensor Composition	Execute Update HW Element Firmware Package	Perform a replacement of one or more firmware and/or software elements on the sensor as solicited by the <i>Request Update Hardware Element Firmware Package</i> function.	V1.0
Manage Sensor Composition	Provide Resources	Provide a list of resources on a hardware element, module, or RTE, including current reservation status.	Future
Manage Sensor Composition	Execute Action Reserve Resource	Provide reservation of resources requested or deny request.	Future
Manage Sensor Composition	Execute Action Release Resource Reservation	Release reservation made earlier.	Future

SOSA Functional Group 3	Plug-In Card Function Name	Definition	Support
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Monitor Sensor Security	Provide Sensor Component Security Status	Supply data that describes the security-relevant status of a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Status Parameter Settings	Supply data that describes the current parameter settings for the security status reporting functions for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Status Parameter Settings	Modify the parameter settings for the security status reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Notify Sensor Component Security Alerts	Supply data that indicates a security event for a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Alerts Parameter Settings	Supply data that describes the current parameter settings for security alerts for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Alerts Parameter Settings	Modify the parameter settings for security alerts for a sensor component as solicited by the <i>Request Update</i> function.	Future

6.2.7.2 SOSA Plug-In Card In-Band System Management Interactions

In-band system management interactions provided by the PICs that implement in-band system management interfaces (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.7.2-1.

Table 6.2.7.2-1: SOSA Plug-In Card In-Band System Management Interactions

Plug-In Card Interaction Name	Interaction Type	Input Object	Output Object	Support
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateHealthParameters	Request Response	ComponentHealthParameters		Future
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0
getBitConfig	Request Response		BITConfig	Future
updateBitConfig	Request Response	BITConfig		Future
executeBIT	Request Response			V1.0
getBITResults	Request Response		BITResults	V1.0
getState	Request Response		ComponentState	V1.0
notifyStateCallback	Event Notification	StateNotification		V1.0

Plug-In Card Interaction Name	Interaction Type	Input Object	Output Object	Support
restartSensorComponent	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0
loadApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
unloadApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
startApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
stopApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
pauseApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
resumeApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
resetApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
getApplicationState	Request Response	ApplicationId	ApplicationState	V1.0
getApplicationEventCallbacks	Request Response		LIST Callback	V1.0
createApplicationEventCallback	Request Response	Callback	Callback	V1.0
deleteApplicationEventCallback	Request Response	CallbackId		V1.0
notifyApplicationEventCallback	Event Notification	ApplicationEvent		V1.0

Plug-In Card Interaction Name	Interaction Type	Input Object	Output Object	Support
getMode	Request Response		ComponentMode	V1.0
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0
getPluginCardInventory	Request Response		PluginCardInventory	Future
getFRU	Request Response	FruId	FieldReplaceableUnit	Future
getFirmwareInfo	Request Response		FirmwarePackageInfo	V1.0
updateFirmware	Request Response	FirmwarePackage		V1.0
getResources	Request Response		HardwareResources	Future
reserveResources	Request Response	ResourceReservationRequest	ResourceReservation	Future
releaseResources	Request Response	ReservationId		Future
getPluginCardConfig	Request Response		PluginCardConfig	V1.0
notifyPluginCardConfigCallback	Event Notification	PluginCardConfigNotification		V1.0

Plug-In Card Interaction Name	Interaction Type	Input Object	Output Object	Support
updateConfig	Request Response	PluginCardConfig		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getConfigCallbacks	Request Response		LIST Callback	V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0
deleteConfigCallback	Request Response	CallbackId		V1.0
getSecurityStatus	Request Response		SecurityStatus	Future
getSecurityStatusParameters	Request Response		SecurityStatusParameters	Future
updateSecurityStatusParameters	Request Response	SecurityStatusParameters		Future
notifySecurityCallback	Event Notification	SecurityNotification		Future
getSecurityCallbacks	Request Response		LIST Callback	Future
createSecurityCallback	Request Response	Callback	Callback	Future
deleteSecurityCallback	Request Response	CallbackId		Future

6.2.7.3 SOSA Plug-In Card In-Band System Management Interface Rules

Rule 6.2.7.3-1: SOSA PICs shall be either directly managed or indirectly managed. Conformance Methodology (D)

Observation 6.2.7.3-1: As described in Chapter 6, sensor components can be managed or unmanaged, and managed sensor components could be directly or indirectly managed.

Observation 6.2.7.3-2: A SOSA PIC could be indirectly managed by another interconnected PIC or by the Chassis Manager.

Rule 6.2.7.3-2: The current edition of the SOSA Technical Standard does not define rules for every kind of PIC stating requirements for it to being unmanaged, managed, directly managed, or indirectly managed. That could be specified in a system requirement.

Rule 6.2.7.3-3: Directly managed PICs shall implement a built-in in-band system management interface. Conformance Methodology (D)

Rule 6.2.7.3-4: Indirectly managed PICs shall be represented by an in-band system management interface. Conformance Methodology (D)

Rule 6.2.7.3-5: In the General Profile, PIC in-band system management interfaces shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.7.3-6: In the General Profile, the PIC in-band system management interfaces shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T)

6.2.8 SOSA Plug-In Card with Software RTE In-Band System Management Definitions

This section defines the in-band system management interactions to be implemented by PICs that host a SOSA software RTE. This interface allows the PIC and its software RTE to be managed by the System Manager.

A PIC that hosts one or more instances of the software RTE is called a SOSA Plug-In Card with Software Run-Time Environment (PIC with SW RTE).

6.2.8.1 SOSA PIC with SW RTE In-Band System Management Functions

Table 6.2.8.1-1 provides the detailed list of in-band system management functions to be provided by a PIC with SW RTE.

Note that the contents of the column marked “SOSA Functional Group 3” maps back to the same column in the System Management SvcV-4 defined in Table 6.1.1-1.

Table 6.2.8.1-1: SOSA PIC with SW RTE In-Band System Management Functions

SOSA Functional Group 3	Plug-In Card with SW RTE Function Name	Definition	Support
Monitor Sensor Health	Provide Sensor Component Health Information	Supply data that describes the current and/or projected condition and well-being of a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Parameter Settings	Supply data that describes the current parameter settings for the health monitoring and reporting functions for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Parameter Settings	Modify the parameter settings for the health monitoring and reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future

SOSA Functional Group 3	Plug-In Card with SW RTE Function Name	Definition	Support
Monitor Sensor Health	Notify Sensor Component Health Alerts	Supply data that indicates a change in health information for a sensor component.	V1.0
Monitor Sensor Health	Provide Sensor Component Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor component.	V1.0
Monitor Sensor Health	Execute Update Sensor Component Health Alerts Parameter Settings	Modify the parameter settings for health alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Parameter Settings	Solicit data that describes the current parameter settings for a BIT for a sensor component.	Future
Manage Sensor Diagnostics	Execute Update Sensor Component Built-In Test Parameter Settings	Modify the parameter settings for a BIT for a sensor component as solicited by the <i>Request Update</i> function.	Future
Manage Sensor Diagnostics	Execute Action Start Sensor Component Built-In Test	Initiate a BIT for a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Diagnostics	Provide Sensor Component Built-In Test Results	Supply data that describes the outcome of BIT execution on the sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State	Supply data that describes the current state for the sensor component.	V1.0
Manage Sensor State	Notify Sensor Component State Events	Supply data that indicates a change in state status, or state transition, for a sensor component.	V1.0
Manage Sensor State	Execute Update Sensor Component State	Perform a state transition on a sensor component as solicited by the <i>Request Action</i> function.	Future
Manage Sensor State	Execute Action Restart Sensor Component	Initiate a <i>Restart</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor State	Execute Action Shutdown Sensor Component	Receive and act upon a request to shut down a sensor component.	V1.0
Manage Sensor State	Provide Sensor Component State Alerts Parameter Settings	Supply data that describes the current parameter settings for state alerts for a sensor component.	V1.0

SOSA Functional Group 3	Plug-In Card with SW RTE Function Name	Definition	Support
Manage Sensor State	Execute Update Sensor Component State Alerts Parameter Settings	Modify the parameter settings for state alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Execute Update Application State	Receive a request to modify an application's state. State update requests include; load, unload, start, stop, pause, resume, reset. Provide an application ID when the infrastructure component loads the application.	V1.0
Manage Sensor State	Provide Sensor Application Health	Provide a report of the current health (status, faults) of a sensor application.	Future
Manage Sensor State	Provide Application State	Provide a report of the current state of an application.	V1.0
Manage Sensor State	Provide Application Health Alerts Parameter Settings	Supply data that describes the current parameter settings for health alerts for a sensor.	V1.0
Manage Sensor State	Execute Update Application Health Alerts Parameter Settings	Modify the parameter settings for health alerts for an application solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor State	Notify Application State Change	Send notifications of changes in the state of an application running on an RTE or hardware element.	V1.0
Manage Sensor State	Notify Application Event	Send notifications of events (such as faults) in an application running on an RTE or hardware element.	Future
Manage Sensor Mode	Provide Sensor Component Mode	Supply data that describes the current mode for the sensor component.	V1.0
Manage Sensor Mode	Notify Sensor Component Mode Events	Supply data that indicates a change in mode status, or mode transition, for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode	Perform a mode transition on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Zeroize Sensor Component	Initiate a <i>Zeroize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0
Manage Sensor Mode	Execute Action Sanitize Sensor Component	Initiate a <i>Sanitize</i> function on a sensor component as solicited by the <i>Request Action</i> function.	V1.0

SOSA Functional Group 3	Plug-In Card with SW RTE Function Name	Definition	Support
Manage Sensor Mode	Provide Sensor Component Mode Alerts Parameter Settings	Supply data that describes the current parameter settings for mode alerts for a sensor component.	V1.0
Manage Sensor Mode	Execute Update Sensor Component Mode Alerts Parameter Settings	Modify the parameter settings for mode alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Manage Sensor Inventory	Provide Sensor Component Inventory Information	Supply data that identifies the aggregate list current procurable entities contained within a sensor component.	Future
Manage Sensor Composition	Provide Field Replaceable Unit Info	Supply a description of a particular FRU.	Future
Manage Sensor Composition	Provide Sensor Component Firmware Package Info	Supply data that identifies the firmware package running on the component.	V1.0
Manage Sensor Composition	Execute Update HW Element Firmware Package	Perform a replacement of one or more firmware and/or software elements on the sensor as solicited by the <i>Request Update Hardware Element Firmware Package</i> function.	V1.0
Manage Sensor Composition	Execute Update Run-time Environment Application Firmware Package	Perform a replacement of one or more firmware and/or software elements on the sensor as solicited by the <i>Request Update Run-time Environment Application Firmware Package</i> function.	Future
Manage Sensor Composition	Provide Resources	Provide list of resources on a hardware element, module, or RTE, including current reservation status.	Future
Manage Sensor Composition	Execute Action Reserve Resource	Provide reservation of resources requested or deny request.	Future
Manage Sensor Composition	Execute Action Release Resource Reservation	Release reservation made earlier.	Future
Manage Sensor Composition	Reserve Run-time Resources		Future
Manage Sensor Composition	Release Run-time Resources		Future
Manage Sensor Parameterization	Provide Sensor Component Configuration	Supply data that identifies the aggregate list of user-modifiable settings and their values for the sensor component.	V1.0

SOSA Functional Group 3	Plug-In Card with SW RTE Function Name	Definition	Support
Manage Sensor Parameterization	Notify Sensor Component Configuration Modification	Supply data that indicates an alteration in one or more values of a user-modifiable setting for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Configuration	Perform an alteration to one or more user-modifiable setting values for the sensor component as solicited by the <i>Request Update Sensor Component Configuration</i> function.	Future
Manage Sensor Parameterization	Execute Action Verify Sensor Component Configuration	Initiate determination of whether a sensor component configuration is authentic/trustable.	Future
Manage Sensor Parameterization	Provide Sensor Component Config Alerts Parameter Settings	Supply data that describes the current parameter settings for config alerts for a sensor component.	V1.0
Manage Sensor Parameterization	Execute Update Sensor Component Config Alerts Parameter Settings	Modify the parameter settings for config alerts for a sensor component as solicited by the <i>Request Update</i> function.	V1.0
Monitor Sensor Security	Provide Sensor Component Security Status	Supply data that describes the security-relevant status of a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Status Parameter Settings	Supply data that describes the current parameter settings for the security status reporting functions for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Status Parameter Settings	Modify the parameter settings for the security status reporting functions for a sensor component as solicited by the <i>Request Update</i> function.	Future
Monitor Sensor Security	Notify Sensor Component Security Alerts	Supply data that indicates a security event for a sensor component.	Future
Monitor Sensor Security	Provide Sensor Component Security Alerts Parameter Settings	Supply data that describes the current parameter settings for security alerts for a sensor component.	Future
Monitor Sensor Security	Execute Update Sensor Component Security Alerts Parameter Settings	Modify the parameter settings for security alerts for a sensor component as solicited by the <i>Request Update</i> function.	Future

6.2.8.2 SOSA PIC with SW RTE In-Band System Management Interactions

In-band system management interactions provided by the PIC with SW RTE (meaning that this sensor component implements the service side of request-response and publish-subscribe interactions and initiates event notification interactions) are listed in Table 6.2.8.2-1.

Table 6.2.8.2-1: PIC with SW RTE In-Band System Management Interactions

Plug-In Card with SW RTE Interaction Name	Interaction Type	Input Object	Output Object	Support
getHealth	Request Response		ComponentHealth	V1.0
getFaults	Request Response		LIST Fault	V1.0
getHealthParameters	Request Response		ComponentHealthParameters	V1.0
updateHealthParameters	Request Response	ComponentHealthParameters		Future
notifyHealthCallback	Event Notification	HealthNotification		V1.0
getHealthCallbacks	Request Response		LIST Callback	V1.0
createHealthCallback	Request Response	Callback	Callback	V1.0
deleteHealthCallback	Request Response	CallbackId		V1.0
getBitConfig	Request Response		BITConfig	Future
updateBitConfig	Request Response	BITConfig		Future
executeBIT	Request Response			V1.0
getBITResults	Request Response		BITResults	V1.0
getState	Request Response		ComponentState	V1.0
notifyStateCallback	Event Notification	StateNotification		V1.0

Plug-In Card with SW RTE Interaction Name	Interaction Type	Input Object	Output Object	Support
restartSensorComponent	Request Response			V1.0
shutdownSensorComponent	Request Response			V1.0
getStateCallbacks	Request Response		LIST Callback	V1.0
createStateCallback	Request Response	Callback	Callback	V1.0
deleteStateCallback	Request Response	CallbackId		V1.0
loadApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
unloadApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
startApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
stopApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
pauseApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
resumeApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
resetApplication	Request Response	ApplicationStateRequest	ApplicationState	V1.0
getApplicationState	Request Response	ApplicationId	ApplicationState	V1.0
getApplicationEventCallbacks	Request Response		LIST Callback	V1.0
createApplicationEventCallback	Request Response	Callback	Callback	V1.0
deleteApplicationEventCallback	Request Response	CallbackId		V1.0
notifyApplicationEventCallback	Event Notification	ApplicationEvent		V1.0

Plug-In Card with SW RTE Interaction Name	Interaction Type	Input Object	Output Object	Support
getMode	Request Response		ComponentMode	V1.0
notifyModeCallback	Event Notification	ModeNotification		V1.0
updateMode	Request Response	ComponentMode		V1.0
zeroize	Request Response	ZeroizeConfig		V1.0
sanitize	Request Response	SanitizeConfig		V1.0
getModeCallbacks	Request Response		LIST Callback	V1.0
createModeCallback	Request Response	Callback	Callback	V1.0
deleteModeCallback	Request Response	CallbackId		V1.0
getPluginCardSWRTEInventory	Request Response		PluginCardSWRTEInventory	Future
getFRU	Request Response	FruId	FieldReplaceableUnit	Future
getFirmwareInfo	Request Response		FirmwarePackageInfo	V1.0
updateFirmware	Request Response	FirmwarePackage		V1.0
getResources	Request Response		HardwareResources	Future
reserveResources	Request Response	ResourceReservationRequest	ResourceReservation	Future
releaseResources	Request Response	ReservationId		Future
getPluginCardSWRTEConfig	Request Response		PluginCardSWRTEConfig	V1.0
notifyPluginCardSWRTEConfigCallback	Event Notification	PluginCardSWRTEConfigNotification		V1.0

Plug-In Card with SW RTE Interaction Name	Interaction Type	Input Object	Output Object	Support
updateConfig	Request Response	PluginCardSWRTEConfig		Future
verifyConfig	Request Response	VerifyConfigRequest		Future
getConfigCallbacks	Request Response		LIST Callback	V1.0
createConfigCallback	Request Response	Callback	Callback	V1.0
deleteConfigCallback	Request Response	CallbackId		V1.0
getSecurityStatus	Request Response		SecurityStatus	Future
getSecurityStatusParameters	Request Response		SecurityStatusParameters	Future
updateSecurityStatusParameters	Request Response	SecurityStatusParameters		Future
notifySecurityCallback	Event Notification	SecurityNotification		Future
getSecurityCallbacks	Request Response		LIST Callback	Future
createSecurityCallback	Request Response	Callback	Callback	Future
deleteSecurityCallback	Request Response	CallbackId		Future

6.2.8.3 PIC with SW RTE In-Band System Management Interface Rules

Rule 6.2.8.3-1: In the General Profile, the PIC with SW RTE hardware element shall implement in-band system management interactions that conform to the rules defined in Section 6.2.1. Conformance Methodology (D)

Rule 6.2.8.3-2: In the General Profile, the PIC with SW RTE hardware element shall implement in-band system management interactions specifically as defined by the OpenAPI Specification in Section B.3. Conformance Methodology (T)

6.3 Out-of-Band Hardware Management Overview

SOSA out-of-band hardware management provides the capability to diagnose and debug hardware assemblies while the system infrastructure (processing and transports) could not be operational. This is accomplished via a set of existing lower-level hardware management interface standards. More detail on the out-of-band hardware system management functionality is described below.

SOSA out-of-band hardware management interfaces provide a well-defined set of standardized hardware-centric capabilities across SOSA hardware elements that can be relied upon and utilized by the SOSA System Manager module via a standardized set of logical and physical interfaces to fully satisfy the required SOSA system management functionality. SOSA out-of-band hardware management leverages and builds upon ANSI/VITA 46.11.

Capabilities provided by SOSA hardware management architecture include but are not limited to the following:

- **Hardware Element Sensor Management** – e.g., temperature, voltage, current, vibration, intrusion
- **Hardware Chassis/Element Inventory** – e.g., vendor identification, model number, serial number, revision identification, software/firmware revision information
- **Hardware Chassis/Element Configuration** – e.g., parameter settings, policy settings
- **FRU Recovery** – e.g., reset a hardware element, power cycle a hardware element
- **Diagnostic Management** – e.g., initiate diagnostics, collect diagnostic results

The ANSI/VITA 46.11 standard provides a large array of commands and parameters, a subset of which are used to support the SOSA hardware management architecture.

As shown in Figure 6.3-1, the SOSA Architecture defines two logical interfaces through which SOSA modules can interact with SOSA hardware elements. The interaction is enabled via SOSA defined chassis management and system management interfaces that provide access to the status and control capability of the underlying hardware element management features.

The in-band chassis management interface (labeled CMI in Figure 6.3-1) provides access to the ANSI/VITA 46.11 Chassis Manager software capabilities. This interface provides a path to access the entirety of the out-of-band hardware management platform via a single logical element, the Chassis Manager. In this scenario, the Chassis Manager utilizes an out-of-band interface, the Intelligent Platform Management Bus (IPMB), to extend status and control capabilities of its chassis management interface to all the managed hardware elements. This can be helpful when performing activities such as discovery of the SOSA hardware element as the summary of this information is collected and stored by the Chassis Manager and can thus be retrieved from a single location in the chassis.

The in-band system management interfaces (labeled SMI in Figure 6.3-1) provide a local interface from an application processor on a hardware element, when applicable, to its Intelligent Platform Management Controller (IPMC) via a payload interface. This path can be helpful for fault management, performance, and/or security-related reasons *versus* communicating over the shared IPMB interface via the Chassis Manager.

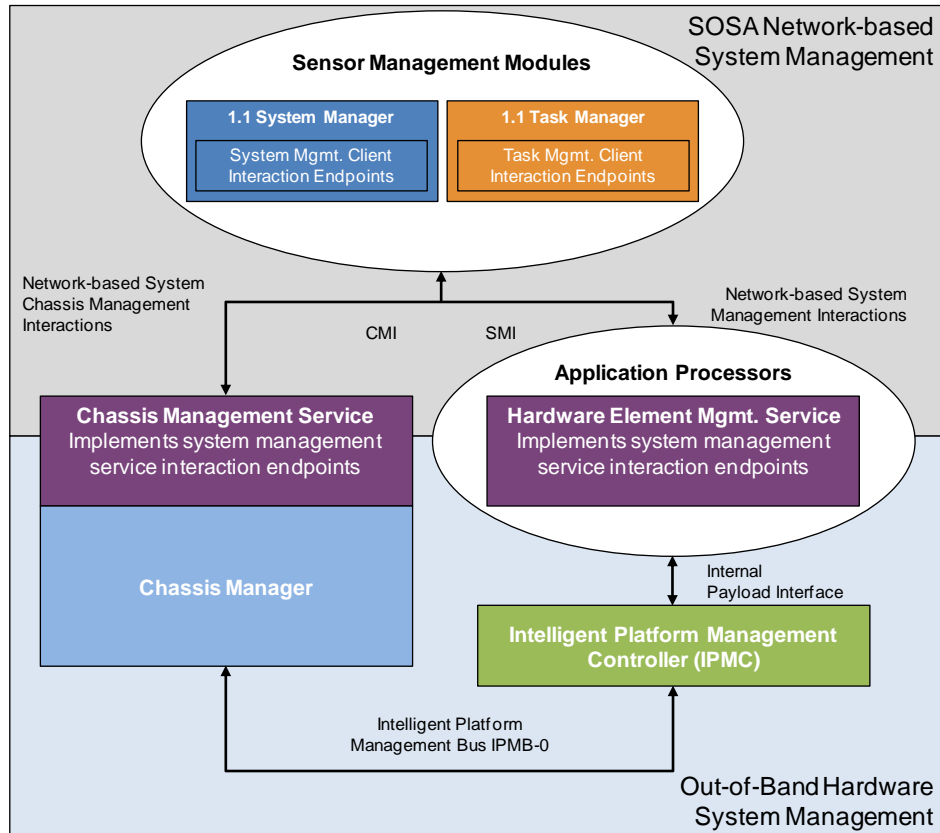


Figure 6.3-1: SOSA Hardware System Management Logical Block Diagram

Physically, hardware management is implemented in a hierarchical manner where each managed FRU contains an IPMC, each managed chassis implements functionality of the Chassis Manager, and each managed platform contains one or more System Managers (e.g., the SOSA System Manager and the SOSA Task Manager). Each layer of the hierarchy enables a greater set of management capabilities. Note that it is not necessary that the functionality associated with the Chassis Manager in Figure 6.3-2 be implemented as a stand-alone entity if the chassis management interface and chassis management functions are implemented and have access to the IPMB interface.

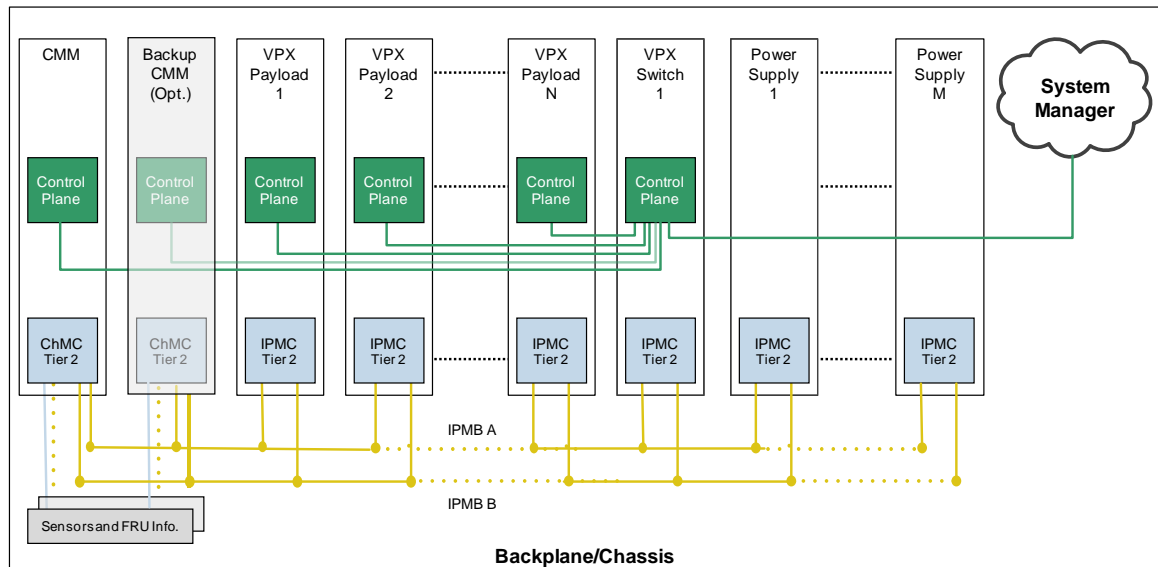


Figure 6.3-2: Example SOSA System Management Backplane/Chassis Implementation

As shown in Figure 6.3-2, each SOSA payload and switch hardware element contains an ANSI/VITA 46.11-compliant IPMC. Each hardware element provides redundant IPMB connections from the IPMC to the backplane. Power Supply Cards (PSCs) also contain an ANSI/VITA 46.11-compliant IPMC which provides redundant IPMB connections to the backplane. A Chassis Management Module (CMM) which hosts an ANSI/VITA 46.11 Chassis Manager function also provides redundant IPMB connections and a 1GbE Control Plane connection for the chassis management interface. The IPMB connections are bussed or radially routed across the backplane such that IPMB-A and IPMB-B connect to each IPMC/Chassis Management Controller (ChMC) on each hardware element. The Chassis Manager Control Plane interface is connected to the Control Plane switch network. The Chassis Manager Inter-IC (I^2C) busses are connected to chassis sensors and FRU information devices. A System Manager is connected to the Control Plane switch network.

In a SOSA system, a CMM is typically a discrete entity that is “part of the chassis” and exists on a non-specified form factor. This allows chassis FRU information, logs, etc. to stay with the chassis independent of changes to its content.

It is possible to support redundant Chassis Managers within an enclosure to achieve increased Reliability, Availability, and Serviceability (RAS) support. The Chassis Manager acts as an access point for the System Manager into the IPMC capabilities. The Chassis Manager additionally provides interfaces to chassis-level sensors, FRU information, power, and/or thermal management infrastructure. All FRUs in the system are identifiable via the system management infrastructure.

Figure 6.3-3 shows an example SOSA hardware management implementation on a SOSA hardware element. As shown in Figure 6.3-3, the IPMC exists in the Management Power Domain on the SOSA hardware element that allows it to operate in a “lights out” condition when only management power is applied to the PIC, backplane, and/or chassis. The remainder of the electronics on the hardware element, including the application processor which could be a general-purpose processor, a Field-Programmable Gate Array (FPGA), a Graphics Processing Unit (GPU), or any other processing engine that runs the payload application, exists on the Payload Power Domain. System management communication can occur to/from the application

processor over the Control Plane (system management interface) or via the payload interface of its IPMC (out-of-band), and system management communication can also occur over the System IPMB to/from the IPMC independent of the application processor.

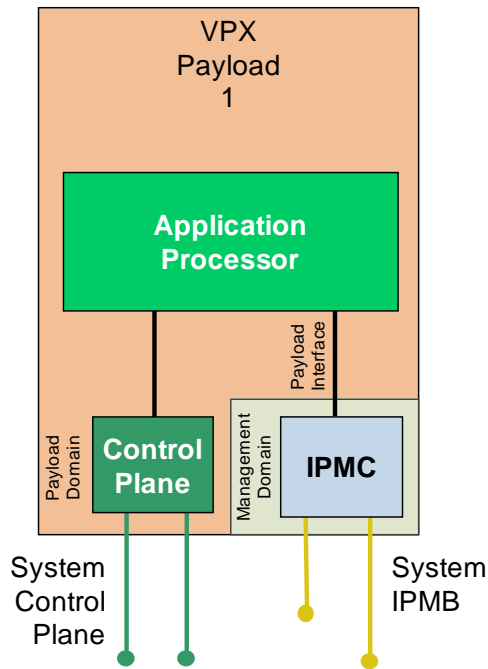


Figure 6.3-3: Example SOSA System Management Plug-In Card Implementation

In a SOSA system, communication to/from the IPMC over the system IPMB provides a set of system management capabilities that are accessible in a “lights out” condition when only management power is enabled and/or when there are soft and/or hard faults preventing communication with the application processor. As such, this system IPMB enables fault isolation and recovery operations, hardware configuration, sensor management, and inventory functions that are available out-of-band of the application and when limited power is available to the platform (e.g., during 2 Level Maintenance (2LM) operations and/or in theater).

Once the payload domain is activated, system management applications running on the application processor and communicating over the Control Plane can be used to increase the performance of the run-time system management functions. The application processor can locally communicate with the IPMC over its payload interface to access its capabilities and communicate with the Chassis Manager, System Manager, and/or other application processors. This enables the installation and usage of standards-based system management applications.

6.4 Out-of-Band Hardware Management Definitions

Rule 6.4-1: A SOSA hardware element’s IPMC shall be powered by the 3.3V_AUX power rail.

Permission 6.4-1: A SOSA CMM may derive its Management Power Domain independently of 3.3V_AUX so long as it powers up before or concurrently with the 3.3V_AUX power rail.

Rule 6.4-2: A SOSA CMM that does not follow Permission 6.4-1 shall be powered by the 3.3V_AUX power rail.

Rule 6.4-3: A SOSA backplane shall implement a system IPMB interface as described in ANSI/VITA 46.11 §9. Conformance Methodology (D)

Rule 6.4-4: Backplanes shall implement a single, 2.49K Ohm, +/- 1%, pull-up resistor from each IPMB signal to the 3.3V_AUX rail. Conformance Methodology (A)

Rule 6.4-5: A SOSA backplane shall include the redundant system IPMB channel (IPMB-B) as described in ANSI/VITA 46.11 §9. Conformance Methodology (D)

Observation 6.4-1: Rules 6.4-6 and 6.4-9 below comprise a subset of capabilities included in Rule 6.4-10 and are explicitly called out here to provide a progression of capabilities for phased conformance.

Rule 6.4-6: A SOSA hardware element's IPMC or ChMC shall implement all commands listed as mandatory in ANSI/VITA 46.11 Table 10.1.1-1 and Table 10.1.2-1 for an "IPMC Tier-2" to provide a successful response as defined by the relevant section of the referenced standard.

Rule 6.4-7: A SOSA hardware element's IPMC or ChMC that conforms to Rule 6.4-6 shall meet all the requirements for a "Tier-2" IPMC or ChMC as described by ANSI/VITA 46.11. Conformance Methodology (D)

Rule 6.4-8: A SOSA hardware element's IPMC or ChMC shall implement all commands listed as mandatory in HOST Tier-2 v3.0 Table 5-16 to provide a successful response as defined by the relevant section of the referenced standard. Conformance Methodology (D)

Rule 6.4-9: A SOSA hardware element's IPMC or ChMC shall implement all commands listed as mandatory in ANSI/VITA 46.11 Table 10.1.1-1 and Table 10.1.2-1 for an "IPMC Tier-3" to provide a successful response as defined by the relevant section of the referenced standard. Conformance Methodology (D)

Rule 6.4-10: A SOSA hardware element's IPMC or ChMC that conforms to Rule 6.4-9 shall meet all the requirements for a "Tier-3" IPMC or ChMC as described by ANSI/VITA 46.11. Conformance Methodology (D)

Rule 6.4-11: A SOSA hardware element's IPMC or ChMC shall implement the optional firmware firewall commands listed in the IPMI Specification, Second Generation, Version 2.0, Table 21-1. Conformance Methodology (D)

Rule 6.4-12: A SOSA PIC that includes a VITA 46.11 Payload Mode sensor shall populate the "Discrete Reading Mask" in the sensor data record for its Payload Mode sensor with 0x007F.

Rule 6.4-13: A SOSA PIC that includes a VITA 46.11 Payload Mode sensor shall indicate its current operational state(s) as defined in Section 6.2 of this document by asserting the corresponding "event/state" bit (0-6) in its IPMC's Payload Mode Sensor.

Rule 6.4-14: A SOSA PIC that includes a VITA 46.11 Payload Mode sensor shall respond to the "Get Payload Mode Capabilities" request with 0x001E in the "supported modes" field.

Observation 6.4-2: The VITA 46.11 FRU State Sensor (M0-M7) independently provides information about the IPMC and Payload Activation (power state) of the card, while the VITA 46.11 Payload Mode sensor provides additional information about the operational state of the functionality that can be activated/deactivated through the IPMC. For the SOSA Technical Standard, the two sensors "overlap" at M1/P0 and M6/P4. The M1 state (stand-by) in the FRU State sensor indicates that the IPMC is ready but has not enabled power to the payload functions.

This corresponds to state P0 (Off) in the Payload Mode sensor. Once conditions in the IPMC are met to activate the payload, power is applied and the FRU State Sensor transitions to state M4 (active). At this point the Payload Mode sensor will typically transition to state P1 (starting) and then move to subsequent states, as described in Section 6.2. Then, when the IPMC receives a deactivation request (or local conditions are met) the FRU State sensor will transition to state M6 (shutdown). This should trigger the payload to enter state P4 (stopping). The IPMC then waits for the Payload Mode to transition to state P0 (ready to power down) or provide a timeout delay before the IPMC disables power and transitions to back to state M1 (stand-by).

Rule 6.4-15: A SOSA PIC that includes a VITA 46.11 Payload Mode sensor and detects a fault condition that prevents the PIC from performing its intended role shall assert state bit #5 in the Payload Mode sensor simultaneously with the current operational state, except when the P0 state is asserted, in which case bit #5 shall be de-asserted.

Observation 6.4-3: By continuing to assert both the operating state and simultaneously asserting state P5, the out-of-band channel maintains visibility to both the state in which the PIC is attempting to operate and the fault condition.

Observation 6.4-4: The M7 state in the VITA 46.11 FRU State sensor, as described in ANSI/VITA 46.11, indicates “loss of com” for the out-of-band channel between the Chassis Manager and an IPMC, or between the IPMC and one of its intelligent subsidiary FRUs. The state P6 in a SOSA implementation of the Payload Mode sensor indicates “loss of com” for the in-band system management interface between the SOSA module that is running on the PIC and the SOSA System Manager.

Rule 6.4-16: A SOSA PIC that includes a VITA 46.11 Payload Mode Sensor and detects loss-of-communication via the in-band System Management Interface **shall** assert state bit #6 in the Payload Mode Sensor simultaneously with the current operational state except when the P0 state is asserted, in which case bit #6 shall be de-asserted.

Observation 6.4-5: By continuing to assert the current operating mode and simultaneously asserting state P6, the out-of-band channel maintains visibility to both the current operating state and the “loss of com” indication for the in-band channel.

Recommendation 6.4-1: When a SOSA hardware element can host one or more SOSA modules, its IPMC should include a payload interface as defined in ANSI/VITA 46.11 §4.1.3. Conformance Methodology (I)

Permission 6.4-2: A SOSA hardware element’s IPMC or ChMC may include additional IPMI-aware interfaces that do not include LUN 10b message routing. Conformance Methodology (I)

Observation 6.4-6: The payload interface described in ANSI/VITA 46.11 §4.1.3 supports LUN 10b message routing. Only one interface into the payload can support this feature. This is the preferred implementation for an IPMI-aware interface from the IPMC or ChMC to software running in the payload. Additional IPMI-aware interfaces between an IPMC or ChMC and various payload elements can also support message bridging, but they must support only “tracked” message routing to avoid contention with the payload interface.

Rule 6.4-17: When SOSA hardware element’s IPMC or ChMC follows Recommendation 6.4-1 (above) the hardware element’s IPMC or ChMC shall implement the bridge firewall commands listed in Table 10.1.2-1 in ANSI/VITA 46.11-2022. Conformance Methodology (D)

Observation 6.4-7: Some SOSA PICs could contain processors, complex FPGA, XMC modules, etc. which could host IPMI-aware payload entities that can be represented on the system IPMB as subsidiary FRUs by the IPMC.

Observation 6.4-8: The IPMB and IPMI specifications define interface protocols for various physical interfaces including I²C, serial, and Ethernet to carry IPMB formatted IPMI messages.

6.4.1 Chassis Manager Out-of-Band System Management Definitions

Rule 6.4.1-1: A chassis that includes PICs shall include a Chassis Manager as described in ANSI/VITA 46.11. Conformance Methodology (I)

Permission 6.4.1-1: The SOSA Chassis Manager may be implemented on a SOSA PIC.

Permission 6.4.1-2: The SOSA Chassis Manager may be implemented on a dedicated non-standard hardware element.

Rule 6.4.1-2: A hardware element that implements SOSA Chassis Manager functions shall include a ChMC as described in ANSI/VITA 46.11. Conformance Methodology (I)

Rule 6.4.1-3: A SOSA Chassis Manager implementation shall support the interactions defined for the SOSA Chassis Manager interface. Conformance Methodology (D)

Permission 6.4.1-3: The SOSA Chassis Manager may be distributed across multiple hardware elements to provide redundancy.

Permission 6.4.1-4: A SOSA chassis may include multiple independent Chassis Managers that manage distinct enclaves within a single chassis.

6.4.2 Hardware Element Out-of-Band System Management Definitions

The Non-Volatile Memory Read Only (NVMRO) signal defined in ANSI/VITA 46.0 and ANSI/VITA 65.0 is provided across the backplane to each and all PICs for the purpose of inhibiting changes to non-volatile memories on PICs. The behavior of NVMRO and the interpretation of its validity by PICs are defined in this section. It is the intent of this section to define NVMRO as a means of providing chassis-wide write protection of non-volatile memories.

It is important to recognize that individual PICs might be write-disabled by other system mechanisms, if the state of NVMRO is write-enabled, but no PIC can be write-enabled if NVMRO is in the write-disabled state.

The three intended operational use-cases of chassis-wide write protection can be summarized as:

- Write enabled at power on – this allows firmware updates to be installed
- Write protected at power on – this ensures that if a chassis is processing sensitive information, that sensitive information cannot be inadvertently written to non-volatile memory
- Write enabled at power on – this allows required mission data to be loaded, then system is write-disabled prior to mission execution

Rule 6.4.2-1: A chassis that includes PICs shall have only one source of NVMRO. Conformance Methodology (I)

Observation 6.4.2-1: Because NVMRO is an open drain signal pulled high through a resistor to its asserted (high) state, the write-disabled state could be defeated if more than one entity could pull it to a logic low (de-asserted).

Rule 6.4.2-2: When a SOSA hardware element receives NVMRO and NVMRO is asserted, the SOSA hardware element shall set a latched flag that denotes the write-disabled state and is persistent until 3.3V_AUX power is removed. Conformance Methodology (T)

Rule 6.4.2-3: When a SOSA hardware element supports running one or more SOSA modules, the SOSA hardware element shall make the state of the latched NVMRO flag visible to any SOSA modules that are running in the payload. Conformance Methodology (I)

Permission 6.4.2-1: If NVMRO is de-asserted at system power-on, any module may be placed in a write-disabled state by other means.

Rule 6.4.2-4: The SOSA hardware element shall respond to the write-disabled state by suppressing change to some or all its non-volatile memory components as stated in the vendor's Certificate of Volatility. Conformance Methodology (I)

Observation 6.4.2-2: Not all non-volatile memory components can be inhibited from change in some PIC designs. However, this can be tolerable in some system applications.

Rule 6.4.2-5: When a SOSA hardware element is not hosting the active SOSA Chassis Manager, a SOSA hardware element shall use the NVMRO signal as an input only. Conformance Methodology (I)

Observation 6.4.2-3: Because NVMRO is an open drain signal pulled high through a resistor to its asserted (high) state, the write-disabled state can be defeated if more than one entity can drive it to a logic low (de-asserted). One approach to address this is to provide a manual switch, jumper, or series resistor to connect the driver circuit to the backplane connection only when the hardware element will be used as a SOSA Chassis Manager.

Rule 6.4.2-6: When a SOSA hardware element is hosting the active SOSA Chassis Manager and can source NVMRO, it shall conform to the low current open-drain signal specifications of ANSI/VITA 65.0 §3.3.1 in Table 6.4.2-1.

Table 6.4.2-1: Selected Specifications from ANSI/VITA 65.0 §3.3.1

ANSI/VITA 65.0 Rule	Topic	ANSI/VITA 65.0 Conformance	SOSA Conformance
Rule 3.3.1-1	3.3V Signaling	A,T	A
Rule 3.3.1-2	Vol < 0.6V @ 24ma	A,T	A
Rule 3.3.1-3	Vil < 0.8V Vih > 2.0V	A,T	A
Rule 3.3.1-4	Cload =< 20pf	A,T	A
Rule 3.3.1-5	Ileak =< 50uA	A,T	A
Rule 3.3.1-6	dVin > 3mV/ns	A,T	A

Rule 6.4.2-7: When a SOSA hardware element receives SYSRESET* as an input, the SOSA PIC shall be able to register a valid low for any pulse length of 10ms or longer. Conformance Methodology (D)

Rule 6.4.2-8: When a SOSA hardware element can source SYSRESET* it shall conform to the high current open-drain signal specifications of ANSI/VITA 65.0 §3.3.3 per Table 6.4.2-2.

Table 6.4.2-2: Selected Specifications from ANSI/VITA 65.0 §3.3.3

ANSI/VITA 65.0 Rule	Topic	ANSI/VITA 65.0 Conformance	SOSA Conformance
Rule 3.3.3-1	3.3V Signaling	A,T	A
Rule 3.3.3-2	Vol < 0.6V @ 48ma	A,T	A
Rule 3.3.3-3	Vil < 0.8V Vih > 2.0V	A,T	A
Rule 3.3.3-4	Cload =< 20pf	A,T	A
Rule 3.3.3-5	Ileak =< 50uA	A,T	A
Rule 3.3.3-6	dVin > 3mV/ns	A,T	A

Rule 6.4.2-9: When a SOSA PIC uses MaskableReset* as PERST# it shall use MaskableReset* as the PERST# signal, as defined in the PCIe Base Specification. Conformance Methodology (A)

Recommendation 6.4.2-1: A SOSA PIC should use MaskableReset* as an additional source of PERST#. Conformance Methodology (I)

Observation 6.4.2-4: MaskableReset* can be used as an additional source of PCIe Reset. When used, the root of a PCIe cluster would drive MaskableReset* while the endpoints consume MaskableReset*. Either a radial or bussed MaskableReset* topology can be used. The bussed MaskableReset* will correspond to a PCIe root complex cluster established either by hardwired backplane connection or through a logical switch partition.

Observation 6.4.2-5: ANSI/VITA 65.0, Permissions 3.4.3-4 and 3.4.3-5, which allow for MaskableReset* to be bussed and driven by other PICs, do not apply to SOSA PICs.

Rule 6.4.2-10: A SOSA PIC that receives GDiscrete1 and is not hosting the active SOSA Chassis Manager shall use the GDiscrete1 signal as an input only with respect to ANSI/VITA 65.0, Permission 3.6-1. Conformance Methodology (I)

Observation 6.4.2-6: ANSI/VITA 65.0, Permission 3.6-1, which allows for GDiscrete1 to be configured as an input, an output, or bidirectional does not apply to SOSA PICs.

Permission 6.4.2-2: MaskableReset* may be driven by the SOSA Chassis Manager to individual slots or groups of slots.

Permission 6.4.2-3: A SOSA PIC that is hosting the active SOSA Chassis Manager may source the GDiscrete1 signal.

Rule 6.4.2-11: When SOSA hardware element can source GDiscrete1, it shall conform to the lower-current open-drain interfaces signal specifications of ANSI/VITA 65.0 §3.3.2 per Table 6.4.2. Conformance Methodology (I)

Rule 6.4.2-12: When a SOSA hardware element receives GDiscrete1 and GDiscrete1 is asserted, the SOSA hardware element shall assert a non-volatile flag which is persistent until any associated action taken by the SOSA hardware element is complete. Conformance Methodology (A/D)

Observation 6.4.2-7: The GDiscrete1 flag persists through resets and power cycles. It is cleared only by the hardware element itself once any associated action is complete.

Permission 6.4.2-4: The GDiscrete1 flag may be asserted by other means.

Observation 6.4.2-8: For example, the GDiscrete1 flag on a PIC could be settable via in-band or out-of-band management interactions.

Observation 6.4.2-9: A given PIC could be configured to “take no action” when GDiscrete1 is asserted. In this case, the PIC could clear the GDiscrete1 flag immediately after asserting it, regardless of the FRU activation state. Likewise, a given PIC could be able to complete an action while running only on management power (3.3V_AUX). In this case, the action could occur very quickly after assertion of the flag, and it could not be practical to demonstrate persistence through reset or power-cycle events. Conversely, a PIC could require payload activation, boot, and take a significant amount of time to complete any associated action. In this case, the payload entity that is responsible for the action must be resilient to resets and power cycles and immediately restart or resume the desired action when power is available and the GDiscrete1 flag is set.

Rule 6.4.2-13: When a SOSA PIC receives GDiscrete1 and supports running one or more SOSA modules, the SOSA PIC shall make the state of the non-volatile GDiscrete1 flag visible to any SOSA modules running in the payload. Conformance Methodology (I)

Rule 6.4.2-14: When a SOSA PIC receives GDiscrete1 and supports running one or more SOSA modules, the PIC shall provide a method for a SOSA module to set and clear the non-volatile GDiscrete1 flag state. Conformance Methodology (I)

Rule 6.4.2-15: When a SOSA PIC Card receives GDiscrete1 and its GDiscrete1 flag is asserted, and payload power is available from the backplane, and the PIC requires payload activation to complete an action associated with assertion of the GDiscrete1 flag, the SOSA IPMC on that PIC shall autonomously activate its payload. Conformance Methodology (D)

Rule 6.4.2-16: SOSA PICs shall receive a unique slot number that is based upon the PIC ANSI/VITA 65.0 §3.4.6, Geographic Address as referenced in ANSI/VITA 46.0. Conformance Methodology (I)

Rule 6.4.2-17: A SOSA PIC shall contain an IPMC as described in ANSI/VITA 46.11. Conformance Methodology (I)

Rule 6.4.2-18: A SOSA PIC shall include support for the redundant IPMB-B channel as described in ANSI/VITA 46.11 §4. Conformance Methodology (D)

6.5 SOSA Component State Management

The System Manager can determine, maintain, control, and provide dynamic state representations for the SOSA sensor and for the individual sensor components that comprise the sensor. State management is part of the configuration management functionality within the System Manager. It is implemented by System Manager sub-function managers and/or sub-function agents depending on the sensor component state being provided and the viewpoint of the state being represented.

Each state and transition diagram for each sensor component is constructed to be similar. This is done intentionally to optimize modeling of the state machines in Model-Based Systems Engineering (MBSE) environments.

Note: For the SOSA Technical Standard, Edition 1.0 the System Manager state management functionality defines the state and transition diagrams for the entire sensor, for PICs, and for modules. The states are defined for each type of entity and an informative description supplied to explain the intended functionality that will most typically occur within the state. The defined states align with enumerated data elements within the System Manager interactions. Valid state transitions are documented, and the expected most common state transitions are highlighted. Specific policies and associated normative language for making a particular state transition are not currently included in this document but are planned for a future version.

6.5.1 Sensor State Management

Sensor state is determined, maintained, and provided to other SOSA components by the System Manager. Sensor state is presented from the viewpoint of the System Manager and is accessible to other sensor components via message-based interactions with the System Manager. Sensor state provides a view into the system that encompasses the actions of start-up, configuration, cleansing, and shutdown of the sensor. Run-time states provide insight into the broad view of health of the as-configured sensor and provide the platform upon which other SOSA state and state transition management activities launch; e.g., specific modality task management state and state transition management.

Figure 6.5.1-1 depicts the SOSA sensor state and transition diagram. In Figure 6.5.1-1, the most heavily weighted state transition arrows are used to highlight the expected, most commonly occurring, valid transitions for sensor state. The other, lightly weighted, state transition arrows show the remaining valid transitions that are expected to be less commonly taken. Red dotted-lined state-transition arrows show fault detection and resolution transitions. States represented by circles with dotted-lined perimeters are *unreported* states that are not expected to be maintained by the System Manager. These *unreported* states are primarily stating when the System Manager is not generally expected to be available when the sensor is in the state; e.g., when the hardware element upon which the System Manager sub-function manager or sub-function agent runs is unpowered. These *unreported* states are included for completeness of the state/transition diagrams. The *unreported* states are also included because it is not impossible to envision specific System Manager and sensor implementations that could support reporting of these states; e.g., an implementation where the System Manager operates on a hardware element powered by auxiliary power.

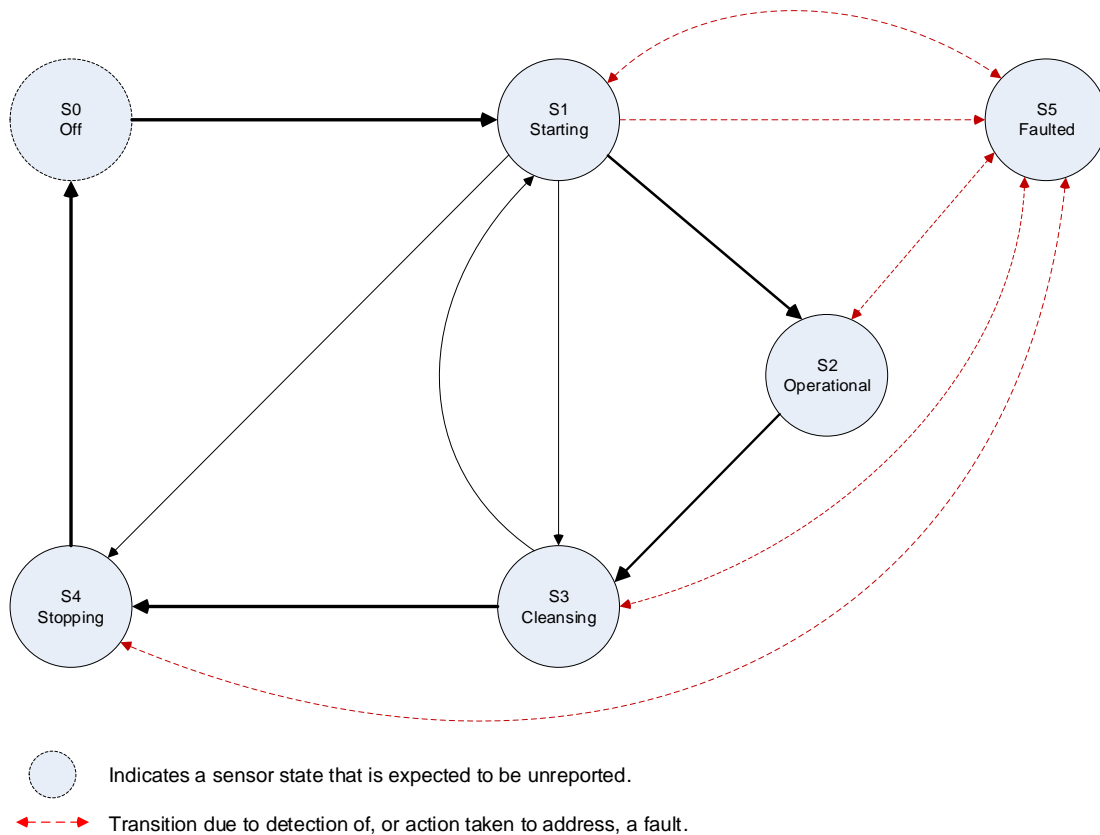


Figure 6.5.1-1: SOSA Sensor State and Transitions Diagram

6.5.1.1 Sensor State 0 (S0): Off

When a sensor is in the S0 state, its configuration and health status is unknown. Generally, it is expected the sensor’s hardware elements (e.g., PICs) are unpowered, and the sensor’s modules are unloaded/unavailable. The S0 state is represented as an *unreported* state as it is generally expected that a System Manager will not be able to report on this state either due to the unavailability of the interface to the System Manager when the sensor is in the S0 state or the unavailability of the System Manager itself. The transition out of the S0 state to the S1 state is intended to occur when communications to/from the System Manager are available.

6.5.1.2 Sensor State 1 (S1): Starting

When a sensor is in the S1 state, it is in the process of configuration and health management. In the S1 state, it is expected that sensor components are discovered, composed into a defined platform framework, and parameterized to defined settings. Diagnostics are also expected to be run in the S1 state. The transition out of the S1 state to the S2 state is intended to occur when a sensor is configured, determined to be healthy, and not required to be cleansed. The transition out of the S1 state to the S5 state is intended to occur when a sensor cannot be fully configured and/or is determined to not be healthy and is not required to be cleansed. The transition out of the S1 state to the S3 state is intended to occur when the sensor is required to be cleansed.

6.5.1.3 *Sensor State 2 (S2): Operational*

When the sensor is in the S2 state, it has been successfully configured and determined to be healthy by the System Manager. In the S2 state, it is expected that application-specific managers (e.g., the SOSA Task Manager) will utilize the sensor and represent its application-specific state and state transitions. In the S2 state, the System Manager is intended to continuously monitor the health of the sensor and be available for sensor configuration changes. The transition out of the S2 state to the S5 state occurs if a fault is detected. It is expected that a cleansing of some sort will be required as part of a reconfiguration and if this is unnecessary the step through the S3 state will be essentially instantaneous.

6.5.1.4 *Sensor State 3 (S3): Cleansing*

When the sensor is in the S3 state, it is expected that sanitization, zeroization, and/or one-ization (setting memory to all ones as opposed to all zeros) actions will take place as needed. The transition out of the S3 state to the S1 state is intended to occur if a reconfiguration of the sensor is needed post-cleanse. The transition out of the S3 state to the S4 state is intended to occur if the sensor is expected to shut down post-cleanse. The transition out of the S3 to the S5 state occurs if a *fault* is detected.

6.5.1.5 *Sensor State 4 (S4): Stopping*

When the sensor is in the S4 state, it is in the process of shutting down and preparing for transition to the S0, or off, state. The transition out of the S4 to the S5 state occurs if a *fault* is detected. The transition out of the S4 state to the S0 state is intended to occur when the sensor is ready to shut down.

6.5.1.6 *Sensor State 5 (S5): Faulted*

When a sensor is in the S5 state, the sensor has been determined to be unhealthy or unable to be configured correctly. Transition out of the S5 state to the S1 state is intended to occur if the resolution of the *fault* requires a reconfiguration of the sensor. Transition out of the S5 state to the S2 state is intended to occur if the *fault* is found to not be an issue or blocker for the sensor to perform its intended roles as currently configured. Transition out of the S5 state to the S3 state is intended to occur if the result of the *fault* processing requires that the sensor be cleansed. Transition out of the S5 state to the S4 state is intended to occur if the result of the *fault* processing requires the sensor to be *shut down*.

6.5.2 **PIC State Management**

PIC state is determined, maintained, and provided to other SOSA components by the System Manager. PIC state is presented from the viewpoint of the System Manager and is accessible to other sensor components via message-based interactions with the System Manager sub-function managers and agents. PIC state provides a view into the system that encompasses the actions of start-up, configuration, cleansing, and shutdown of an individual PIC. Run-time states provide insight into the broad view of health of the as-configured PIC and provide the platform upon which other SOSA state and state transition management activities launch; e.g., specific modality task management state and state transition management.

Figure 6.5.2-1 depicts the PIC state and transition diagram. In Figure 6.5.2-1, the most heavily weighted state transition arrows are used to highlight the expected, most commonly occurring, valid transitions for sensor state. The other, lightly weighted, state transition arrows show the remaining valid transitions that are expected to be less commonly taken. Red dotted-lined state-

transition arrows show fault detection and resolution transitions. Blue dotted-lined state-transitions show loss and recovery of communication capabilities between the sub-function agent and sub-function manager.

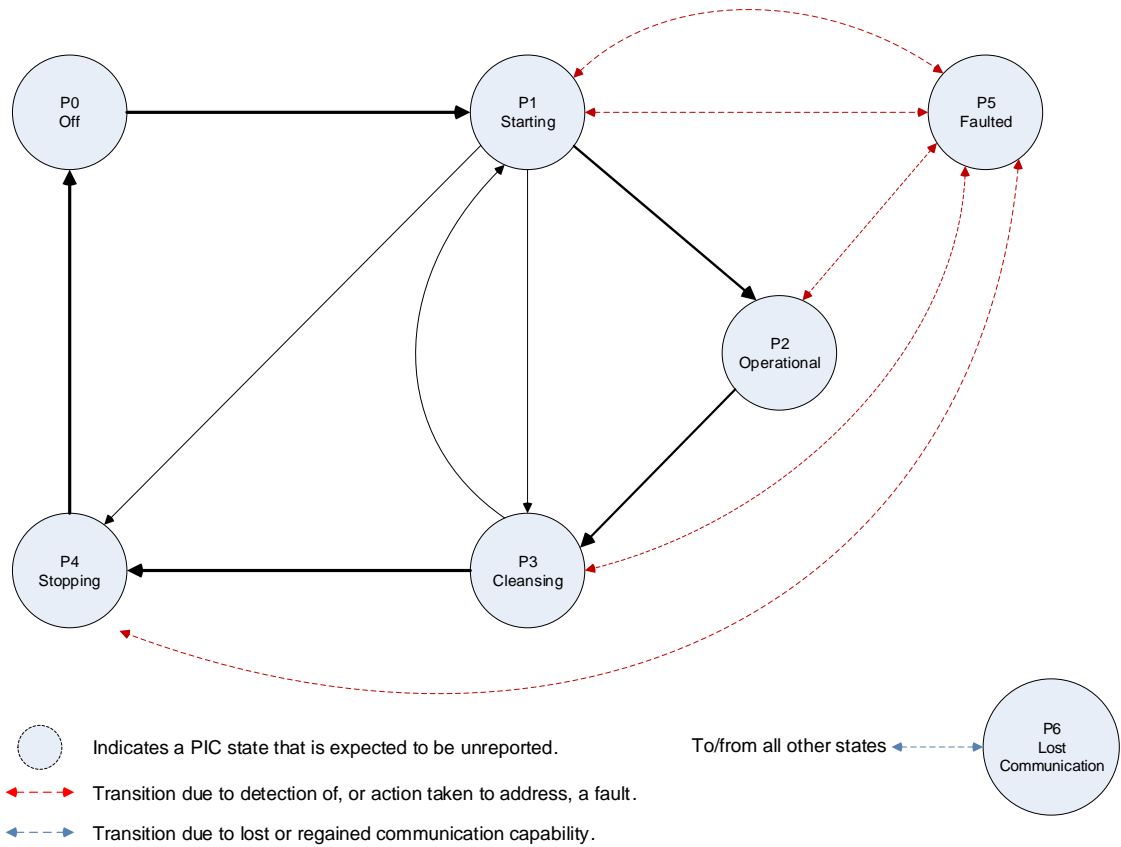


Figure 6.5.2-1: SOSA PIC State and Transitions Diagram

6.5.2.1 PIC State 0 (P0): Off

When a PIC is in the P0 state, its configuration and health status is unknown. It is expected that the PIC’s payload and/or primary power rails are unenergized. Transitions out of the P0 state are intended to occur when the PIC is available for configuration-related interactions; i.e., discovery, composition, and parameterization. This generally would be the case when the PIC’s payload and primary power rails are energized.

6.5.2.2 PIC State 1 (P1): Starting

When a PIC is in the P1 state, it is in the process of configuration and health management. In the P1 state, it is expected that PIC is discovered, composed into a defined platform framework, and parameterized to defined settings. Diagnostics are also expected to be run in the P1 state on the PIC and possibly its interfaces. The transition out of the P1 state to the P2 state is intended to occur when a PIC is configured, determined to be healthy, and not required to be cleansed. The transition out of the P1 state to the P5 state is intended to occur when a sensor cannot be fully configured and/or is determined to not be healthy and is not required to be cleansed. The transition out of the P1 state to the P3 state is intended to occur when the sensor is required to be cleansed. The transition out of the P1 state to the P6 state is intended to occur if communication

between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, is unavailable.

6.5.2.3 *PIC State 2 (P2): Operational*

When the PIC is in the P2 state, it has been successfully configured and determined to be healthy by the System Manager. In the P2 state, it is expected that application-specific managers (e.g., the SOSA Task Manager) will utilize the PIC and represent its application-specific state and state transitions. In the P2 state, the System Manager is intended to continuously monitor the health of the PIC and be available for PIC-related configuration changes. The transition out of the P2 state to the P5 state occurs if a *fault* is detected for the PIC. The transition out of the P5 state to the P3 occurs if the PIC needs to be cleansed or reconfigured. It is expected that a cleansing of some sort will be required as part of a reconfiguration and if this is unnecessary the step through the P3 state will be essentially instantaneous. The transition out of the P2 state to the P6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, is unavailable.

6.5.2.4 *PIC State 3 (P3): Cleansing*

When the PIC is in the P3 state, it is intended that sanitization, zeroization, and/or one-ization actions will take place as needed. The transition out of the P3 state to the P1 state is intended to occur if a reconfiguration of the PIC is needed post-cleanse. The transition out of the P3 state to the P4 state is intended to occur if the PIC is expected to shut down post-cleanse. The transition out of the P3 to the P5 state occurs if a *fault* is detected. The transition out of the P3 state to the P6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, is unavailable.

6.5.2.5 *PIC State 4 (P4): Stopping*

When the PIC is in the P4 state, it is in the process of shutting down and preparing for transition to the P0, or off, state. The transition out of the P4 to the P5 state occurs if a fault is detected. The transition out of the P4 state to the P0 state is intended to occur when the PIC is ready to shut down. The transition out of the P4 state to the P6 (Lost Communication) state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, is unavailable.

6.5.2.6 *PIC State 5 (P5): Faulted*

When a PIC asserts the P5 state, the PIC has been determined to be unhealthy or unable to be configured correctly. Assertion of the P5 state is intended to occur if the resolution of the *fault* requires a reconfiguration of the PIC. Assertion of the P5 state to the P2 state is intended to occur if the *fault* is found to not be an issue or blocker for the PIC to perform its intended roles as currently configured. Transition out of the P5 state to the P3 state is intended to occur if the result of the *fault* processing requires that the PIC be cleansed. Transition out of the P5 state to the P4 state is intended to occur if the result of the *fault* processing requires the PIC to be *shut down*.

6.5.2.7 *PIC State 6 (P6): Lost Communication*

When a PIC asserts the P6 state, communication between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, is unavailable. It is often important to present this situation as a separate condition than a known fault as the PIC might be performing all other actions correctly and communication channels could be restored.

A PIC asserting the P6 state is expected to retain the state from which it transitioned as it is expected to transition back to that state upon restoration of communication. Transition out of the P6 state to the previous state from which the state machine transitioned into the P6 state occurs when communications between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, are once again available.

6.5.3 Module State Management

Module state is determined, maintained, and provided to other SOSA components by the System Manager. Module state is presented from the viewpoint of the System Manager and is accessible to other sensor components via message-based interactions with the System Manager sub-function managers and agents. Module state provides a view into the system that encompasses the actions of start-up, configuration, cleansing, and shutdown of an individual SOSA module. Run-time states provide insight into the broad view of health of the as-configured SOSA module and provide the platform upon which other SOSA state and state transition management activities launch; e.g., specific modality task management state and state transition management.

Figure 6.5.3-1 depicts the module state and transition diagram. In Figure 6.5.3-1, the most heavily weighted state transition arrows are used to highlight the expected, most commonly occurring, valid transitions for sensor state. The other, lightly weighted, state transition arrows show the remaining valid transitions that are expected to be less commonly taken. Red dotted-lined state-transition arrows show fault detection and resolution transitions. Blue dotted-lined state-transitions show loss and recovery of communication capabilities between the sub-function agent and sub-function manager.

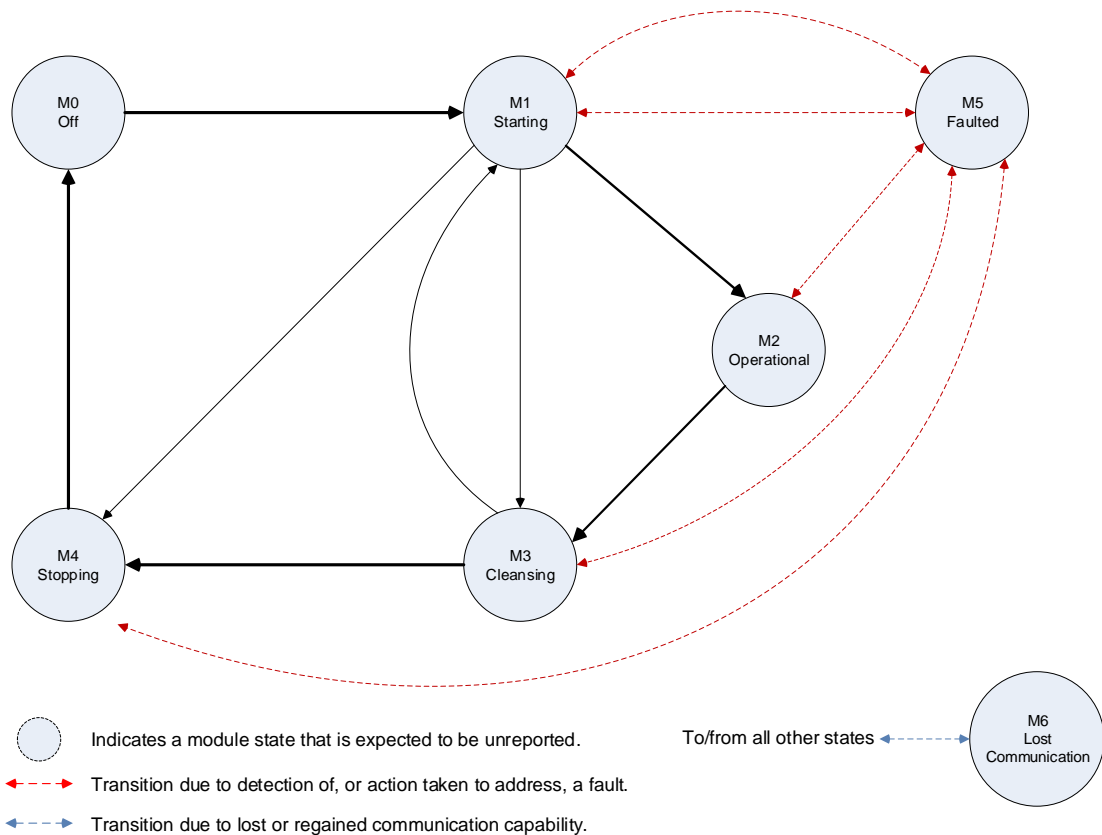


Figure 6.5.3-1: SOSA Module State and Transitions Diagram

6.5.3.1 *SOSA Module State 0 (M0): Off*

When a SOSA module is in the M0 state, its configuration and health status is unknown. It is expected that the SOSA module is not currently capable of performing its intended operation and in many implementations could not even be available for configuration; e.g., a software SOSA module implementation has not been decrypted from storage and loaded into the main memory of an application processor. Transitions out of the M0 state are unintended to occur when the SOSA module is available for configuration-related interactions; i.e., discovery, composition, and parameterization.

6.5.3.2 *SOSA Module State 1 (M1): Starting*

When a SOSA module is in the M1 state, it is in the process of configuration and health management. In the M1 state, it is expected that the SOSA module is discovered, composed into a defined platform framework, and parameterized to defined settings. Diagnostics are also expected to be run in the M1 state on the module, possibly its interfaces, and possibly any other SOSA sensor components that comprise the module. The transition out of the M1 state to the M2 state is intended to occur when a SOSA module is configured, determined to be healthy, and not required to be cleansed. The transition out of the M1 state to the M5 state is intended to occur when a SOSA module cannot be fully configured and/or is determined to not be healthy and is not required to be cleansed. The transition out of the M1 state to the M3 state is intended to occur when the SOSA module is required to be cleansed. The transition out of the M1 state to the M6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable.

6.5.3.3 *SOSA Module State 2 (M2): Operational*

When the SOSA module is in the M2 state, it has been successfully configured and determined to be healthy by the System Manager. In the M2 state, it is expected that application-specific managers (e.g., the SOSA Task Manager) will utilize the SOSA module and represent its application-specific state and state transitions. In the M2 state, the System Manager is intended to continuously monitor the health of the SOSA module and be available for SOSA module-related configuration changes. The transition out of the M2 state to the M5 state occurs if a fault is detected for the SOSA module. The transition out of the M5 state to the M3 state occurs if the module needs to be cleansed or reconfigured. It is expected that a cleansing of some sort will be required as part of a reconfiguration and if this is unnecessary the step through the M3 state will be essentially instantaneous. The transition out of the M2 state to the M6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable.

6.5.3.4 *Module State 3 (M3): Cleansing*

When the SOSA module is in the M3 state, it is intended that sanitization, zeroization, and/or one-ization actions will take place as needed. The transition out of the M3 state to the M1 state is intended to occur if a reconfiguration of the SOSA module is needed post-cleanse. The transition out of the M3 state to the M4 state is intended to occur if the SOSA module is expected to shut down post-cleanse. The transition out of the M3 state to the M5 state occurs if a fault is detected. The transition out of the M3 state to the M6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable.

6.5.3.5 *Module State 4 (M4): Stopping*

When the SOSA module is in the M4 state, it is in the process of shutting down and preparing for transition to the M0, or off, state. The transition out of the M4 state to the M5 state occurs if a fault is detected. The transition out of the M4 state to the M0 state is intended to occur when the SOSA module is ready to shut down. The transition out of the M4 state to the M6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable.

6.5.3.6 *Module State 5 (M5): Faulted*

When a SOSA module is in the M5 state, the SOSA module has been determined to be unhealthy or unable to be configured correctly. Transition out of the M5 state to the M2 state is intended to occur if the resolution of the fault requires a reconfiguration of the PIC. Transition out of the M5 state to the M2 state is intended to occur if the fault is found to not be an issue or blocker for the SOSA module to perform its intended roles as currently configured. Transition out of the M5 state to the M3 state is intended to occur if the result of the fault processing requires that the SOSA module be cleansed. Transition out of the M5 state to the M4 state is intended to occur if the result of the fault processing requires the SOSA module to be shut down. The transition out of the M5 state to the M6 state is intended to occur if communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable.

6.5.3.7 *Module State 6 (M6): Lost Communication*

When a SOSA module is in the M6 state, communication between the System Manager configuration manager and the System Manager configuration agent, that represents the SOSA module, is unavailable. It is often important to present this situation as a separate condition than a known fault as the SOSA module might be performing all other actions correctly and communication channels could be restored. A PIC entering the M6 state is expected to retain the state from which it transitioned as it is expected to transition back to that state upon restoration of communication. Transition out of the M6 state to the previous state from which the state machine transitioned into the M6 state occurs when communications between the System Manager configuration manager and the System Manager configuration agent, that represents the PIC, are once again available.

6.5.4 **Secure System Start-Up**

This section provides a high-level decomposition of a start-up sequence for SOSA modules in a sensor system, and associated rules. Figure 6.5.4-1 describes a high-level decomposition of major events which could occur within a start-up sequence. The start-up sequence begins by the activation of the hardware modules in the system through initialization of its IPMC function (*Initialize Hardware*).

Upon a successful discovery by the Chassis Manager, the modules continue their initialization process by the authentication of their hardware configuration. Once validated, the boot RTE is retrieved, authenticated, and loaded (*Initialize and Boot Run-time Environment*), follow by software packages (*Load Software Packages*).

The modules in the sensor system are then configured and composed to support the mission operations (*Compose Sensor*). Details on how each event is accomplished is implementation-dependent. A behavioural model of these events is described in the RIG for reference only.

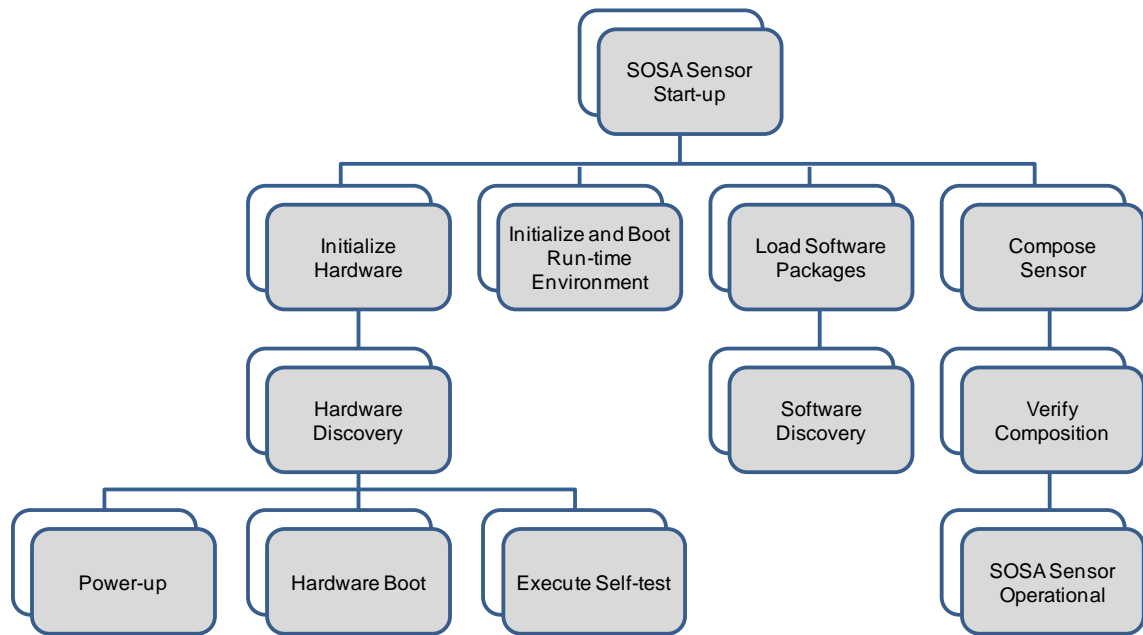


Figure 6.5.4-1: Sensor System Start-Up Decomposition

During the start-up process through operation, the sensor system and its components transition through numerous states and modes. The states are defined separately at the system, hardware element, and module level, respectively. State-machine at each level is also defined differently depending on the perspective.

Securing the sensor system is critical at start-up as new or modified components are potentially introduced. The definition of the security states is meant to provide references for rules that describe the mechanisms in authenticating and validating the components of the system throughout the start-up process. The security authentication and validation are primarily facilitated by the Security Manager. While the secured start-up rules define the required security state transition sequence and the associated mechanisms, the management of the system or module at a particular security state and implementation of the mechanisms are to be defined by the system designer/integrator.

The series of security state-machines described below defines transitions among security states for the system, the PICs, the modules, and the Inter-Module Interfaces (IMIs). The security states can be perceived as parallel to that of the operational states. The security states of the system, PIC, module, and IMI could contribute as conditions to the transitions of the operation states.

The system level security states are defined in Figure 6.5.4-2. The default security state of the system is *Evaluating*, where the integrity of the system is being evaluated. Upon completion of the evaluation, the system would transition to *Protected*, *Compromised*, or *Degraded*. While the evaluation process will be primarily performed by the System Manager during operation, it can also take places while the system is powered off if it contains battery-backed security monitors that can detect security events. The *Evaluating* state is mostly a transitional state; prior to start-up, the system will likely be in one of the other three steady states. Once the System Manager is operational during start-up, the system will transition from one of the steady states to *Evaluating*.

If the system integrity is evaluated to be assured, it transitions to the *Protected* state. In addition to start-up, upon detection of a security event, BIT event, or command, the system in *Protected*

state will transition to the *Evaluating* state to re-assess the security posture. The system transitions to *Compromised* if the integrity of the system is severely degraded where the system is likely be sanitized, zeroized and then powered down. The determination of the system integrity depends on the composition of the system and the associated security policy. The system transitions to *Degraded* if integrity of certain components cannot be verified, but not critical enough to cease operation. The system would operate in a limited fashion to minimize security vulnerability to attack or exploitation.

- **Evaluating:** default transitional state where the security state of the system is being assessed; the system will transition back to this state during start-up, upon detection of a security/BIT event, or commanded
- **Protected:** the integrity of the system is evaluated to be intact from the last assessment
- **Degraded:** the integrity of the system is evaluated to be degraded from the last assessment – such evaluation depends on the composition of the system and the associated security policy; for example, this can be a case where certain component(s), hardware, and/or software cannot be authenticated, but the component(s) are not critical to the operation in the security perspective
- **Compromised:** the integrity of the system is evaluated to be severely degraded from the last assessment – such evaluation depends on the composition of the system and the associated security policy

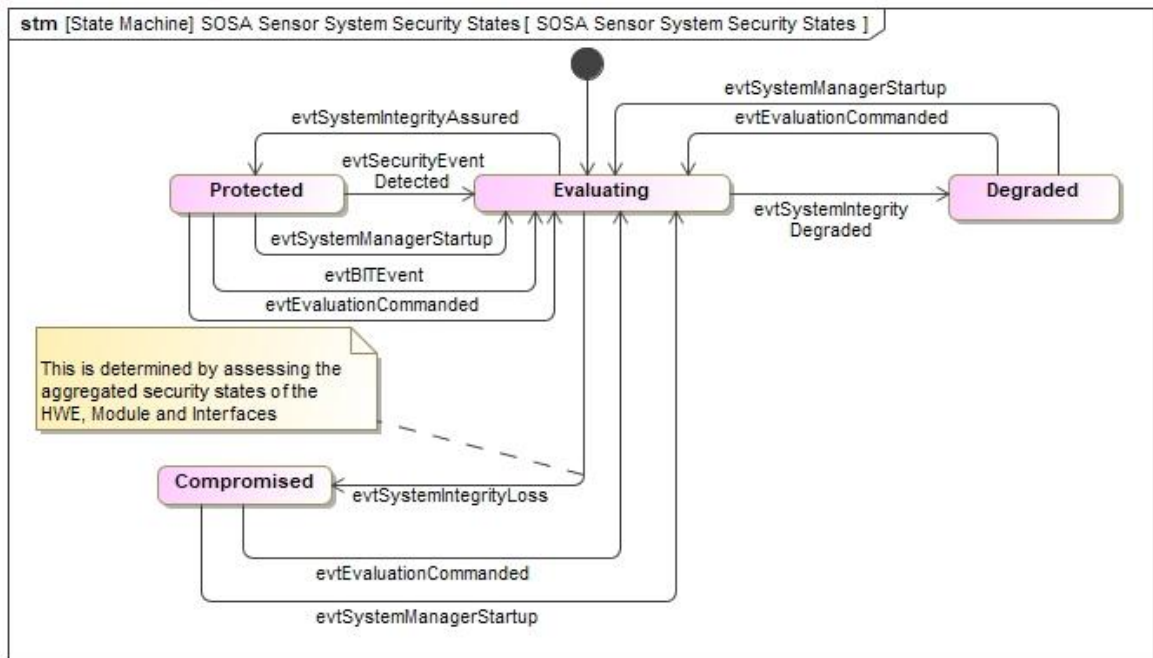


Figure 6.5.4-2: SOSA System Security States

At the SOSA PIC/module level, each SOSA PIC/module would go through multiple of stages of authentication to ensure the integrity of the module before being fully composed into the sensor system. These authentication stages associate with the transition of the SOSA module between security states. Figure 6.5.4-3 describes the state transition model of the security states at the PIC/module level. Note that the SOSA PIC/module security states are from the perspective of the System Manager. The System Manager designates, monitors, and reports the security states

of each PIC/module. The collective security states of all the SOSA PIC/modules are used by the System Manager to assess the security posture and integrity of the system.

A Root of Trust (RoT) is an inherently trusted entity which can be implemented in software or hardware. The inherent trust can be established via cryptographic means (e.g., keys/certificate from trusted source) and/or design (e.g., anti-tamper), which is implementation dependent. The security management role of the SOSA System Manager module would be coupled with a RoT to perform hardware authentication functions.

The security states for a SOSA PIC are defined as follows. A PIC transitions into the default state, Trust Pending, upon completion of the hardware element start-up transitions. The System Manager is required to support a hardware authentication, or attestation, of the PIC for the PIC to transition to the Trusted state. If the attestation fails or times out, the PIC transitions to the Untrusted state. Note that the attestation is expected to be performed by the System Manager. Therefore, to transition from Trust Pending to Trusted, the System Manager must be operational. The PIC can transition from Untrusted to Trust Pending upon reset or commanded by a trusted entity such as the System Manager if allowed by security policy. To reiterate, these security states are from the perspective of the System Manager. The PIC can operate independent of how the System Manager perceives its trust. However, the System Manager could limit tasks or resources associate with an Untrusted PIC to minimize security vulnerabilities.

- **Trust Pending:** the PIC transitions into this default state during start-up or transitions back to this state when a security event is detected
- **Trusted:** the PIC transitions into this state when the hardware configuration is successfully authenticated to a RoT/System Manager
- **Untrusted:** the PIC transitions into this state when the hardware configuration fails or is unable to authenticate to a RoT/System Manager

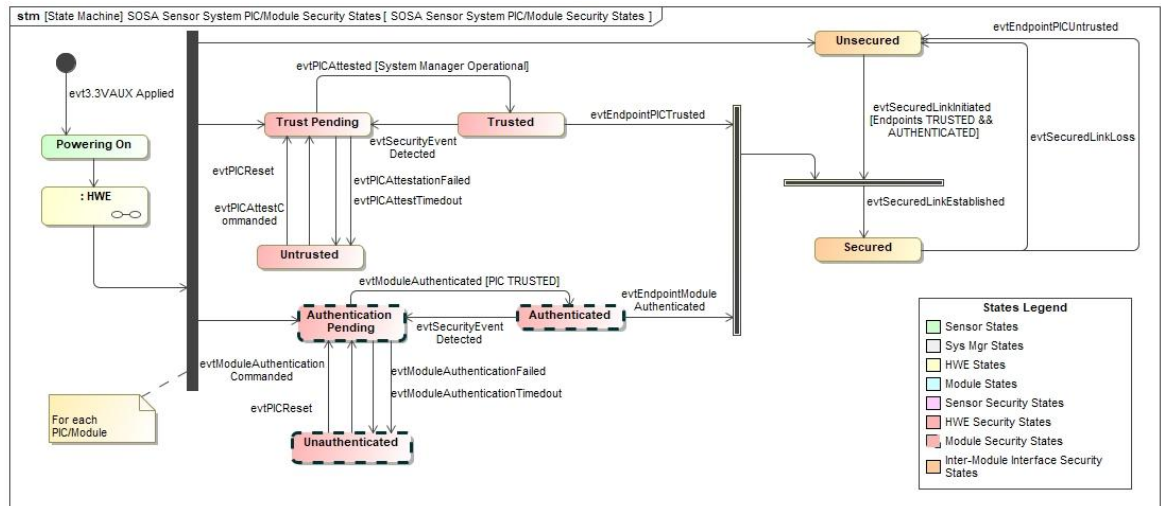


Figure 6.5.4-3: SOSA PIC/Module Security States

The security states for SOSA module software are defined as follows. It follows similar patterns to the SOSA PIC security states. To transition from the default Authentication Pending to Authenticated, the PIC that is hosting the module software must be Trusted by the System Manager. If not, the authentication will automatically fail. Unauthenticated software should not be executed by its hosting environment.

- **Authentication Pending:** the SOSA module software transitions into this default state during initial loading, or transitions back to this state when a security event is detected
- **Authenticated:** the SOSA module software transitions into this state when the software package associated with the module is successfully authenticated by Security Services
- **Unauthenticated:** the SOSA module software transitions into this state when the software package associated with the module failed or unable to be authenticated by Security Services

Lastly, the following security states are associated with an IMI. An IMI can be perceived as a point-to-point link between two SOSA modules, which can be at the IP or Message Authentication Code (MAC) level. The default state of an IMI is Unsecured. For certain use-cases, it can operate fully at this state. If a secured connection is required by policy for this link, both endpoints of the IMI need to be Trusted and Secured. A SOSA module should inquire about the security state of the other endpoint before initiating or accepting a secured connection request. An IMI can operate as Unsecured throughout the mission if allowed by security policy or if the data being exchanged is not sensitive. For example, pre-encrypted data can be exchanged via an Unsecured interface.

- **Secured:** a SOSA IMI is considered Secured when the end-to end inter-module communication is secured by appropriate means based on the system security policy; e.g., Transport Layer Security (TLS)
- **Unsecured:** a SOSA IMI considered Unsecured when the end-to-end inter-module communication is unable to be secured by appropriate means (e.g., TLS), unable to be re-secured upon interruptions, or a loss of integrity associated with one of the endpoints is detected

6.5.4.1 *Initialize Hardware*

Rule 6.5.4.1-1: When requested, the SOSA System Manager shall authenticate the hardware configuration of internal SOSA PIC(s). Conformance Methodology (D)

Rule 6.5.4.1-2: A SOSA managed PIC shall authenticate its hardware configuration to the SOSA System Manager. Conformance Methodology (D)

Rule 6.5.4.1-3: The SOSA System Manager shall designate a SOSA PIC as Untrusted if a SOSA PIC is unable to authenticate its hardware configuration to the SOSA System Manager. Conformance Methodology (D)

Rule 6.5.4.1-4: The SOSA System Manager shall designate a SOSA PIC as Trusted when a SOSA PIC authenticates its hardware configuration to the SOSA System Manager. Conformance Methodology (D)

6.5.4.2 *Initialize and Boot RTE*

The following rules define requirements services necessary for a PIC with SW RTE to boot the run-time system from a remote storage device. Related rules on the SOSA Storage/Retrieval Manager module are described in Section 10.5.

Rule 6.5.4.2-1: The SOSA Security Services module shall authenticate all remote RTE software prior to execution. Conformance Methodology (D)

Rule 6.5.4.2-2: Where decryption is required for the remote RTE software, the SOSA Encryptor/Decryptor module shall be used for decryption. Conformance Methodology (D)

The following rules describe status reporting that is necessary for the SOSA System Manager to facilitate start-up and composing SOSA modules into the system.

Rule 6.5.4.2-3: A managed SOSA PIC shall provide its current operational state to the SOSA System Manager module. Conformance Methodology (D)

Rule 6.5.4.2-4: A SOSA PIC shall provide its current version information to the SOSA System Manager module. Conformance Methodology (D)

Rule 6.5.4.2-5: A directly managed SOSA PIC shall provide the status, active or inactive, of its MAC layer ports to the SOSA System Manager module. Conformance Methodology (D)

Rule 6.5.4.2-6: A directly managed SOSA PIC shall provide the status, active or inactive, of its IP layer ports to the SOSA System Manager module. Conformance Methodology (D)

6.5.4.3 *Load Software Packages*

Rule 6.5.4.3-1: All sensor software packages shall be authenticated prior to execution. Conformance Methodology (D)

Rule 6.5.4.3-2: Where decryption is required for a sensor software package, the SOSA Encryptor/Decryptor module shall be used for decryption. Conformance Methodology (D)

Rule 6.5.4.3-3: If a sensor software package fails authentication or is unable to be authenticated, the sensor software shall be designated by the SOSA System Manager as Unauthenticated. Conformance Methodology (D)

Rule 6.5.4.3-4: The sensor software shall be designated by the SOSA System Manager as Authenticated when a sensor software package is successfully authenticated. Conformance Methodology (D)

6.5.4.4 *Compose Sensor*

Rule 6.5.4.4-1: If a SOSA IMI is unable to be secured, the SOSA IMI shall be designated by the SOSA System Manager as Unsecured. Conformance Methodology (D)

Rule 6.5.4.4-2: The SOSA IMI shall be designated by the SOSA System Manager as Secured when a SOSA IMI is secured. Conformance Methodology (D)

7 Task Management

7.1 Task Manager Module

7.1.1 Module Definition

The Task Manager module is responsible for coordinating all mission operations, including managing mission operations, and executing mission tasks. It accepts external sensor tasking and initiates actions to execute those mission tasks by developing Receiver/Exciter control actions. In addition, the Task Manager is responsible for reporting the status of a specific set of mission task or tasks. In the current version of this document, the SOSA task management interaction definitions are defined based on three RF sensor threads: SAR, EW, and SIGINT.

The high-level description of the Task Manager module is provided in Table 7.1.1-1, which provides a detailed functional decomposition for this module.

See Section 4.2 for the definition of this module.

Table 7.1.1-1: Task Manager Module Description (SvcV-1)

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Manage Mission Tasking	Process External Tasking	The action of accepting, starting, pausing, resuming, or canceling a mission task or tasks.
Coordinate Mission Operations	Manage Mission Tasking	Report Mission Tasking Status	The action of reporting the status of a specific mission task or tasks.
Coordinate Mission Operations	Manage Mission Tasking	Notify Mission Product of Interest	The action of informing processing modules of the intended output products to be generated for a given mission.
Coordinate Mission Operations	Execute Mission Tasking	Control Receiver/Exciter Action	The action of starting, pausing, resuming, or canceling a Conditioner-Receiver-Exciter task or tasks.
Coordinate Mission Operations	Execute Mission Tasking	Notify Processing Modules	The action of informing processing modules of a Conditioner-Receiver-Exciter task or tasks.
Coordinate Mission Operations	Execute Mission Tasking	Control Calibration Action	The action of initiating calibration events to calibrate the Conditioner-Receiver-Exciter and Emitter/Collector.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Execute Mission Tasking	Manage Mode/State Changes	The action of managing the configuration, state, and mode of the other SOSA modules based on mission tasking.

7.1.2 Task Manager Interactions

Overall, the Task Manager receives mission tasks via the Host Platform Interface and interacts with the Conditioner-Receiver-Exciter, Signal/Object Detector & Extractor, and Image Pre-processor modules to execute SAR, EA, and SIGINT tasks. It coordinates with Reporting Services to convey results back to Host Platform Interface. Figure 7.1.2-1 shows the sequence mission initiation from the Host Platform Interface and registration with Nav Data and Time Data Services. The sequence diagram does not capture any System Manager interaction such as health and status or sensor registration.

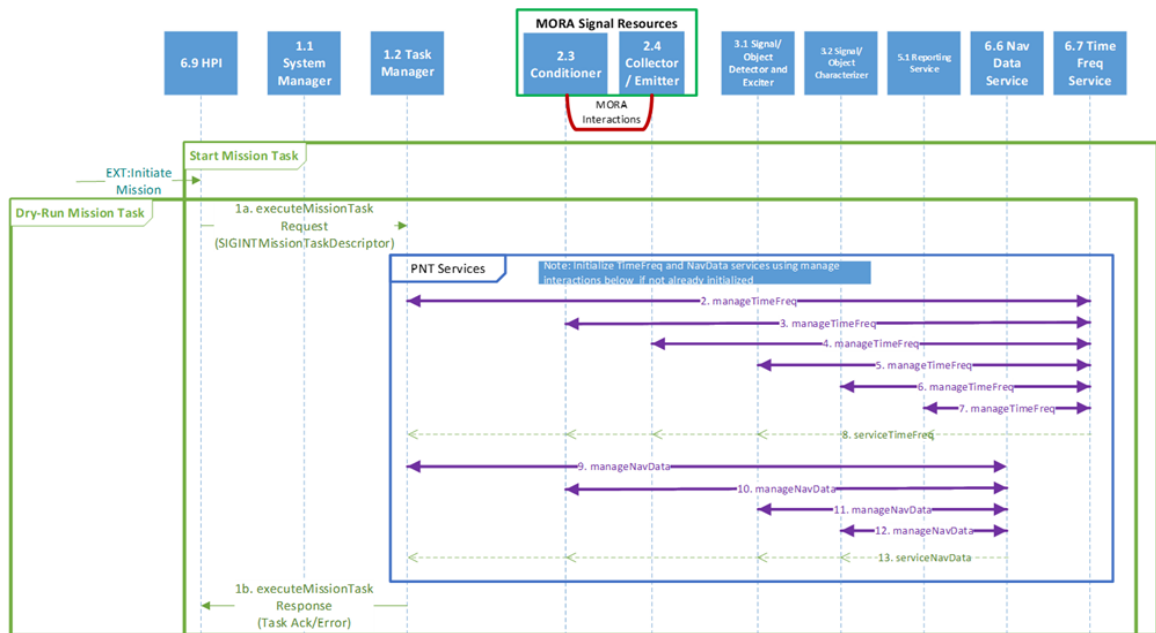


Figure 7.1.2-1: Initiating Mission Task

Once the Task Manager has received the mission task, the Task Manager coordinates with Conditioner-Receiver-Exciter and other SOSA modules to execute the mission loop as shown in Figure 7.1.2-2 (SIGINT example).

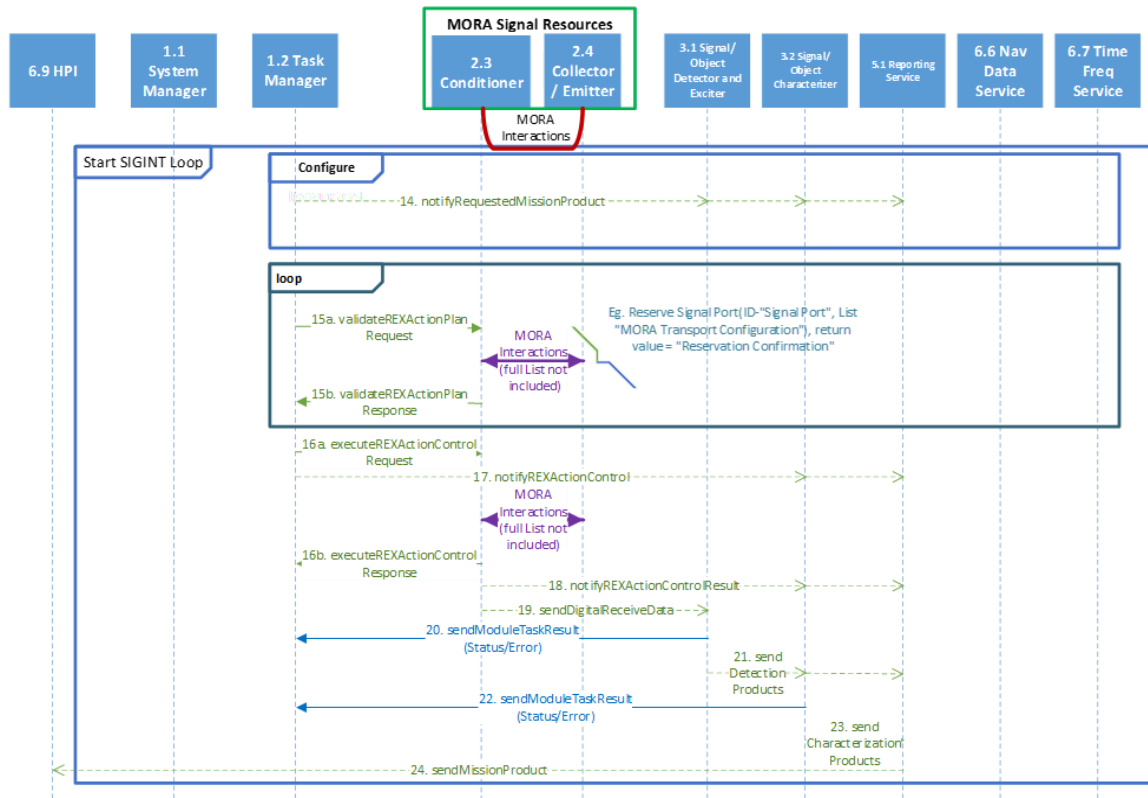


Figure 7.1.2-2: Task Manager Coordinating Mission Execution Loop and Conveying Status to the Host Platform Interface Module

Finally, the Task Manager negotiates any mission update messages from the Host Platform Interface such as mission cancellation, pause, or restart as shown in Figure 7.1.2-3.

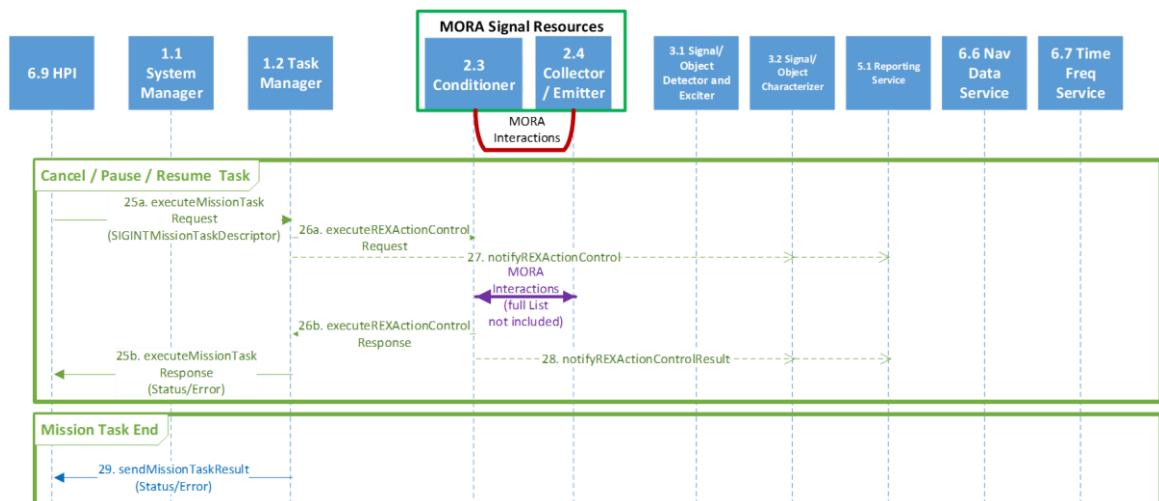


Figure 7.1.2-3: Task Manager Coordinating Mission Task Updates

Table 7.1.2-1 shows the interactions that have been defined for the Task Manager module based on the three RF sensor threads considered under the current version of this document, as shown in Figure 7.1.2-1 through Figure 7.1.2-3.

Table 7.1.2-1: Task Manager Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
executeMissionTask	The action of accepting or rejecting a mission task request.	MissionTaskDescriptor	MissionTaskResponse	Required	Response
executeREXActionControl	The action of starting, pausing, resuming, or canceling a Conditioner-Receiver-Exciter task.	REXActionControl	REXActionResult	Required	Request
notifyRequestedMissionProduct	The action of informing processing modules of the intended output products to be generated for a given mission request.	MissionProduct		Required	Multicast
notifyREXActionControl	The action of informing processing modules of the Conditioner-Receiver-Exciter task or tasks being executed.	REXActionControl		Required	Multicast
sendMissionTaskResult	Action of informing the execution results of a mission task request.	MissionTaskResult		Required	Unicast
validateREXActionPlan	Action of coordinating a REX action plan.	REXActionPlan	REXActionPlanResponse	Required	Response

7.1.3 Task Manager Interaction Rules

The following rules apply to the interactions for the Task Manager defined in Section 7.1.1.

Observation 7.1.3-1: The SOSA Task Manager in the current version supports SAR, SIGINT, and EA (barrage jamming) missions. The interactions described make no assumptions on prioritizing resources to support various competing tasks in a multi-modal SOSA sensor.

Rule 7.1.3-1: The SOSA Task Manager shall keep track of all mission task states as WAITING_TO_START, IN_PROGRESS, PAUSED, COMPLETED, CANCELED, FAULTED, and ABORTED by mission TaskID. Conformance Methodology (T)

Rule 7.1.3-2: The SOSA Task Manager shall implement all required interactions defined in Table 7.1.2-1. Conformance Methodology (T)

8 Transmission/Reception

Transmission/reception is the set of functionalities required to translate back and forth between Electromagnetic (EM) energy and digital representations of imagery or RF signals. This includes conversion between EM energy and electric signals, conditioning those signals, and conversion between electric signals and digital representations.

These functions are provided by two SOSA modules; Conditioner-Receiver-Exciter (module 2.3) and Emitter/Collector (module 2.4). These modules are intended to support both imagery-based and RF signal-based sensing modalities.

The following sections define the functional decomposition, specific functions, interactions, and rules that apply to these modules.

8.1 Conditioner-Receiver-Exciter

The high-level description of the Conditioner-Receiver-Exciter module is provided in Section 4.2. Table 8.1-1 provides a detailed functional decomposition for this module.

Table 8.1-1: Conditioner-Receiver-Exciter Functions (SvcV-4)

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Conditioner-Receiver-Exciter Tasking	Manage Task	Control Task	The action of starting, pausing, resuming, or canceling a Conditioner-Receiver-Exciter task.
Manage Conditioner-Receiver-Exciter Tasking	Manage Task	Plan Task	The action of negotiating a viable plan for Conditioner-Receiver-Exciter task execution.
Manage Conditioner-Receiver-Exciter Tasking	Manage Task	Monitor Task Status	The action of monitoring the status for a specific Conditioner-Receiver-Exciter task or tasks. (Note: A corresponding interaction is needed in Task Manager and will be added in a future version.)
Execute Conditioner-Receiver-Exciter Tasking	Execute Task	Notify Result	The action of notifying the result of a specific Conditioner-Receiver-Exciter task.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Execute Conditioner-Receiver-Exciter Tasking	Execute Task	Generate Data of Interest	The action of generating production results for a specific Conditioner-Receiver-Exciter task.
Execute Conditioner-Receiver-Exciter Tasking	Execute Task	Consume Data of Interest	The action of consuming signal data of interest for a specific Conditioner-Receiver-Exciter task. (Note: A capability is needed for Task Manager and will be added in a future version.)
Execute Conditioner-Receiver-Exciter Tasking	Execute Receive Tasking	Execute Channelization	The action of channelizing the receive signal data to achieve the acquisition of specific data of interest.
Execute Conditioner-Receiver-Exciter Tasking	Execute Receive Tasking	Execute Metadata Tagging	The action of tagging the receive data of interest for effective subsequent processing.
Execute Conditioner-Receiver-Exciter Tasking	Execute Receive Tasking	Execute Data Framing	The action of framing the receive data of interest for effective subsequent processing.
Execute Conditioner-Receiver-Exciter Tasking	Execute Receive Tasking	Execute Data Cube Formation	The action of forming multi-dimensional receive data of interest for subsequent processing.
Execute Conditioner-Receiver-Exciter Tasking	Execute Transmit Tasking	Execute Adaptation	The action of optimizing temporal, spatial, and/or frequency aspects of transmit tasking for interoperability and/or enhanced performance.
Execute Conditioner-Receiver-Exciter Tasking	Execute Transmit Tasking	Execute Calibration	The action of phase and amplitude calibrating the transmit signal resources to achieve complex transmit manifold performance.
Execute Conditioner-Receiver-Exciter Tasking	Execute Transmit Tasking	Execute Waveform Generation	The action of generating a transmit waveform including content, frequency, spatial, and temporal aspects.
Manage Conditioner-Receiver-Exciter Module	Manage RF Device	Manage RF Device Parameters	The action of managing the configuration, state, status, and health of the RF device.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Conditioner-Receiver-Exciter Module	Manage RF Signal Resources	Manage Signal Resource Parameters	The action of reserving and releasing signal resources.
Manage Conditioner-Receiver-Exciter Module	Manage RF Signal Resources	Provide Signal Resource Parameters	The action of providing the profile of signal resources.
Execute RF Functions (Rx/Tx)	Execute RF Conditioning	Amplify/Attenuate RF Signal	The action of amplifying or attenuating RF signals including Low Noise Amplifiers (LNAs), RF attenuators, and High-Power Amplifiers (HPAs).
Execute RF Functions (Rx/Tx)	Execute RF Conditioning	Filter RF Signal	The action of frequency filtering of RF signals including band pass, band reject, low pass, and high pass RF filters.
Execute RF Functions (Rx/Tx)	Execute RF Distribution	Distribute RF Signal	The action of distributing analog RF signals including RF switches, RF combiners, and RF splitters.
Execute RF Functions (Rx/Tx)	Execute RF Translation	Frequency Translate RF Signals	The action of frequency translating RF signals including RF down converters, RF up converters, digital down converters, and digital up converters.
Execute RF Functions (Rx/Tx)	Execute RF Signal Domain Conversion	Convert Domain of RF Signals	The action of ADC or DAC for RF signals.

8.2 Emitter/Collector

The high-level description of the Emitter/Collector module is provided in Section 4.2. Table 8.2-1 provides a detailed functional decomposition for this module.

Table 8.2-1: Emitter/Collector Functions (SvcV-4)

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Emitter/Collector Module	Manage RF Device	Manage RF Device Parameters	The action of managing the configuration, state, status and health of the RF device.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Manage Emitter/Collector Module	Manage RF Signal Resources	Manage Signal Resource Parameters	The action of reserving and releasing of signal resources.
Manage Emitter/Collector Module	Manage RF Signal Resources	Provide Signal Resource Parameters	The action of providing the profile of signal resources.
Execute RF Functions (Rx/Tx)	Execute RF Aperture	Collect Electro-magnetic Energy	The action of collecting EM energy into electric signals.
Execute RF Functions (Rx/Tx)	Execute RF Aperture	Emit Electro-magnetic Energy	The action of emitting EM energy from electric signals.
Execute RF Functions (Rx/Tx)	Execute RF Conditioning	Amplify/Attenuate RF Signal	The action of amplifying or attenuating RF signals including LNAs, RF attenuators, and HPAs.
Execute RF Functions (Rx/Tx)	Execute RF Conditioning	Filter RF Signal	The action of frequency filtering RF signals including band pass, band reject, low pass, and high pass RF filters.
Execute RF Functions (Rx/Tx)	Execute RF Distribution	Distribute RF Signal	The action of distributing analog RF signals including RF switches, RF combiners, and RF splitters.
Execute RF Functions (Rx/Tx)	Execute RF Translation	Frequency Translate RF Signals	The action of frequency translating RF signals including RF down converters, RF up converters, digital down converters, and digital up converters.
Execute RF Functions (Rx/Tx)	Execute RF Signal Domain Conversion	Convert Domain of RF Signals	The action of ADC or DAC for RF signals.

8.3 RF Signal Layer Definitions

In sensor applications that collect and/or emit RF EM energy the Conditioner-Receiver-Exciter and Emitter/Collector modules together perform the conversion from RF EM energy to digital representations for receive tasks and conversion from a digital representation to RF EM energy for transmit tasks. These two modules are referred to as the RF Signal Layer. The RF-based applications supported by this document currently include EW, Radar, and SIGINT. A future version is intended to further support additional RF applications such as tactical communications.

This section defines the specific functions, interactions, and rules for the RF Signal Layer modules.

The SOSA RF Signal Layer modules include:

- Module 2.3: Conditioner-Receiver-Exciter
- Module 2.4: Emitter/Collector

8.3.1 Modular Open Radio Frequency Architecture (MORA)

The SOSA Consortium has adopted portions of the Modular Open Radio Frequency Architecture (MORA) Specification for the RF instantiation of the Conditioner-Receiver-Exciter and Emitter/Collector modules. MORA is an extension to the Vehicular Integration for C4ISR/EW Interoperability (VICTORY) architecture, which is an OSA for integrating electronics into military platforms.

MORA extends the scope of VICTORY by adding a low-latency transport mechanism, data streaming interfaces, new message types, management operations, and functional concepts that are specific to RF applications. A module in MORA is known as a MORA device, which provides standardized access to configurable signal and processing resources.

The parts of MORA that have been adopted at this point are limited to signal resources, which provide open interfaces to the RF Signal Layer aspects of RF chains, that emit or collect RF energy.

As MORA is an extension of VICTORY, adopting these MORA interface standards implies adoption of a subset of the VICTORY interface standards. This includes the use of Simple Object Access Protocol (SOAP) technologies and XML formatted payloads encapsulated in Transmission Control Protocol (TCP) datagrams for request-response interactions. MORA also adopts VICTORY's use of SYSLOG payloads encapsulated in User Datagram Protocol (UDP) multicast for publish-subscribe interactions for health monitoring. Additionally, MORA adds RF layer and operation interfaces that use UDP unicast and UDP multicast interactions with binary payloads.

8.3.2 Application of MORA to RF Signal Layer Modules

Figure 8.3.2-1 illustrates the interfaces contained within the RF Signal Layer modules. Note the outlined boxes within the module boxes to which the interactions connect. These are “interaction endpoints”, which group together a set of related interactions. For instance, the box labeled “MORA Device Service” indicates that the module implements the service side of a group of interactions. Interaction endpoints will be important to interpreting the rules stating requirements for the RF Signal Layer modules.

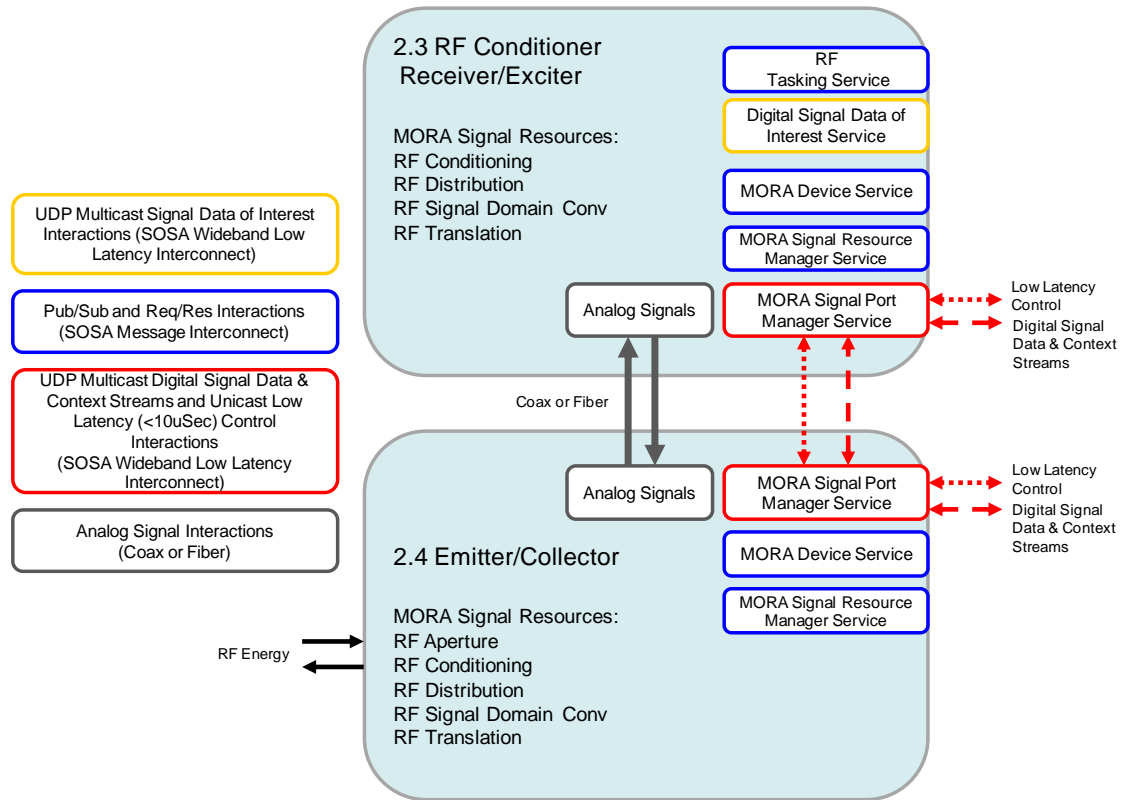


Figure 8.3.2-1: RF Signal Layer Module Interactions

8.3.3 RF Conditioner-Receiver-Exciter Module

See Section 4.2 for the definition of this module.

The Conditioner-Receiver-Exciter module, shown in Figure 8.3.3-1, performs receive tasking, transmit tasking, or both. The receive tasking could include calibration, channelization, image formation, tagging with metadata, data framing, and data cube formation. The transmit tasking could include waveform generation, calibration, and adaptation to spectrum use. The signal could be amplified, filtered, frequency translated, distributed, and signal domain converted (ADC and DAC).

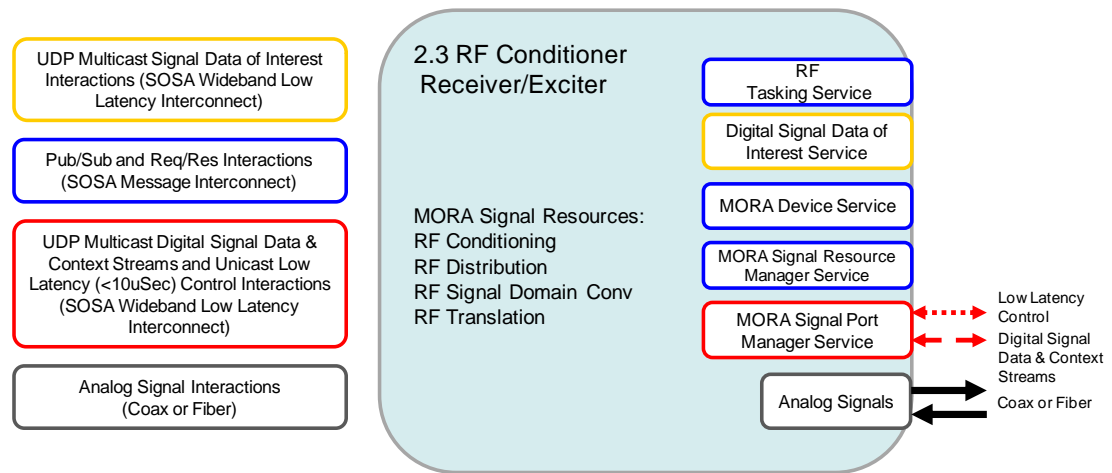


Figure 8.3.3-1: RF Conditioner Receiver/Exciter Interactions (Refer to Table 8.1-1)

The MORA Device Service is a set of interactions that support discovery, configuration, control, and health management of the module. These interactions report the health, send notifications of key events such as state changes and faults, and report BIT results. They also allow the module configuration to be managed, and its state to be controlled. For example, modules can be made to execute a BIT, reset, or the software or configuration could be updated.

The MORA Signal Resource Manager Service is a group of interactions that support management of the RF resources that support capabilities such as RF signal domain conversion, RF translation, RF conditioning, RF distribution, and RF apertures. Through these interactions the signal resource client can request information about the signal resources capability profile provided by the Conditioner-Receiver-Exciter module to determine whether the signal resources available can meet the requirements of a given task. These interactions support discovery of detailed characteristics of the Conditioner-Receiver-Exciter signal resources such as the fixed and variable parameters, the fixed and settable interconnections, and the real-time data, control, and context endpoints attached to the SOSA Wideband Low-Latency Interconnect. These interactions also support the reservation and release of signal resources by clients.

The RF Conditioner-Receiver-Exciter module exchanges RF signals with Emitter/Collector modules via analog (coax or fiber) and/or digital (binary packets over SOSA Wideband Low-Latency Interconnect) methods. Regardless of the signal data exchange methods employed, the associated context packets and control packets as well as the digital signal data packets occur via its MORA Signal Port Manager Service. The Signal Port Manager Service interactions implement low-latency control of signal resources, which are realized by MORA Data Messages (MDMs) transported on the SOSA Wideband Low-Latency Interconnect. Once resources have been reserved by a client through the MORA Signal Resource Manager Service on the SOSA Message Interconnect, the signal resources are then configured, and signal data and context streams occur via the MORA Signal Port Manager Service interactions on the SOSA Wideband Low-Latency Interconnect.

The difference between the RF Conditioner-Receiver-Exciter module, shown in Figure 8.3.3-1, *versus* the Emitter/Collector module, shown in Figure 8.3.4-1, is that the RF Conditioner-Receiver-Exciter module will not contain any RF aperture signal resource capabilities, as those signal resource functions are exclusively resident in RF Emitter/Collector modules. Additionally, the RF Conditioner-Receiver-Exciter module has an additional interface for controlling and monitoring Conditioner-Receiver-Emitter tasks.

A summary of the RF Conditioner-Receiver-Exciter module functions is shown in Table 8.3.3-1.

Table 8.3.3-1: Conditioner-Receiver-Exciter Functions

SOSA Functional Group 3	RF Conditioner-Receiver-Exciter Module Function Name	Definition	Support
Control Task	RF Receiver-Exciter Tasking Service	The action of starting, pausing, resuming, or canceling a Conditioner-Receiver-Exciter task.	V2.0
Plan Task	RF Receiver-Exciter Tasking Service	The action of negotiating a viable plan for Conditioner-Receiver-Exciter task execution.	V2.0
Monitor Task Status	RF Receiver-Exciter Tasking Service	The action of monitoring the status for a specific Conditioner-Receiver-Exciter task or tasks.	Future
Notify Result	RF Receiver-Exciter Tasking Service	The action of notifying the result of a specific Conditioner-Receiver-Exciter task.	V2.0
Generate Data of Interest	Digital Signal Data of Interest Service	The action of generating production results for a specific Conditioner-Receiver-Exciter task.	V2.0
Consume Data of Interest	Digital Signal Data of Interest Service	The action of consuming signal data of interest for a specific Conditioner-Receiver-Exciter task.	Future
Execute Calibration	RF Receiver-Exciter Tasking Service	The action of phase and amplitude calibrating the receive signal resources to achieve complex receive manifold performance.	Future
Execute Channelization	RF Receiver-Exciter Tasking Service	The action of channelizing the receive signal data to achieve the acquisition of specific data of interest.	V2.0
Execute Metadata Tagging	RF Receiver-Exciter Tasking Service	The action of tagging the receive data of interest for effective subsequent processing.	V2.0
Execute Data Framing	RF Receiver-Exciter Tasking Service	The action of framing the receive data of interest for effective subsequent processing.	Future
Execute Data Cube Formation	RF Receiver-Exciter Tasking Service	The action of forming multi-dimensional receive data of interest for subsequent processing.	V2.0

SOSA Functional Group 3	RF Conditioner-Receiver-Exciter Module Function Name	Definition	Support
Execute Adaptation	RF Receiver-Exciter Tasking Service	The action of optimizing temporal, spatial, and/or frequency aspects of transmit tasking for interoperability and/or enhanced performance.	Future
Execute Waveform Generation	RF Receiver-Exciter Tasking Service	The action of generating a transmit waveform including content, frequency, spatial, and temporal aspects.	V2.0
Manage RF Device Parameters	MORA Device Service	The action of managing the configuration, state, status, and health of the RF device.	V1.0
Manage Signal Resource Parameters	MORA Signal Resource Service	The action of reserving and releasing of signal resources.	V1.0
Provide Signal Resource Parameters	MORA Signal Resource Service	The action of providing the profile of signal resources.	V1.0
Amplify/Attenuate RF Signal	MORA Signal Port Manager Service	The action of amplifying or attenuating RF signals including LNAs, RF attenuators, and HPAs.	V1.0
Filter RF Signal	MORA Signal Port Manager Service	The action of frequency filtering of RF signals including band pass, band reject, low pass, and high pass RF filters.	V1.0
Distribute RF Signal	MORA Signal Port Manager Service	The action of distributing analog RF signals including RF switches, RF combiners, and RF splitters.	V1.0
Frequency Translate RF Signals	MORA Signal Port Manager Service	The action of frequency translating RF signals including RF down converters, RF up converters, digital down converters, and digital up converters.	V1.0
Convert Domain of RF Signals	MORA Signal Port Manager Service	The action of ADC or DAC for RF signals.	V1.0

8.3.4 RF Emitter/Collector Module

See Section 4.2 for the definition of this module.

The Emitter/Collector module, shown in Figure 8.3.4-1, is responsible for converting between EM energy and electric signals, performing receive functions, transmit functions, or both. This module could include electronic steering, beam forming, and focus control. The signal could be amplified, filtered, frequency translated, distributed, and signal domain converted (ADC and DAC).

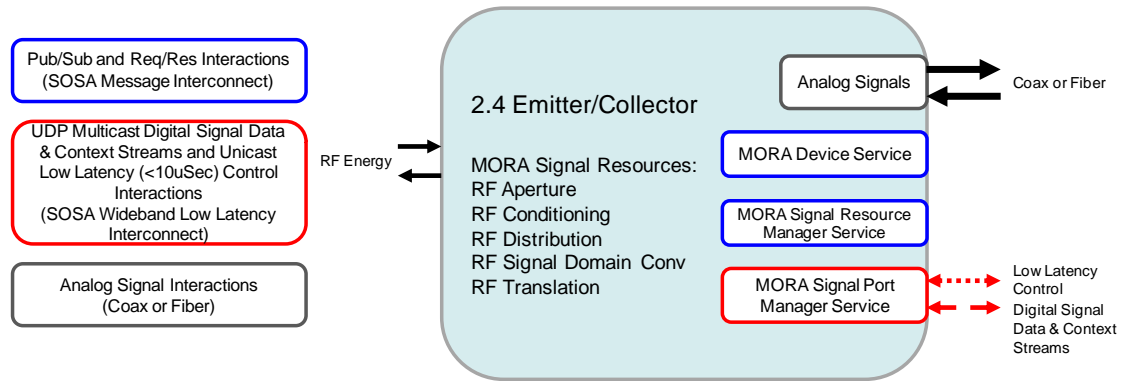


Figure 8.3.4-1: RF Emitter/Collector Interactions (Refer to Table 8.3.4-1)

The MORA Device Service interactions of this module are equivalent to those of the Conditioner-Receiver-Exciter module interfaces. The MORA Signal Resource Manager Service interactions of this module include the functionality of the Conditioner-Receiver-Exciter module as well as an additional exclusive RF capability for RF apertures.

A summary of the RF Emitter/Collector module interface definitions is shown in Table 8.3.4-1.

Table 8.3.4-1: Emitter/Collector Functions

SOSA Functional Group 3	RF Conditioner-Receiver-Exciter Module Function Name	Definition	Support
Manage RF Device Parameters	MORA Device Service	The action of managing the configuration, state, status, and health of the RF device.	V1.0
Manage Signal Resource Parameters	MORA Signal Resource Manager	The action of reserving and releasing signal resources.	V1.0
Provide Signal Resource Parameters	MORA Signal Resource Service	The action of providing the profile of signal resources.	V1.0
Collect Electromagnetic Energy	MORA Signal Port Manager Service	The action of collecting EM energy into electric signals.	V1.0
Emit Electromagnetic Energy	MORA Signal Port Manager Service	The action of emitting EM energy from electric signals.	V1.0
Amplify/Attenuate RF Signal	MORA Signal Port Manager Service	The action of amplifying or attenuating RF signals including LNAs, RF attenuators, and HPAs.	V1.0
Filter RF Signal	MORA Signal Port Manager Service	The action of frequency filtering of RF signals including band pass, band reject, low pass, and high pass RF filters.	V1.0

SOSA Functional Group 3	RF Conditioner-Receiver-Exciter Module Function Name	Definition	Support
Distribute RF Signal	MORA Signal Port Manager Service	The action of distributing analog RF signals including RF switches, RF combiners, and RF splitters.	V1.0
Frequency Translate RF Signals	MORA Signal Port Manager Service	The action of frequency translating of RF signals including RF down converters, RF up converters, digital down converters, and digital up converters.	V1.0
Convert Domain of RF Signals	MORA Signal Port Manager Service	The action of ADC or DAC for RF signals.	V1.0

The following sections describe the interactions that make up each of these interaction endpoint services, and then state the rules that are required for each of the RF Signal Layer modules.

8.3.5 RF Receiver-Exciter Interactions

Table 8.3.5-1 shows the interactions that have been defined for the RF Receiver-Exciter Tasking Service and Digital Signal Data of Interest Service.

The column headings in Table 8.3.5-1 have the following meanings:

- Interaction Name: begins with an “operation” verb
- Interaction Description: executive summary description of the Interaction Name in one phrase/sentence
- Input Objects: a comma-separated list of objects (DIV-2 or DIV-3 references)
- Output Objects: a comma-separated list of objects (DIV-2 or DIV-3 references)
- Required/Optional, Applicability: an indication of the requirement for the provider to implement this interaction and the version of the SOSA Technical Standard where this is required
- Interaction Type: Response or Multicast

Table 8.3.5-1: RF Receiver-Exciter Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
executeREXActionControl	The action of starting, pausing, resuming, or canceling a Conditioner-Receiver-Exciter task.	REXActionControl	REXActionResult	Required	Response

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
notifyREXActionResult	The action of notifying the result of a specific Conditioner-Receiver-Exciter task.	REXActionResult		Required	Multicast
sendDigitalReceiveData	The action of generating production results for a specific Conditioner-Receiver-Exciter task.	DigitalReceiveData		Required based on modality mode specific	Multicast
validateREXActionPlan	The action of negotiating a viable plan for Conditioner-Receiver-Exciter task execution.	REXActionPlan	REXActionPlanResponse	Required	Response

8.3.6 RF Receiver-Exciter Rules

Rule 8.3.6-1: RF Receiver-Exciter implementations of module 2.3 shall execute interactions defined in Table 8.3.4-1 that comply with definitions in the MORA Specification. Conformance Methodology (T)

8.3.7 RF Signal Layer Interactions

Table 8.3.7-1 shows the interactions that have been defined for the three endpoint services required for RF Signal Layer modules, which include the 2.3 Conditioner-Receiver-Exciter and 2.4 Emitter/Collector modules. The source of these interaction definitions is the MORA Specification. Optional interactions are denoted with an * at the end of the interaction name. Some MORA UDP unicast interactions conducted over the SOSA Wideband Low-Latency Interconnect (denoted with **) could utilize an optional receipt acknowledge request. Some MORA UDP unicast interactions conducted over the SOSA Wideband Low-Latency Interconnect (denoted with ***) could utilize an optional receipt acknowledge request and/or optional VRT validation acknowledge request.

Notes

To reiterate, in Table 8.3.7-1, the following notation is used:

- * denotes an optional interaction
- ** denotes UDP unicast with an available optional receipt acknowledge request
- *** denotes UDP unicast with an available optional receipt acknowledge request and/or optional VRT validation acknowledge request

Table 8.3.7-1: RF Signal Layer Interactions

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Device	getDeviceDescription	Request Response		“MORA Device”	V1.0
MORA Device	getDeviceStatus	Request Response		“Device Status”	V1.0
MORA Device	getFileList	Request Response	“File Type”	List of “MORA File”, OUT_OF_RANGE Error	V1.0
MORA Device	pullFile	Request Response	“File Name”	“MORA File”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	pushFile	Request Response	“MORA File”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	deleteFile	Request Response	“File Name”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	getAvailableMoraConfigurations	Request Response		List of “MORA Configuration”	V1.0
MORA Device	getCurrentMoraConfiguration	Request Response		“MORA Configuration ID”	V1.0
MORA Device	setCurrentMoraConfiguration	Request Response	“MORA Configuration ID”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	runBuiltInTest	Request Response		NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Device	getBuiltInTestResults	Request Response		List of “Built-In Test Result”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	sendCommand	Request Response	OPERATE, STANDBY, TRANSMIT_INHI BIT, POWER_ON, SHUT_DOWN, RESTART, MAINTENANCE_ MODE, ZEROIZE, SANITIZE	NO_ERROR, GENERIC_FAULT Error, NOT_SUPPORTED Error, OUT_OF_RANGE Error	V1.0
MORA Device	getAvailableWaveforms*	Request Response		List of “Waveform”	V1.0
MORA Device	getAvailableWaveformOperations*	Request Response		List of “Waveform Operation”	V1.0
MORA Device	getCurrentWaveformOperation*	Request Response		“Waveform Operation ID”, GENERIC_FAULT Error	V1.0
MORA Device	setCurrentWaveformOperation*	Request Response	“Waveform Operation ID”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device	getManufacturer	Request Response		Manufacturer	V1.0
MORA Device	getModel	Request Response		Model	V1.0
MORA Device	getEquipmentId	Request Response		Equipment ID	V1.0
MORA Device	getGenericEndNodeEthernetInterfaces	Request Response		List of “Ethernet Interface”	V1.0
MORA Device	getGenericEndNodeDhcpEnabled	Request Response	“Unique Name”	“DHCP Enabled”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Device	getGenericEndNodeHostName	Request Response		“Hostname”	V1.0
MORA Device	setGenericEndNodeHostName	Request Response	“Hostname”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device	getGenericEndNodeDateTime	Request Response		“Date Time”	V1.0
MORA Device	setGenericEndNodeDateTime	Request Response	“Date Time”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device	getGenericEndNodeAutodiscoveryEnabled	Request Response		“Enabled”, NOT_SUPPORTED Error	V1.0
MORA Device	setGenericEndNodeAutodiscoveryEnabled	Request Response	“Enabled”	NO_ERROR, NOT_SUPPORTED Error	V1.0
MORA Device	getGenericEndNodeDisplayBlackoutEnabled	Request Response		“Enabled”, NOT_SUPPORTED Error	V1.0
MORA Device	setGenericEndNodeDisplayBlackoutEnabled	Request Response	“Enabled”	NO_ERROR, NOT_SUPPORTED Error	V1.0
MORA Device	restartGenericEndNode	Request Response		NO_ERROR	V1.0
MORA Device	standbyGenericEndNode	Request Response		NO_ERROR	V1.0
MORA Device	purgeGenericEndNode	Request Response		NO_ERROR, NOT_SUPPORTED Error	V1.0
MORA Signal Resource Manager	getSignalPorts	Request Response		List of “Signal Port”	V1.0
MORA Signal Resource Manager	reserveSignalPort	Request Response	“Signal Port ID”, List of “MORA Transport Configuration”	“Reservation Confirmation”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Signal Resource Manager	releaseSignalPort	Request Response	“Reservation Confirmation”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Signal Resource Manager	getSignalPortReservations	Request Response		List of “Signal Port Reservation”	V1.0
MORA Signal Resource Manager	getSignalPortDescription	Request Response	“Signal Port ID”	“Signal Port Description”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Signal Resource Manager	getSignalPortDefaultPerformanceData	Request Response	“Signal Port ID”	“Port Default Performance Data”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Signal Resource Manager	getStaticExternalConnectionMap	Request Response		List of “External Connection”	V1.0
MORA Signal Resource Manager	getStaticInternalConnectionMap	Request Response		List of “Connection”	V1.0
MORA Signal Resource Manager	getInternalReferenceConnections	Request Response		List of “Reference Connection”	V1.0
MORA Signal Resource Manager	getAntennaArrays	Request Response		List of “Antenna Array”	V1.0
MORA Signal Resource Manager	getManifoldBands	Request Response		List of “Manifold Band”	V1.0
MORA Signal Resource Manager	getSwitchGroups*	Request Response		List of “Switch Group”	V1.0
MORA Signal Resource Manager	reserveSwitchGroup*	Request Response	“Switch Group ID”, List of “MORA Transport Configuration”	“Reservation Confirmation”, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Signal Resource Manager	releaseSwitchGroup*	Request Response	“Reservation Confirmation”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Signal Resource Manager	getSwitchGroupReservations*	Request Response		List of “Switch Group Reservation”	V1.0
MORA Device & MORA Signal Resource Manager	getAuthenticationService*	Request Response		“Authentication Service URI”, GENERIC_FAULT Error	V1.0
MORA Device & MORA Signal Resource Manager	setAuthenticationService*	Request Response	“Authentication Service URI”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getPolicyEnforcementService*	Request Response		“Policy Enforcement Service URI”, GENERIC_FAULT Error	V1.0
MORA Device & MORA Signal Resource Manager	setPolicyEnforcementService*	Request Response	“Policy Enforcement Service URI”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getHealthDataTransportConfigurations	Request Response		List of "Data Transport Configuration"	V1.0
MORA Device & MORA Signal Resource Manager	setHealthDataTransportConfigurations	Request Response	List of “Data Transport Configuration”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	addHealthDataTransportConfiguration	Request Response	“Data Transport Configuration”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Device & MORA Signal Resource Manager	removeHealthDataTransportConfiguration	Request Response	“Data Transport Configuration Unique Name”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getFaultUpdatePeriod	Request Response		“Update Period”	V1.0
MORA Device & MORA Signal Resource Manager	setFaultUpdatePeriod	Request Response	“Update Period”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getStatusUpdatePeriod	Request Response		“Update Period”	V1.0
MORA Device & MORA Signal Resource Manager	setStatusUpdatePeriod	Request Response	“Update Period”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getEnabledFaultSeverity Levels	Request Response		List of “Severity Level”	V1.0
MORA Device & MORA Signal Resource Manager	enableFaultSeverityLevel	Request Response	“Severity Level”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	disableFaultSeverityLevel	Request Response	“Severity Level”	NO_ERROR, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getStatusEnabled	Request Response		“Enabled”	V1.0
MORA Device & MORA Signal Resource Manager	setStatusEnabled	Request Response	“Enabled”	NO_ERROR	V1.0
MORA Device & MORA Signal Resource Manager	getAcknowledgedFaults	Request Response		List of “Fault”	V1.0
MORA Device & MORA Signal Resource Manager	acknowledgeFault	Request Response	“Fault ID”, “Origin”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Device & MORA Signal Resource Manager	resumeFault	Request Response	“Fault ID”, “Origin”	NO_ERROR, GENERIC_FAULT Error, OUT_OF_RANGE Error	V1.0
MORA Device & MORA Signal Resource Manager	getActiveFaults	Request Response		List of “Fault”	V1.0
MORA Device & MORA Signal Resource Manager	getInterfaceType	Request Response		“Interface Type”	V1.0
MORA Device & MORA Signal Resource Manager	getInterfaceStandardVersion	Request Response		“Interface Standard Version”	V1.0
MORA Device & MORA Signal Resource Manager	getInterfaceSoapComponents	Request Response		List of “SOAP Component”	V1.0
MORA Device & MORA Signal Resource Manager	Fault Message	Publish Subscribe		PRI, Version, Timestamp, Hostname, App- Name, PROCID, MSGID, SD-ID, SD- PARAM, MSG	V1.0
MORA Device & MORA Signal Resource Manager	Status Message	Publish Subscribe		PRI, Version, Timestamp, Hostname, App- Name, PROCID, MSGID, SD-ID, SD- PARAM, MSG	V1.0
MORA Signal Port Manager	MDM Type 1 VRT Command Packet	UDP Unicast***	See MORA 48610	See MORA 48610	V1.0
MORA Signal Port Manager	MDM Type 1 VRT Context Packet	UDP Multicast	See MORA 48609	See MORA 48609	V1.0
MORA Signal Port Manager	MDM Type 1 VRT Signal Data Packet	UDP Multicast	See MORA 48608	See MORA 48608	V1.0
MORA Signal Port Manager	MDM Type 2 Acknowledgement	UDP Unicast	See MORA 48611	See MORA 48611	V1.0
MORA Signal Port Manager	MDM Type 3 Time of Day	UDP Unicast**	See MORA 48612	See MORA 48612	V1.0

RF Signal Layer Service Name	RF Signal Layer Interaction Name	Interaction Type	Input Object	Output Object	Support
MORA Signal Port Manager	MDM Type 4 Signal Port User ID	UDP Unicast**	See MORA 48613	See MORA 48613	V1.0
MORA Signal Port Manager	MDM Type 5 Health	UDP Unicast**	See MORA 48614	See MORA 48614	V1.0
MORA Signal Port Manager	MDM Type 6 Command	UDP Unicast**	See MORA 48615	See MORA 48615	V1.0
MORA Signal Port Manager	MDM Type 7 Switch Group User ID	UDP Unicast**	See MORA 48617	See MORA 48617	V1.0

8.3.8 RF Signal Layer Module Rules

Rule 8.3.8-1: RF implementations of modules 2.3 and 2.4 shall comply with the appropriate MORA Specifications, as shown below. The following documents provide the complete, detailed specifications referenced in this section:

- MORA Specification, Version 2.4 (see [Referenced Documents](#)):
 - Distribution A: Main body and Appendices A-D
 - Distribution C: Appendices E-G
- VICTORY Standard Specifications, Version 1.9 (see [Referenced Documents](#)):
 - Distribution A: Main body
 - Distribution C and/or ITAR: Appendices
- ANSI/VITA 49.2 (see [Referenced Documents](#))

Each bullet item in the rules below uniquely specifies a section of the MORA Specification adopted by the SOSA Consortium for the SOSA Technical Architecture.

Rule 8.3.8-2: A component implementing RF Signal Resources in the SOSA 2.3 RF Conditioner-Receiver-Exciter module shall be compliant with the following MORA Specifications: Conformance Methodology (T)

- MORA Device Service: MORA Device Component Type MT92010-V2.4
- MORA Signal Resource Manager Service: MORA Signal Resource Manager Component Type MT92013-V2.4
- MORA Signal Port Manager Service: MORA Signal Port Manager Component Type MT92016-V2.4

Rule 8.3.8-3: A component implementing RF Signal Resources in the SOSA 2.4 RF Emitter/Collector module shall be compliant with the following MORA Specifications: Conformance Methodology (T)

- MORA Device Service: MORA Device Component Type MT92010-V2.4

- MORA Signal Resource Manager Service: MORA Signal Resource Manager Component Type MT92013-V2.4
- MORA Signal Port Manager Service: MORA Signal Port Manager Component Type MT92016-V2.4

8.4 EO/IR Definitions

Interaction definitions for EO/IR sensor types in these modules will be added in a future version of this document. The current version of this document specifies the requirements for the transmission/reception modules when operating on RF signals in EW, Radar, and SIGINT modalities.

9 Process Signals/Targets

Process Signals/Targets is the set of functionalities required to take raw collected RF data and detect, extract, track, or produce imagery for downstream processing. In the current version of this document, the SOSA Process Signals/Targets interaction definitions are focused on three RF sensor threads: SAR, EW, and SIGINT. In particular, no object detection, classification, or tracking is considered under the SAR sensor thread; only offensive EA barrage jamming is considered for EW; and only survey is considered for SIGINT (no direction-finding).

The functions are provided by four SOSA modules under the Process Signal/Targets functionality; Signal/Object Detector & Extractor (module 3.1), Signal/Object Characterizer (module 3.2), Image Pre-Processor (module 3.3), and Tracker (module 3.4). Interaction definitions associated with the Tracker module (module 3.4) will be added in a future version when tracker functionality is considered. The following sections define the functional decomposition, interactions, and rules that apply to these modules.

9.1 Signal/Object Detector & Extractor

The Signal/Object Detector & Extractor module provides the initial detection of known signal types from the RF input data. This detection would determine demodulation results and other measurements regarding the input signal. Detected signals would be extracted by this module and passed on for further processing.

The high-level description of the Signal/Object Detector & Extractor module is provided in Table 9.1-1, which provides a detailed functional decomposition for this module.

Table 9.1-1: SOSA SvcV-1: Module Descriptions

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Manage Detection Processing Task	Process Signal Detection Tasking Request	The action of determining the processing based on the mission product of interest.
Execute Mission Operations	Execute Detection Processing Tasking	Extract Signal of Interest	The action of processing raw data and detecting a signal of interest, including clutter suppression, detection thresholding, etc.
Execute Mission Operations	Execute Detection Processing Tasking	Disseminate Detection Products	The action of disseminating the detection products for further processing or providing product of interest to reporting services.

9.1.1 Signal/Object Detector & Extractor Interactions

Table 9.1.1-1 shows the interactions that have been defined for the Signal/Object Detector & Extractor module based on the three RF sensor threads considered under the current version of this document.

Table 9.1.1-1: Signal/Object Detector & Extractor Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
sendDetectionProducts	The action of publishing products for a specific detection task.	DetectionProducts		Required	Multicast
sendModuleTaskResult	The action of informing the execution results of a task request.	ModuleTaskResult		Required	Unicast

9.1.2 Signal/Object Detector & Extractor Interaction Rules

The following rules apply to the interactions for the Signal/Object Detector & Extractor module defined in Section 9.1.1.

Observation 9.1.2-1: Until the Storage and Retrieval module is defined, the Signal/Object Detector & Extractor module might provide data product storage and retrieval to support any data product queries.

Rule 9.1.2-1: The SOSA Signal/Object Detector & Extractor module shall implement all required interactions defined in Table 9.1.1-1. Conformance Methodology (T)

9.2 Signal/Object Characterizer

The high-level description of the Signal/Object Characterizer module is provided in Table 9.2-1, which provides a detailed functional decomposition for this module.

Table 9.2-1: SOSA SvcV-1 – Module Descriptions

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Manage Signal Characterization Processing Task	Process Signal Characterization Tasking Request	The action of determining the processing based on the mission product of interest.
Execute Mission Operations	Execute Signal Characterization Processing Tasking	Extract Detection Features	The action of extracting detection features from a detected signal.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Execute Mission Operations	ExecuteSignal Characterization Processing Tasking	Estimate Signal Parameters	The action of estimating signal parameters of a detected signal.
Execute Mission Operations	Execute Signal Characterization Processing Tasking	Disseminate Characterization Products	The action of disseminating the characterization products for further processing or providing products of interest to reporting services.

9.2.1 Signal/Object Characterizer Interactions

Table 9.2.1-1 shows the interactions that have been defined for the Signal/Object Characterizer module based on the three RF sensor threads considered under the current version of this document.

Table 9.2.1-1: Signal/Object Characterizer Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
sendCharacterizationProducts	The action of publishing products for a characterization task.	CharacterizationProducts		Required	Multicast
sendModuleTaskResult	The action of informing the execution results of a task request.	ModuleTaskResult		Required	Unicast

9.2.2 Signal/Object Characterizer Interaction Rules

The following rules apply to the interactions for the Signal/Object Characterizer module defined in Section 9.2.1.

Observation 9.2.2-1: Until the Storage and Retrieval module is defined, the Signal/Object Characterizer module might provide data product storage and retrieval to support any data product queries.

Rule 9.2.2-1: The SOSA Signal/Object Characterizer module shall implement all required interactions defined in Table 9.2.1-1. Conformance Methodology (T)

9.3 Image Pre-Processor

SAR processes data into an image of the ground, thereby synthesizing an aperture the length of the aircraft flight path. The Image Pre-Processor module produces the images based on the received RF data.

The high-level description of the Image Pre-Processor module is provided in Table 9.3-1, which provides a detailed functional decomposition for this module.

Table 9.3-1: SOSA SvcV-4 – Image Pre-Processor

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Manage Image Processing Task	Process Image Tasking Request	The action of determining the processing required based on the mission product of interest.
Execute Mission Operations	Execute Image Processing Task	Form Image from Raw Data	The action of forming an image from raw data.
Execute Mission Operations	Execute Image Processing Task	Perform Motion Compensation	The action of compensating for the down-range and cross-range motion of the platform/sensor to provide high-precision image formation.
Execute Mission Operations	Execute Image Processing Task	Georegister Imagery	The action of registering the image to geographical coordinates.
Execute Mission Operations	Execute Image Processing Task	Disseminate Imagery Product	The action of disseminating the imagery product for further processing or providing the product of interest to reporting services.

9.3.1 Image Pre-Processor Interactions

Table 9.3.1-1 shows the interactions that have been defined for the Image Pre-Processor module based on the three RF sensor threads considered under the current version of this document.

Table 9.3.1-1: Image Pre-Processor Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
sendImageProducts	The action of publishing products for a specific image task.	ImageData		Required	Multicast
sendModuleTaskResult	The action of informing the execution results of a task request.	ModuleTaskResult		Required	Unicast

9.3.2 Image Pre-Processor Interaction Rules

The following rules apply to the interactions for the Image Pre-Processor module defined in Section 9.3.1.

Observation 9.3.2-1: Until Storage and Retrieval module is defined, the Image Pre-Processor module might provide data product storage and retrieval to support any data product queries.

Rule 9.3.2-1: The SOSA Image Pre-Processor module shall implement all required interactions defined in Table 9.3.1-1.

9.4 Tracker

This module will be described in a future version.

10 Analyze and Exploit

10.1 External Data Ingestor

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 10.1-1: SOSA SvcV-4 – External Data Ingestor

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
4 Analyze/Exploit			
4.1 External Data Ingestor	Ingest data from other SOSA sensors or other sources	SOSA Mission Data	(Data products output by module 5.1)
	Convert from external formats to SOSA format	SOSA Non-conformant Data	(Including sensor/source)
	Distribute the ingested data to other SOSA modules as appropriate	SOSA Mission Data	
	Enable fusion or correlation across sensors		

10.2 Encoded Data Extractor

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 10.2-1: SOSA SvcV-4 – Encoded Data Extractor

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
4 Analyze/Exploit			
4.2 Encoded Data Extractor	Extract internals	Detection	
	Extract message content from signal	Extracted Electromagnetic Signal Stream	(Digital only)
	Demodulate	Extracted Image or Stream	(Digital only)

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
	Perform human language processing	Encoded Data Extractor Assignment	
		<i>A Priori</i> Target Properties	
		Demodulated Electromagnetic Signal Stream	
		Extracted Data	

10.3 Situation Assessor

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 10.3-1: SOSA SvcV-4 – Situation Assessor

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
4 Analyze/Exploit			
4.3 Situation Assessor	Correlate same signal/object from multiple sensors	Characterization	
	Associate multiple signals/objects	Track	
	Develop and store history of detections and correlations over time	Detection	Of signals/objects
		Association	Among signals/objects
		Situation Assessor Data	
		Situation Assessor Assignment	
		Assessed Situation	
		Association	Among signals/objects

10.4 Impact Assessor & Responder

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 10.4-1: SOSA SvcV-4 – Impact Assessor & Responder

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
4 Analyze/Exploit			
4.4 Impact Assessor & Responder	Determine entity affiliation	Demodulated Electromagnetic Signal Stream	
	Assess impacts, threats, and vulnerabilities	Detection	Of signals/objects
	Maintain alternate hypotheses	Track	
	Project assessments into the future	Characterization	
	Analyze response and send request	Extracted Data	
		Association	Among signals/objects
		Impact Assessor Data	
		Impact Assessor & Responder Assignment	
		Assessed Impact	
		Assessed Impact Response	

10.5 Storage/Retrieval Manager

The Storage/Retrieval Manager module provides the capability to manage data storage within a SOSA system. The Storage/Retrieval Manager module rules are defined in alignment with Data-At-Rest Encryption (DARE) Encryptor/Decryptor module rules specified in Section 12.1.7.

Rule 10.5-1: The SOSA Storage/Retrieval Manager module shall provide the following protocols for an upstream data provider, where upstream is defined as an endpoint at the origination of the link. Conformance Methodology (D)

- Network File System (NFS)-based file storage capability over Ethernet
- Non-Volatile Memory Express (NVMe) over Fabric (NVMe-oF) via Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE), Version 2

Rule 10.5-2: A SOSA Storage/Retrieval Manager module shall interface with downstream storage device(s) using NVMe. Conformance Methodology (D)

Rule 10.5-3: The SOSA Storage/Retrieval Manager module shall store data of different security associations/need-to-know into storage device encrypted with the associated key. Conformance Methodology (D)

Rule 10.5-4: The SOSA Storage/Retrieval Manager module shall run a Preboot Execution Environment (PXE) server for internal SOSA PICs. Conformance Methodology (I)

Rule 10.5-5: Where remote boot-up capability is required for a SOSA RTE, the PIC shall boot the RTE via the PXE server instantiated by the SOSA Storage/Retrieval Manager module. Conformance Methodology (D)

Rule 10.5-6: NVMe commands shall use NVMe v1.2 or later.

Table 10.5-1: SOSA SvcV-4 – Storage/Retrieval Manager

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
4 Analyze/Exploit			
4.6 Storage/Retrieval Manager	Capture real-time streaming data	Electromagnetic Signal Stream	(Digital only)
	Retrieve	Image Stream	(Digital only)
	Play back in real-time	Detection	
	Index	Track	
	Store media	Characterization	
		Association	
		Assessed Situation	
		Assessed Impact	
		Storage/Retrieval Manager Assignment	
		Electromagnetic Signal Stream	(Digital only)
		Image Stream	(Digital only)
		Detection	
		Characterization	
		Association	
		Assessed Situation	
	Assessed Impact		

11 Convey

Convey is the set of functionalities required to generate and disseminate reports. The functions are provided by one SOSA module under the Convey functionality; Reporting Services (module 5.1). The following sections define the functional decomposition, interactions, and rules that apply to the module.

11.1 Reporting Services

The high-level description of the Reporting Services module is provided in Table 11.2-1.

Table 11.1-1: SvcV-1 – Module Descriptions

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Execute Mission Operations	Disseminate Formatted Mission Products	Filter Data for dissemination	The action of filtering/selecting data based on mission task request for dissemination.
Execute Mission Operations	Disseminate Formatted Mission Products	Format data for dissemination	The action of formatting data to requested format for dissemination.
Execute Mission Operations	Disseminate Formatted Mission Products	Disseminate Requested Mission Products	The action of disseminating requested mission products to the Host Platform Interface.

11.2 Reporting Services Interactions

Table 11.2-1 shows interactions that have been defined for the Reporting Services module based on the three RF sensor threads considered under the current version of this document.

Table 11.2-1: Reporting Services Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
sendMissionProduct	The action of publishing a final formatted product for a mission task request.	MissionProduct		Required	Multicast

12 Support System Operation

12.1 Security Services Module

12.1.1 Definition

See Section 4.2 for the definition of this module.

12.1.2 Audit Subsystem

12.1.2.1 Definitions

Table 12.1.2.1-1: Identifies and Defines Terms Specific to the Audit Subsystem

Term	Definition
SYSLOG	A standard for logging events, defined by IETF RFC 5424 (March 2009).
Collector	A recipient of audit events that stores and/or processes those audit events.
Relay	A filter that processes an incoming audit event. The Relay could forward the event to other relays or collectors, or it could drop the event as a function of relay policies, which could be a function of other factors.
Audit Event	An event generated by a SOSA module that provides information that could be logged.

12.1.2.2 Introduction

This document defines an audit subsystem as part of the SOSA Security Services module for the purpose of logging events (referred to as audit events) generated by itself and other SOSA modules. The audit subsystem allows for centralized processing and storage of log data sourced from multiple SOSA modules within a SOSA sensor system. The predominant standard in the industry is SYSLOG. This document will leverage the SYSLOG standard for representing audit events, and as a model for transmitting, filtering, and storing audit events.

Audit events are routed within the audit subsystem using Relay modules. Each Relay module contains a set of rules that determine where incoming audit events will be sent, and whether the audit events are forwarded or discarded. Audit events are sent from Relay modules to other Relay modules, and from Relay modules to Collector modules. Figure 12.1.2.2-1 depicts a notional sensor subsystem that contains multiple Relay modules and Collector modules. SOSA modules could use the audit subsystem to log events that could give insight into security-relevant activities. Audit events can be analyzed collectively to determine malicious activity by observing activity within a single module and activity occurring between modules. Examples of tools that consume audit events are Intrusion Detection Systems (IDSs) and System Information and Event

Managers (SIEMs). Such functions could be present within a SOSA sensor system or could be present on a network that has access to the SOSA sensor system.

SOSA modules submit audit events to the audit subsystem within the SOSA Security Services module by sending SYSLOG-formatted messages to the audit subsystem.

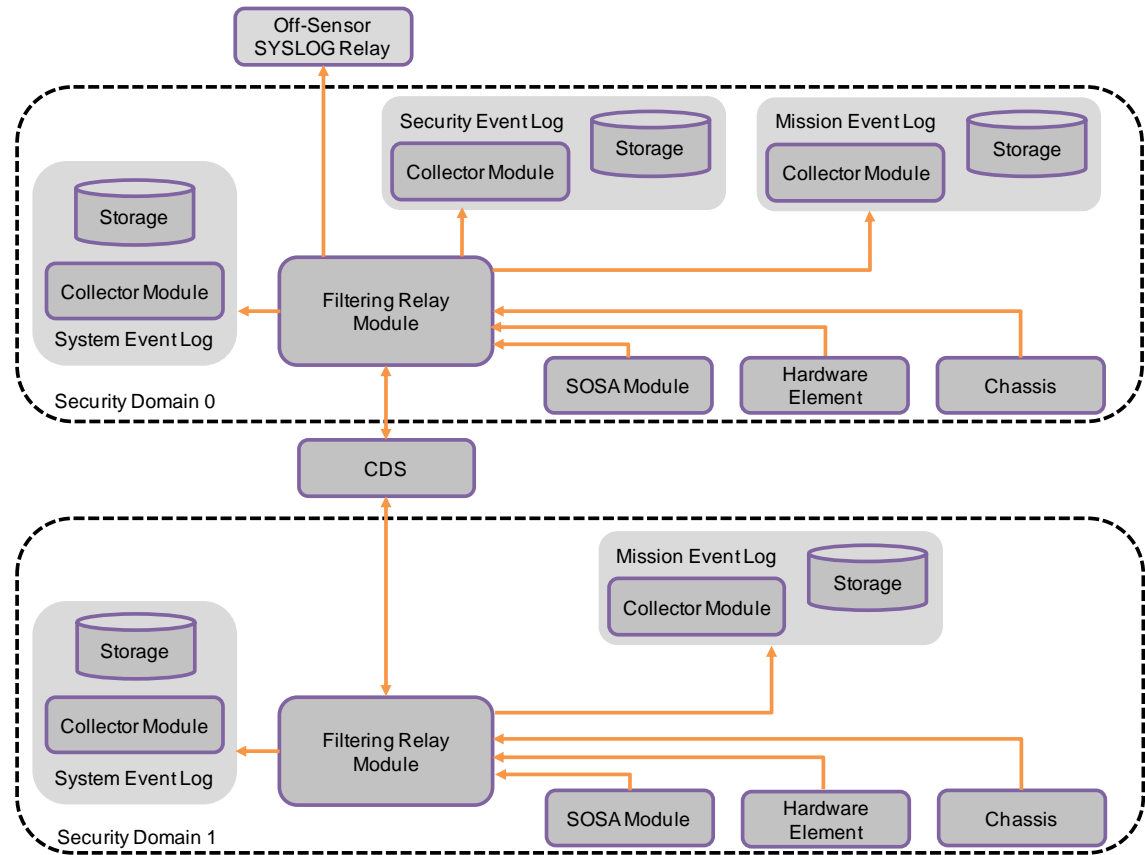


Figure 12.1.2.2-1: Sample of Audit Subsystem Configuration within a SOSA Security Services Module

12.1.2.3 Audit Subsystem Interface and Subsystem Definition

Rule 12.1.2.3-1: The SOSA Security Services module shall provide an interface to submit audit events that accepts SYSLOG-formatted messages compliant to IETF RFC 5424 (March 2009) §6 and Errata. Conformance Methodology (D)

Permission 12.1.2.3-1: When SOSA modules have events to log, SOSA modules may submit audit events as SYSLOG-formatted messages compliant to IETF RFC 5424 (March 2009) §6 and Errata to the SOSA Security Services module.

It is recommended that SOSA modules utilize secure sessions when submitting audit events. It is also noted that there could be times when SOSA modules are unable to establish a secure session due to cryptographic or other reasons, and thus a module could need to submit audit events without the protections provided by a secure channel. The use of different transports could impact the level of trust granted to audit events submitted without the use of a secure channel, although both types are useful.

Permission 12.1.2.3-2: When submitting audit events, SOSA modules may submit those audit events to the SOSA Security Services module using secure channels.

The SYSLOG standard requires the use of Coordinated Universal Time (UTC) as a format for logging time. However, there may be times when UTC is unknown (for example, during start-up). When SOSA modules can provide UTC, UTC should be used. When UTC is not available, a module may only have locally defined or system uptime available as a time reference.

Rule 12.1.2.3-2: While UTC is available, when submitting audit events, SOSA modules shall provide UTC in audit events. Conformance Methodology (D)

Rule 12.1.2.3-3: While UTC is not available, when submitting audit events, SOSA modules shall include uptime in audit events. Conformance Methodology (D)

Permission 12.1.2.3-3: When submitting audit events, SOSA modules may include both UTC and uptime in the content of audit events.

12.1.2.4 *Audit Subsystem Composition*

A logging system requires at least one log repository that stores log data. As noted below, there could be more than one, but all sensors should be capable of logging data.

Rule 12.1.2.4-1: The SOSA Security Services module shall provide at least one Collector module that receives audit events from other SOSA modules. Conformance Methodology (I)

Rule 12.1.2.4-2: The SOSA Security Services module shall provide at least one Relay module that allows users to determine which audit events to log. Conformance Methodology (I)

A SOSA sensor system could contain more than one Collector module. The different modules could receive data that is sent to it from Relay modules. The data could be sorted based on data type (mission-specific logs, sensor diagnostics and system logs, security logs) or data sensitivity (i.e., classification level).

Permission 12.1.2.4-1: The SOSA Security Services module may provide additional Collector modules.

Permission 12.1.2.4-2: The SOSA Security Services module may provide additional Relay modules.

A SOSA sensor system may be implemented over more than one security domain of the same security classification level or via a Cross-Domain Solution (CDS) for interfacing with different security classification levels. Each security domain may implement an interface for the sensor (via a CDS if necessary) to submit log information.

Permission 12.1.2.4-3: The SOSA Security Services module may implement multiple interfaces to store events located in different security domains.

12.1.2.5 *Auditable Events*

A sensor has an expectation that certain audit events will be recorded. Those audit events are summarized in this section. To process submitted audit rules, the audit events should have unique identifiers that are used to refer to audit event types.

Permission 12.1.2.5-1: The SOSA Security Services module may generate real-time alerts in the event of an audit processing failure.

Rule 12.1.2.5-1: When any of the following events occur, the SOSA Security Services module shall submit audit events describing that event. Conformance Methodology (D)

- Audit subsystem starts up
- Audit subsystem shuts down
- Audit subsystem restarts
- Zeroization requests
- Zeroization events
- Changes to Relay module settings and policies
- Changes to Collector module settings and policies

Permission 12.1.2.5-2: When any of the following events occur, the SOSA Security Services module may submit audit events describing that event.

- Critical failures
- Maintenance operations to Security Services modules while module is active
- Power-on, periodic, and on-demand Built-In Self Test (BIST) failures
- Power-on, periodic, and on-demand BIST passes
- Maintenance operations to Security Services modules while module is active
- Privileged operations such as key store insertion, retrieval, and configuration changes
- The SOSA Security Services module determines the initial NVMRO state
- NVMRO state changes

12.1.2.6 *Off-Sensor Log Forwarding and Sensor-to-Sensor Logging*

A SOSA sensor system could forward logging events to other SOSA sensor systems or other SYSLOG-compatible Relay modules and Collector modules (such as an off-sensor SIEM or another SOSA sensor system). This could be done for the purposes of intrusion or error detection, or to aggregate logging in a centralized logging repository within the next level of aggregation.

Permission 12.1.2.6-1: When the SOSA Security Services module receives audit events, the SOSA Security Services module may forward those audit events to other SYSLOG-compatible Relay modules and Collector modules that are outside the SOSA Security Services module.

12.1.3 **Key Management Service**

Key management is an essential part of any system. Keys must be generated, stored, and distributed securely to prevent inadvertent disclosure of the key and the data that the key protects. The approach will be consistent with NIST SP 800-57: Recommendation for Key Management (see [Referenced Documents](#)).

Keys within a SOSA sensor can be divided into four categories:

- Keys used to decrypt or authenticate software/firmware resident on a PIC
- Keys used to decrypt or authenticate SOSA software components
- Keys controlled by the National Security Agency (NSA) or other agencies
- Keys ephemerally generated and used when the sensor is operational

Keys for resident software/firmware will be managed by the PIC where the software/firmware resides. Keys controlled by NSA or other agencies will be managed within their associated PICs (e.g., the PIC instantiating the Encrypt/Decrypt module 6.2), where the Security Services module can support the distribution and loading of such keys. SOSA module software keys can be managed by the Security Services module. Ephemeral keys are managed by its associated Encrypt/Decrypt module, or by the Security Services module.

Rule 12.1.3-1: The SOSA Security Services module shall use DS-101 per the EKMS 308 standard or Key Management Infrastructure (KMI) Over-the-Network Key (OTNK) key delivery to load cryptographic keys. Conformance Methodology (D)

Rule 12.1.3-2: When a zeroization request is received, the SOSA Security Services module shall zeroize cryptographic key(s) specified by the authenticated requestor. Conformance Methodology (D)

Observation 12.1.3-1: Zeroization can be applied to keys directly managed by the Security Services module, or by an associated Encrypt/Decrypt module. This will depend on the security architecture of the target system. The allowable levels of zeroization to be supported by the Security Services module will vary by mission authority.

Rule 12.1.3-3: When a key inventory request is received, the SOSA Security Services module shall provide inventory status of stored cryptographic key(s) to an authenticated requestor. Conformance Methodology (D)

Rule 12.1.3-4: The SOSA Security Services module shall provide a key tag in accordance with EKMS or KMI associated with stored cryptographic key(s) as a response to a key inventory status request. Conformance Methodology (D)

Rule 12.1.3-5: When a key request is received, the SOSA Security Services module shall provide cryptographic key(s) to an authenticated requestor. Conformance Methodology (D)

Rule 12.1.3-6: When a SOSA Encrypt/Decrypt module configuration request is received, the SOSA Security Services module shall configure the SOSA Encrypt/Decrypt module(s) (module 6.2) for cryptographic key association. Conformance Methodology (D)

Rule 12.1.3-7: When a key distribution request is received, the SOSA Security Services module shall distribute cryptographic key(s) to module(s) specified by an authenticated requestor. Conformance Methodology (D)

Rule 12.1.3-8: When a key store request is received, the SOSA Security Services module shall store cryptographic key(s). Conformance Methodology (D)

Observation 12.1.3-2: Note that this is different than key loading because this assumes the key has been loaded into the sensor system. This is strictly for inter-module exchange, where key loading involves receiving the key from an external entity.

Rule 12.1.3-9: Cryptographic material shall be stored in SOSA Security Services modules that are certified to handle data at the associated classification level. Conformance Methodology (I)

Observation 12.1.3-3: The rule assumes the hardware element that hosts the SOSA Security Services module under conformance evaluation have been certified by the appropriate certification authority to handle classified key material at its associated classification level.

Table 12.1.3-1: Key Management Interactions

Interaction Name	Interaction Description	Input Object	Output Object	Required/Optional, Applicability
LoadKey	Facilitate loading of cryptographic key via DS101 interface.	* Cryptographic key or key package; varied by systems	N/A (status on the key(s) loaded are requested via GetKeyInventory interaction)	Required, V1.0
StoreKey	Facilitate loading of cryptographic key via KMI or other OTNK protocol.	* Cryptographic key or key package; varied by systems	numKeyReceived, numKeyAccepted, idKeyAccepted	Required, V1.0
ZeroizeKey	Zeroize a specified key in key store.	keyID	Status	Required, V1.0
ZeroizeAll	Zeroize all keys in key store.	N/A	Status	Required, V1.0
GetKeyInventory	Request info on the keys in key store.	N/A	keyIDs	Required, V1.0
GetKey	A SOSA module requests a specific key/key package to be sent to it.	keyID	Cryptographic key material	Required, V1.0
CreateConfigGroup	Creates a security configuration for a cryptographic subsystem, which is associated with crypto channel(s).	groupType, channelID, ceaIDs	groupID	Required, V1.0
CreateConfig	Creates a security configuration within the specified security configuration group within a cryptographic subsystem.	groupID, ceaID, keyID, certificateID, infosecMode	configID	Required, V1.0
DestroyConfigGroup	Destroys an instantiated security configuration group.	groupID	Status	Required, V1.0

Interaction Name	Interaction Description	Input Object	Output Object	Required/Optional, Applicability
DestroyConfig	Destroys an instantiated security configuration.	groupID, configID	Status	Required, V1.0
GetConfigGroup	Retrieves the configuration information of an instantiated security configuration group.	channelID, groupID	groupType, groupID, configIDs, channelID	Required, V1.0
GetConfig	Retrieves the configuration information of an instantiated security configuration.	groupID, configID	keyID, ceaID	Required, V1.0
SendKey	A request from a SOSA module to Security Services to send key/key packages to another SOSA module.	moduleID, keyID	Status	Required, V1.0
PushKey	In response to SendKey, Security Services sends key/key packages to the SOSA module specified in SendKey.	* Cryptographic key or key package; varied by systems	Status	Required, V1.0

* Adopted from the Joint Tactical Networking Center (JTNC) RSS standards.

12.1.4 Authentication Service

The authentication service is a centralized service that verifies that a SOSA module instance comes from an authenticated source.

The authentication service is used to provide authentication tokens to entities in the system that can be used by other Security Services, such as authorization. The detailed requirements for the authentication service are planned for a future version of this document.

The authentication service is a centralized service that verifies that a SOSA module instance is intended to be used on the SOSA sensor. In particular, the SOSA module instance would be verified that it comes from an authentic source.

The authentication service is used to provide authentication tokens to entities in the system that can be used by other Security Services, such as authorization. These tokens are generated by the authentication service, potentially based on predetermined information provided to this service.

For authentication, we strive to allow as many options as possible for integrators to confirm the identity of different SOSA module instances utilizing the SOSA Security Services module. Our initial start has been creating an API that has username and password support, along with X.509 Certificate support. Using these we want to verify the identity of the requestor and give them an authentication token that will be used to help authorize the module or user for various privileged interactions they could need.

Rule 12.1.4-1: Upon receipt of a *checkUserCredentials* request from a requestor, Security Services shall evaluate the message and then return to the requestor an authentication token on successful evaluation or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-2: Upon receipt of a *checkUserDigest* request from a requestor, Security Services shall evaluate the message and then return to the requestor an authentication token on successful evaluation or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-3: SOSA modules shall compute password digests in the format of *PasswordDigest* = Base64 (SHA-384 (nonce + createdTime + password)). Conformance Methodology (D)

Rule 12.1.4-4: Upon receipt of an *addUsername* request from a requestor, Security Services shall ensure the username and password pair are able to be used for authentication upon success or return an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-5: Usernames shall be unique within the SOSA Security Services module and an error shall be thrown if a username is attempted to be added that is already within the system. Conformance Methodology (D)

Rule 12.1.4-6: Upon receipt of a *removeUsername* request from a requestor, Security Services shall ensure the username and all associated data is not usable for authentication, then return to the requestor a message upon success or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-7: Upon receipt of a *getUsernames* request from a requestor, Security Services shall send to the requestor a list of all the usernames currently registered in the system, and if Security Services is unable to provide the information to the requestor, Security Services returns an appropriate error message. Conformance Methodology (D)

Rule 12.1.4-8: Upon receipt of a *checkx509Cert* request from a requestor, Security Services shall evaluate the certificate and then return to the requestor a valid authentication token upon successful evaluation or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-9: Upon receipt of a *checkPKIPath* request from a requestor, Security Services shall evaluate the PKIPath and then return to the requestor, a valid authentication token upon successful evaluation or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-10: Upon receipt of a *checkPKCS7Wrapper* request from a requestor, Security Services shall evaluate the PKCS7 wrapper and then return to the requestor a valid authentication token upon successful evaluation or an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-11: Upon receipt of an *addTrustedCert* request from a requestor, Security Services shall add the x509v3 certificate to the usable certificates for authentication upon success or return an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-12: Upon receipt of an *addX509PKIPath* request from a requestor, Security Services shall add the x509PKIPath to the usable certificates for authentication upon success or return an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-13: Upon receipt of an *addPKCS7Wrapper* request from a requestor, Security Services shall add the PKCS7 wrapper to the usable certificates for authentication upon success or return an error message upon failure. Conformance Methodology (D)

Rule 12.1.4-14: Upon receipt of a *removeTrustedCert* request from a requestor, Security Services shall ensure all certificate data associated with the issuer and serial that is provided by the requestor is not usable for authentication; upon failure, Security Services reports the failure to the requestor via an error message. Conformance Methodology (D)

Rule 12.1.4-15: Upon receipt of a *getListofTrustedCerts* request from a requestor, Security Services shall send to the requestor a list of all the X.509 Certificates currently registered in the system; upon failure, Security Services is unable to provide the information to the requestor and Security Services returns an appropriate error message. Conformance Methodology (D)

Rule 12.1.4-16: Upon receipt of a *getTrustedCert* request from a requestor, Security Services shall send to the requestor the X.509 Certificate that matches the issuer and serial that was sent in the message; upon failure, Security Services is unable to provide the information to the requestor and returns an appropriate error message. Conformance Methodology (D)

Table 12.1.4-1: Authentication Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability
checkUserPassword	Checks the username and password provided by the module or user.	Username (String), Plaintext Password (String)	Authentication token on success, error on failure	Required
checkUserCredentials	Checks the username and digest with a nonce and time created if provided by the module or user.	Username (String), Digest (String) with (optional) Nonce (String), (optional) time created (String)	Authentication token on success, error on failure	Required
addUsername	Adds a username and password to Security Services.	Username (String), Password (String)	Error on failure	Required
removeUsername	Removes a username and associated data from Security Services.	Username (String)	Error on failure	Required
getUsernames	Retrieves all usernames in the system.	N/A	List of names (String), Error on failure	Required
addTrustedCert	Adds a trusted certificate to Security Services.	Certificate (base64Binary)	Error on failure	Required
addX509PKIPath	Adds a X.509 PKI Path to Security Services.	X509pkipath (base64Binary)	Error on failure	Required
addPKCS7Wrapper	Adds a PKCS7 wrapper to Security Services.	PKCS7 (base64Binary)	Error on failure	Required
removeTrustedCert	Removes a trusted certificate from Security Services.	Issuer (String), Serial (String)	Error on failure	Required

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability
getTrustedCert	Gets the trusted certificate from Security Services.	Issuer (String), Serial (String), SubjectKeyIdentifier (String)	x.509 Certificate, Error on failure	Required
getListofTrustedCerts	Gets the list of trusted certificates from Security Services.	N/A	Issuer (String), Serial Number (String), (optional) Friendly Subject (String)	Required
checkX509Cert	Checks that the given certificate can be trusted.	Certificate (base64Binary)	Authentication token, Error on failure	Required
checkX509PKIPath	Checks that the given PKIPath can be trusted.	X509PKIPath (base64Binary)	Authentication token, Error on failure	Required
checkPKCS7Wrapper	Checks that the given PKCS #7 wrapper can be trusted.	PKCS #7 wrapper (base64Binary)	Authentication token, Error on failure	Required

12.1.5 Authorization Service

The authorization service is a centralized service that performs access control for privileged functions. The authorization service, when paired with the authentication service, implements many of the policies described in the NIST SP 800-53 Access Control (AC) Family.

Authorization services are intended to be used by a service provider to determine whether a requestor should have access to a privileged function. When a request for a privileged function is received, the service provider will verify that the authenticated requestor has permission to access the function. The Security Services module will grant or deny permission based on user-provided authorization policy, which includes the function, the SOSA module authorized to access the function, and other attributes (e.g., authorization validity). The Security Services module optionally provides the ability for the service provider to cache the authorization for a given time or number of requests.

Rule 12.1.5-1: When requested, Security Services shall provide a response that grants or denies access to a privileged function per the authorization policy. Conformance Methodology (D)

Rule 12.1.5-2: When requested, Security Services shall set the authorization policy for one or more privileged functions and the conditions on which it should grant access. Conformance Methodology (D)

Rule 12.1.5-3: When access to a privileged function is requested, SOSA modules shall verify that authorization is granted before executing the function. Conformance Methodology (D)

Observation 12.1.5-1: SOSA modules could verify authorization via a locally stored cache of a previously received authorization response, so long as the received authorization is still valid.

Table 12.1.5-1 describes authorizing a specific sensor component to privileged functions. A future version of this document will include role-based authorization for SOSA modules.

Table 12.1.5-1: Authorization Interactions

Interaction Name	Interaction Description	InputObjects	Output Objects	Required/Optional, Applicability
RequestAuthorization	Request whether a SOSA sensor component with an authentication token is allowed to access privileged functions.	requestor, service	authorized, validTime, authorizationCount	Required, V1.0
SetAuthorizationPolicy	Sets whether a SOSA sensor component is allowed to access privileged function and associated policies.	entity, service, (optional) validTime, authorizationCount	None	Required, V1.0

12.1.6 Zeroization

A SOSA system supports the concept of zeroization, which refers to removing Critical Security Parameters (CSPs) which, if recovered, would compromise the security of a SOSA system [adapted from NIST FIPS 140-2]. CSPs include cryptographic keys, passwords, and other information that is used to prevent unauthorized access in the system and to protect the exposure of sensitive data. Zeroization can be used to prevent unauthorized persons from gaining access to sensitive data if a security event is detected.

Zeroization is related to but separate from sanitization. Zeroization only clears security-relevant information from memory to prevent recovery of that information; it does not fully wipe memory. It is meant to be a quick response to a command. Sanitization, on the other hand, is much broader. Sanitization fully wipes a memory region often requiring several erase/write cycles to complete. For this reason, sanitization generally takes much longer than zeroization to complete.

In a SOSA system, CSPs could be in many different places. For example, CSPs could be located on individual PICs, or within SOSA modules. The zeroization service only applies to CSPs contained within the Security Services module.

What is considered a CSP varies from system to system. It is up to the system integrator or user to define which information is a CSP for a given system.

This service does not prevent the inadvertent erasure of CSPs. For example, keys could be maintained in battery-backed RAM and inadvertently cleared during a power down if the battery fails.

Rule 12.1.6-1: When a zeroization request is received, the SOSA Security Services module shall erase all instances of CSPs contained within the SOSA Security Services module specified by the authenticated requestor. Conformance Methodology (D)

Observation 12.1.6-1: Zeroization can be applied to CSPs directly managed by the Security Services module, or by an associated Encrypt/Decrypt module. This will depend on the security architecture of the target system. The allowable levels of zeroization supported by the Security Services module will vary by mission authority.

Observation 12.1.6-2: Varying levels of assurance could be achieved when zeroizing CSPs based on the method used for zeroization and the technology used to store the CSPs. This document does not prescribe zeroization methods.

Rule 12.1.6-2: When a zeroization request completes, the SOSA Security Services module shall provide a zeroization status to the requestor. Conformance Methodology (D)

Zeroization events are auditable and are reported to the Security Services audit subsystem (see Section 12.1.2).

Rule 12.1.6-3: The SOSA Security Services module shall report all zeroization events to the Security Services audit subsystem. Conformance Methodology (D)

Table 12.1.6-1: Zeroization Interactions

Interaction Name	Interaction Description	InputObjects	Output Objects	Required/Optional, Applicability
ZeroizeKey	Zeroize a specified key in key store.	keyID	Status	Required, V1.0
ZeroizeAll	Zeroize all keys in key store.	N/A	Status	Required, V1.0

*Adopted from the JTNC RSS standards.

12.1.7 Software Package Verification Service

The software package verification service is a centralized service that assists SOSA RTEs with verification of software packages. It provides an interface for authorized modules to load the accepted software package digests for each software package identifier (e.g., a unique file name). SOSA RTEs can later retrieve these digests as they load software packages to verify these packages before execution.

Note that additional definitions and releases for the Security Services module are defined in Section 6.2.5.

Rule 12.1.7-1: When requested, the SOSA Security Services module shall return a digest for a software package identifier. Conformance Methodology (D)

Rule 12.1.7-2: When requested, the SOSA Security Services module shall accept and store a software digest with its associated software package identifier. Conformance Methodology (D)

Table 12.1.7-1: Software Package Verification Interactions

Interaction Name	Interaction Description	Input Object	Output Object	Required/Optional, Applicability
AuthenticateDigests	Check that a digest is authentic.	software package identifier, digest	Status	Required, V1.0
SetAuthenticatedDigests	Store a list of authenticated digests for software packages.	software package identifier, digest	Status	Required, V1.0

Table 12.1.7-2: SOSA SvcV-4 – Security Services

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.1 Security Services	Check software/data integrity	Security Parameters	(E.g., encryption keys, access control data, module integrity data)
	Manage key(s)	Zeroize Assignment	
	Control access	Access Request	
	Audit	Classification Level Tag(s)	
	Zeroize all sensitive data	Security Audit Report	
		Security Tamper Alert	
		Access Request-Response	
		Zeroize ACK/NAK	
	Zeroize Assignment	(To other modules)	

12.2 Encryptor/Decryptor

12.2.1 Encryptor/Decryptor Common Rules

The Encryptor/Decryptor module provides the cryptographic functions to protect the confidentiality, integrity, and availability against cyber vulnerabilities. Those functions are also used to provide authentication, authorization, and non-repudiation. The Encryptor/Decryptor module is subject to certification based on the sensitivity of the data it handles. The rules defined herein provide general guidance on Encryptor/Decryptor module capabilities, but not specific to a certification level (e.g., High Assurance, FIPS, CSfC).

General rules that are applicable to the SOSA Encryptor/Decryptor module are defined in Section 12.2.1. Rules that are specific for the SOSA Encryptor/Decryptor module that support

the DARE capability are specified in Section 12.2.2. Rules that are specific for the SOSA Encryptor/Decryptor module that support the Data-In-Transit Encryption (DiTE) capability will be specified in Section 12.2.2.

A key capability of a SOSA system is to process signals from sensors and generate data and information to support greater missions. The data and information are likely to be sensitive and should be stored securely at rest. The SOSA aligned DARE architecture is described in Figure 12.2.1-1. The upstream interface of the Storage Retrieval Manager must use Ethernet-based protocols including NFS or RDMA over Converged Ethernet (RoCE). The downstream interface to Storage Media must implement NVMe (v1.2 or newer) over Peripheral Computer Interface Express (PCIe). The selection of the NVMe protocol, over sunsetting protocols such as Serial AT Attachment (SATA) and Internet Small Computer Systems Interface (iSCSI), is to ensure the throughput of data storage access aligns with the high-speed application targeted by SOSA systems.

In Use-Case 1, the Storage Retrieval Manager is used to process requests to store or retrieve data. The data is then processed through the Encryptor/Decryptor used for DARE. The inline Encryptor/Decryptor must operate transparently between the Storage Retrieval Manager and the Storage Media. The Storage Retrieval Manager would interact with the Storage Media as if it is directly connected to it. This implies the Encryptor/Decryptor must implement the required downstream protocol of standard NVMe over PCIe for its interface to the Storage Retrieval Manager and to the Storage Media. Furthermore, the Encryptor/Decryptor must support encryption and decryption of data of mixed classifications seamlessly without requiring explicit commands to switch between classifications levels. In Use-Case 2, the Encryptor/Decryptor is not used. The Storage Retrieval Manager has direct NVMe over PCIe interfaces with the storage media. In Use-Case 3, the Data Source/Sink directly interfaces with the storage media via NVMe over PCIe.

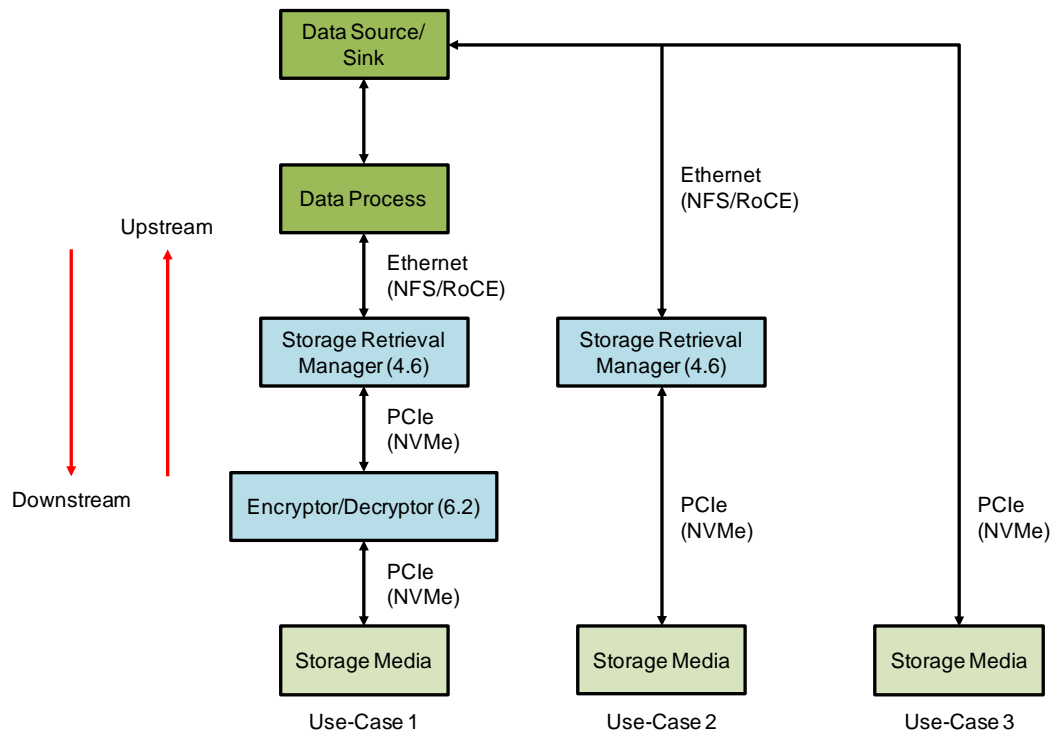


Figure 12.2.1-1: SOSA-Aligned Data-At-Rest Encryption (DARE) Architecture and Use-Cases

Rule 12.2.1-1: Where more than one keyed level is allowed, the SOSA Encryptor/Decryptor module shall allow encryption/decryption operation for all configured keyed levels without re-configuration between use of those levels. This applies to the data-in-transit Encryptor/Decryptor module and the Data-At-Rest Encryptor/Decryptor module. Conformance Methodology (D)

Observation 12.2.1-1: If the Encryptor/Decryptor module has been properly keyed and configured for the allowed keyed levels, the Encryptor/Decryptor module will be able to encrypt or decrypt data traffic of mixed key levels over its Data Plane without any additional commands on the Control Plane.

Rule 12.2.1-2: Where more than one cryptographic channel is allowed, the SOSA Encryptor/Decryptor module shall allow encryption/decryption operation for all configured cryptographic channels independently, without having any cryptographic channel impacting the other cryptographic channels. This applies to the data-in-transit Encryptor/Decryptor module and the Data-At-Rest Encryptor/Decryptor module. Conformance Methodology (A/D)

Observation 12.2.1-2: The encryption/decryption operation includes encrypt or decrypt data traffic over its Data Plane, accepting commands and providing statuses via the Control Plane. Note that the one exception to this is if the Encryptor/Decryptor module is in an ALARM state, which shall prevent the operation of any cryptographic channels which it contains.

Rule 12.2.1-3: When a zeroization request is received, the SOSA Encryptor/Decryptor module shall zeroize cryptographic key(s) specified by the authenticated requestor. Conformance Methodology (D)

Rule 12.2.1-4: When a key inventory request is received, the SOSA Encryptor/Decryptor module shall provide inventory status of stored cryptographic key(s) to an authenticated requestor. Conformance Methodology (D)

Rule 12.2.1-5: The SOSA Encryptor/Decryptor module shall provide key tag in accordance with RSS API stored cryptographic key(s) as a response to a key inventory status request. Conformance Methodology (D)

Rule 12.2.1-6: When a key request is received, the SOSA Encryptor/Decryptor module shall provide cryptographic key(s) to an authenticated requestor. Conformance Methodology (D)

Rule 12.2.1-7: When a Encryptor/Decryptor module configuration is received, the SOSA Encryptor/Decryptor module shall configure for cryptographic key association. Conformance Methodology (D)

Rule 12.2.1-8: When a key store request is received, the SOSA Encryptor/Decryptor module shall store cryptographic key(s). Conformance Methodology (D)

Observation 12.2.1-3: Note that Rule 12.2.1-8 is different from key management rules (Section 12.1.3) because this assumes the key has been loaded into the sensor system. This is strictly for inter-module exchange, where key loading involves receiving the key from an external entity.

Rule 12.2.1-9: Cryptographic material shall be stored in SOSA Encryptor/Decryptor modules that are certified to handle data at the associated classification level. Conformance Methodology (I)

Observation 12.2.1-4: Rule 12.2.1-9 assumes the hardware element that hosts the SOSA Encryptor/Decryptor modules under conformance evaluation have been certified by an

appropriate certification authority to handle classified key material at its associated classification level.

Table 12.2.1-1: Zeroization Interactions

Interaction Name	Interaction Description	Input Object	Output Object	Required/Optional, Applicability
LoadKey	Facilitate loading of cryptographic key via DS101 interface.	* Cryptographic key or key package; varied by systems	N/A (status on the key(s) loaded are requested via GetKeyInventory interaction)	Required, V1.0
StoreKey	Facilitate loading of cryptographic key via KMI or other OTNK protocol.	* Cryptographic key or key package; varied by systems	numKeyReceived, numKeyAccepted, idKeyAccepted	Required, V1.0
ZeroizeKey	Zeroize a specified key in key store.	keyID	Status	Required, V1.0
ZeroizeAll	Zeroize all keys in key store.	N/A	Status	Required, V1.0
GetKeyInventory	Request info on keys in key store.	N/A	keyIDs	Required, V1.0
GetKey	A SOSA module requests a specific key/key package to be sent to it.	keyID	Cryptographic key material	Required, V1.0
CreateConfigGroup	Create a security configuration for a cryptographic subsystem, which is associated with crypto channel(s).	groupType, channelID, ceaIDs	groupID	Required, V1.0
CreateConfig	Create a security configuration within the specified security configuration group within a cryptographic subsystem.	groupID, ceaID, keyID, certificateID, infosecMode	configID	Required, V1.0
DestroyConfigGroup	Destroy an instantiated security configuration group.	groupID	Status	Required, V1.0
DestroyConfig	Destroy an instantiated security configuration.	groupID, configID	Status	Required, V1.0

Interaction Name	Interaction Description	Input Object	Output Object	Required/Optional, Applicability
GetConfigGroup	Retrieve the configuration information of an instantiated security configuration group.	channelID, groupID	groupType, groupID, configIDs, channelID	Required, V1.0
GetConfig	Retrieve the configuration information of an instantiated security configuration.	groupID, configID	KeyID, ceaID	Required, V1.0

12.2.2 Encryptor/Decryptor Rules for Data-At-Rest Encryption (DARE)

The Storage Retrieval Manager (module 4.6) is responsible for storing data in non-volatile storage media. This data could be encrypted through the Encryptor/Decryptor (module 6.2). Interactions between the Storage Retrieval Manager and the Encryptor/Decryptor module are based on the RSS API and shown in Table 12.2.2-1.

Three use-cases have been identified for storing data, as shown in Figure 12.2.1-1. These use-cases demonstrate the flexibility within the SOSA Architecture to write sensor data to non-volatile storage, encrypted or non-encrypted.

The rules for the Storage Retrieval Manager in Section 12.2.1 use the terms “upstream” and “downstream”. Upstream is always from the Storage Retrieval Manager to the data source or sink. Downstream is always toward the storage media.

Rule 12.2.2-1: Where DARE is used, the SOSA Encryptor/Decryptor module shall provide inline NVMe block encryption and decryption capability. Conformance Methodology (D)

Rule 12.2.2-2: Where DARE is used, the SOSA Encryptor/Decryptor module shall allow in-band bypass of the NVMe header. Conformance Methodology (D)

Rule 12.2.2-3: Where DARE is used, the SOSA Encryptor/Decryptor module shall interface with an upstream data provider using NVMe. Conformance Methodology (D)

Rule 12.2.2-4: Where DARE is used, the SOSA Encryptor/Decryptor module shall interface with downstream storage device(s) using NVMe. Conformance Methodology (D)

Rule 12.2.2-5: Where DARE is used, the SOSA Encryptor/Decryptor module shall use DS-101 or KMI OTNK key delivery to load cryptographic keys. Conformance Methodology (D)

Table 12.2.2-1: SOSA SvcV-4 – Encryptor/Decryptor

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.2 Encryptor/Decryptor	Protect data-at-rest	Security Parameters	Encryption keys
	Protect data-in-transit	Zeroize Assignment	

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
	Encrypt/decrypt	Access Control Data	
		Data or Stream to be Encrypted	
		Data or Stream to be Decrypted	
		Zeroize ACK/NAK	
		Encrypted Data or Stream	
		Decrypted Data or Stream	

12.3 Guard/Cross-Domain

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.3-1: SOSA SvcV-4 – Guard/Cross-Domain Service

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.3 Guard/Cross-Domain Service	Prevent data leakage	Data or Stream to be Filtered	
		Security Parameters	(Metadata tags for data/stream, filtering criteria, human verification)
		Filtered Data or Stream	
		Filtering Status	
		Security Auditing Data	

12.4 Network Subsystem

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.4-1: SOSA SvcV-4 – Network Subsystem

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.4 Network Subsystem	Enumerate network elements	Data or Stream to be Sent	

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
	Monitor health of network elements	Network Data Transfer Parameters	
	Detect and isolate network degraded elements	Network Configuration Parameters	
	Transfer data with requested QoS	Data or Stream that was Sent	
	Detect intrusion	Network Health & Status	
		Intrusion Reports	

12.5 Calibration Service

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.5-1: SOSA SvcV-4 – Calibration Service

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.5 Calibration Service	Intake the injected test signal	Injected Test RF Signal	
	Collect output of either calibration test points or main	Injected Test Image/Video Stream	
	Disable modules not under test	Injected Test Demodulated Signal	
		Calibration Assignment Safety Interlock	
		Electromagnetic Source Assignment	
		Calibration Measurement	

12.6 Nav Data Service

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.6-1: SOSA SvcV-4 – Nav Data Service

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.6 Nav Data Service	Ingest platform/sensor location and orientation	Nav Data Stream	(External source – option, since could be internally generated)
	Blend internal and external spatial data	Nav Data Stream	
	Distribute platform/sensor location and orientation		

12.7 Time & Frequency Service

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.7-1: SOSA SvcV-4 – Time & Frequency Service

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.7 Time & Frequency Service	Ingest time from external source	Time Reference	(External source)
	Blend internal and external time data	Time Reference	
	Generate time internally	Frequency Reference	
	Provide time to internal function		
	Provide LO/frequency reference		

12.8 Compressor/Decompressor

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.8-1: SOSA SvcV-4 – Compressor/Decompressor

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.8 Compressor/ Decompressor	Compression	Compressor/Decompressor Assignment	
	Decompression	Compressed Data	
	Codec functions	Compression Metadata	
		Decompressed Data	
		Decompression Metadata	

12.9 SOSA Host Platform Interface

12.9.1 Definition

See Section 4.2 for the definition of this module.

The Host Platform Interface provides a bridge between the SOSA sensor and the host platform. It converts the SOSA interactions to/from the Host Platform Interface protocol. For example, a SOSA sensor plugging into an OMS-based platform would have a Host Platform Interface module that supports OMS interfaces on the outward-facing side and SOSA module interfaces on the inward-facing side.

The SOSA Consortium has accepted a set of interactions and associated DIV-2 Data Entities for external sensor tasking, primarily tasking of RF sensors. These interactions represent a basic set of functionalities distilled from Universal Command & Control Interface (UCI), VICTORY, and STANAG 4586. The Host Platform Interface (module 6.9) receives UCI, VICTORY, or STANAG 4586 command and control messages, translates them into the SOSA message format, and initiates interactions with the System Manager (module 1.1) and Task Manager (module 1.2). The Host Platform Interface also receives messages from within the SOSA sensor about the commanded tasks and translates them from the SOSA message format into messages that adhere to the UCI, VICTORY, or STANAG 4586 message standards.

The high-level description of the Reporting Services module is provided in Table 12.9.1-1, which provides a detailed functional decomposition for this module.

Table 12.9.1-1: SvcV-1 Module Descriptions

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Coordinate Mission Tasking	Translate Mission Tasking	The action of translating external commands to internal SOSA sensor commands.

SOSA Functional Group 1	SOSA Functional Group 2	SOSA Functional Group 3	Definition
Coordinate Mission Operations	Coordinate Mission Tasking	Report Mission Tasking Status	The action of reporting mission tasking status to the mission task requestor.
Coordinate Mission Operations	Disseminate Formatted Mission Products	Disseminate Requested Mission Products	The action of disseminating requested mission products to the requestor.

12.9.2 Host Platform Interface Interactions

Table 12.9.2-1 shows the interactions that have been defined for the Host Platform Interface module based on the three RF sensor threads considered under the current version of this document.

Table 12.9.2-1: Host Platform Interface Interactions

Interaction Name	Interaction Description	Input Objects	Output Objects	Required/Optional, Applicability	Interaction Type
executeMissionTask	The action of start/pause/resume/cancel SOSA mission thread.	MissionTaskDescriptor	MissionTaskResponse	Required	Request

12.9.3 Host Platform Interface Interaction Rules

The following rules apply to the interactions for the Host Platform Interface defined in Section 12.9.2.

Rule 12.9.3-1: The Host Platform Interface shall maintain all association between the platform-facing side and SOSA module interfaces on the inward-facing side and provide a unique SOSA TaskID for all mission requests.

Rule 12.9.3-2: The Host Platform Interface shall maintain metadata from the requestor message to respond to the platform-facing side.

Rule 12.9.3-3: The Host Platform Interface shall implement all required interactions defined in Table 12.9.2-1.

12.10 Power

This SOSA module is not defined for this version of the Technical Standard. The following functional definition is provided for reference only.

Table 12.10-1: SOSA SvcV-4 – Power

Module	Encapsulated Functions	Inputs (above) & Outputs (below)	Input/Output Description
6 Support System Operation			
6.10 Power	Convert between different power characteristics	Host Power	From Host Platform Interface
	Condition/filter power	Power Assignment	From Task Manager
	Store power for intermittent input power loss	Power	To all modules
	Store power to provide long-term power to loads without input power	Power Assignment Response	To Task Manager
	Distribute power from power supplies to power loads		
	Protect against voltage and over-current conditions		
	Provide a digital control interface		

13 Hardware Element

This chapter details a series of Rules, Recommendations, Observations, and Permissions for hardware Plug-In Card Profiles (PICPs) that are based on the OpenVPX (ANSI/VITA 65.0) and VNX+™ (VITA 90.0) PIC form factors. These form factors cover 6U and 3U VPX and 19mm VNX+ size cards.

A future version of this document could include other form factor PICs based on customer and technology needs.

13.1 PIC Use-Cases

The SOSA hardware concepts are predicated on a set of architectural decisions that drive the overall development of the entire effort. The high-level use-case below is illustrative and provides an overview of all the relevant building blocks that encompass the hardware portion of this document. Each element in the use-case, both bubbles and lines, titles those specific building blocks and their connections. It is very important to note that each piece is a family that includes several types that differ in some respects and are similar in others. One of the underlying tenets not reflected in the diagram is the maximization of SOSA PIC interoperability. With that in mind, it is worth considering the connections below and that multiple SOSA PICs are capable of those connections.

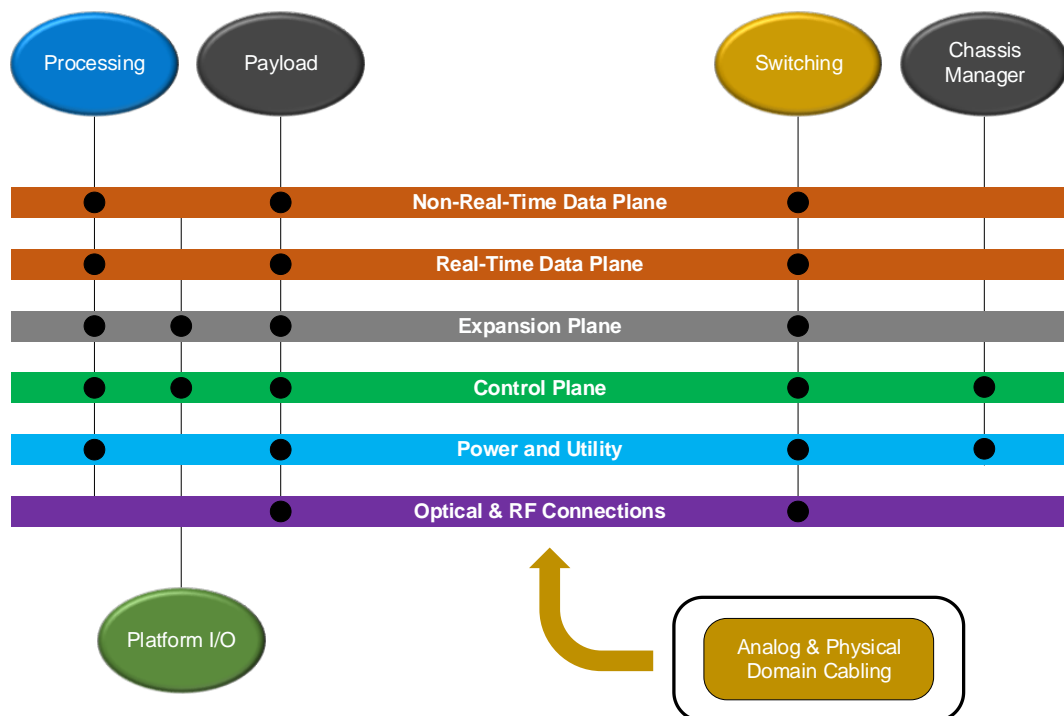


Figure 13.1-1: High-Level SOSA Use-Case

13.2 SOSA Plug-in Cards Using OpenVPX

13.2.1 SOSA PICP Form Factors

Rule 13.2.1-1: SOSA PICs of Section 13.2 shall be designed to one of the following form factors:

- (ANSI/VITA 65.0) 3U Form Factor
- (ANSI/VITA 65.0) 6U Form Factor

13.2.2 SOSA PIC Common Electrical and Functional Requirements

This section has general electrical requirements and some general requirements related to functionality.

Permission 13.2.2-1: SOSA PICs may work cooperatively to increase performance and/or functionality.

13.2.2.1 *Unused but Electrically Connected PIC Pins*

This section gives SOSA requirements for unused but electrically connected pins. This is like ANSI/VITA 65.0 §8.4.1, which covers what it refers to as dormant pin.

Rule 13.2.2.1-1: While in an unused state, any SOSA PIC pins connected to the backplane shall meet all electrical requirements for those pins. Conformance Methodology (I)

Permission 13.2.2.1-1: A SOSA PIC may have pins electrically connected to the backplane but make no use of the connection.

Observation 13.2.2.1-1: The intent of Rule 13.2.2.1-1 and Permission 13.2.2.1-1 is to allow unused pins to still be connected if they are electrically benign. This enables programmable devices on PICs to be electrically connected to defined backplane pins.

13.2.3 Utility Plane Requirements

Reference ANSI/VITA 65.0 §3 for Utility Plane requirements. Utility Plane requirements are extended for this document as follows.

Utility signal design constraints appear in various sections of this document. PIC designers should refer to these sections for implementation guidance:

Utility Signal	SOSA Technical Standard Reference
Vs1	Section 13.2.3
Vs2	Section 13.2.3
Vs3	Section 13.2.3
GA[4:0]*, GAP*	Out-of-Band Section 6.4
SM[3:0]	Out-of-Band Section 6.4

Utility Signal	SOSA Technical Standard Reference
AUX_CLK+/-	Radial Clock Section 13.2.11.5
3.3V_AUX	Section 13.2.3
+/-12V_AUX	Section 13.2.3
SYSRESET*	Out-of-Band Section 6.4
REF_CLK+/-	Radial Clock Section 13.2.11.5
NVMRO	Out-of-Band Section 6.4

13.2.3.1 Power Distribution

Rule 13.2.3.1-1: 3U SOSA PICs shall use VS1 (12V), 3.3V_AUX, and/or VBAT for input power. Conformance Methodology (I)

Rule 13.2.3.1-2: 3U SOSA PICs shall not use VS2 (3.3V) or VS3 (5.0V). Conformance Methodology (T)

Observation 13.2.3.1-1: For information concerning the maximum input current that the VS1 pins can handle, see ANSI/VITA 46.0, Observation 4-11.

Rule 13.2.3.1-3: 6U SOSA PICs shall use VS1 (12V), VS2 (12V), 3.3V_AUX, and/or VBAT as input power. Conformance Methodology (I)

Rule 13.2.3.1-4: SOSA PICs shall not use VS3 (5.0V). Conformance Methodology (I)

Observation 13.2.3.1-2: For information concerning the maximum input current that the VS1 and VS2 pins can handle, see ANSI/VITA 46.0, Observation 4-11.

Rule 13.2.3.1-5: SOSA PICs shall use 3.3V_AUX. Conformance Methodology (T)

Rule 13.2.3.1-6: SOSA PICs shall not use +/-12V auxiliary supplies. Conformance Methodology (T)

Observation 13.2.3.1-3: For more information concerning maximum current draw from 3.3V_AUX, see ANSI/VITA 46.0, Rule 3-11.2.

13.2.3.2 VBAT and ALT_VBAT for PICPs

Rule 13.2.3.2-1: PIC VBAT input shall be a minimum voltage of 2.55V and a maximum of 3.5V. Conformance Methodology (T)

Rule 13.2.3.2-2: PIC shall draw no more than 1 ma from VBAT, except for PICs with the following Slot Profile: SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n. Conformance Methodology (T)

Rule 13.2.3.2-3: PICs with a Slot Profile of SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n shall draw no more than 45 mA from VBAT. Conformance Methodology (T)

Observation 13.2.3.2-1: Rule 13.2.3.2-3 supersedes the 1 mA maximum requirement of ANSI/VITA 46.0, Rule 4-56.1 and the 2.2 Amp maximum specified by ANSI/VITA 65.0, Rule

14.9.2.1.2-1. The higher than ANSI/VITA 46.0 current is intended to enable temperature control of high-precision frequency sources, while operating on batteries. The maximum current is lower than the ANSI/VITA 65.0 requirement in order to limit the current needed to be supplied by batteries, while still allowing for reasonable devices implementing temperature control.

Note: Currently, the only applicable use for ALT_VBAT is on the SOSA 3U I/O Intensive Single Board Computer (SBC). There is an expectation that the use of ALT_VBAT will expand to other SOSA PICPs as the standard and its content evolves.

Rule 13.2.3.2-4: ALT_VBAT input to a PIC shall be a minimum voltage of 3.0V and a maximum of 3.9V. Conformance Methodology (T)

Rule 13.2.3.2-5: PICs shall draw no more than 10 mA from ALT_VBAT. Conformance Methodology (T)

13.2.4 General Mechanical

This section has general mechanical-related requirements. For requirements related to cooling and environmental, see Section 13.2.5.

The SOSA Technical Standard currently supports two conduction cooled 3U depths: the standard 160mm depth and a new shorter 100mm depth. The 100mm version will be referred to as “3U-S VPX” where the “S” stands for the shorter version. The 160mm depth is defined in ANSI/VITA 48.2 while the 100mm depth will be defined in this document until inclusion into the VITA specifications. When this is included in VITA, then the SOSA Technical Standard will reference the VITA dimensions and specifications and they will be removed from this document. Besides the depth, the 100mm depth version will also define a larger slot pitch of 1.2”.

In some cases, a backplane could be designed with 1.2” pitch to support either 160mm/1.0” pitch cards and 100mm/1.2” pitch cards, although it would require a different chassis and/or cold walls due to the different location of ejector handles because of the different depth of module. Note the two 3U conduction cooled variants are generally *not* interchangeable in each system.

13.2.4.1 Front Panel Connections

Rule 13.2.4.1-1: A SOSA PIC’s signals (both electrical and optical, and to and from the PIC) shall pass through the PIC’s backplane connectors, except for the following signals which are allowed to pass through a connector on the front panel: Conformance Methodology (I)

- Key Fill
- Crypto Ignition Key (CIK)
- Fiber Optic:
 - SLT3-SWH-6F1U7U-14.4.14
 - SLT3-SWH-4F1U7U1J-14.8.7-n
 - SLT3-SWH-6F8U-14.4.15
 - SLT6-SWH-14F16U1U15U1J-10.8.1-n

Rule 13.2.4.1-2: Unless signals are included in an XMC Overlay Profile, all signals between SOSA PICs shall pass through the backplane connector(s) before going to another component in a SOSA system. Conformance Methodology (I)

13.2.4.2 *Slot Pitch*

Reference ANSI/VITA 65.0 §4.1 for slot pitch requirements. Slot pitch requirements are extended for the SOSA Technical Standard as follows.

Rule 13.2.4.2-1: The Chassis Slots intended for SOSA PICs that are conformant to ANSI/VITA 48.2 shall be 1.0" pitch or greater as per ANSI/VITA 48.2. Conformance Methodology (I)

Rule 13.2.4.2-2: The Backplane Slots intended for SOSA PICs that are conformant to ANSI/VITA 48.2 shall be 1.0" pitch or greater as per ANSI/VITA 48.2. Conformance Methodology (I)

Rule 13.2.4.2-3: When a 160mm SOSA PIC is conduction cooled, the PIC shall conform to ANSI/VITA 48.2 1.0" pitch requirements. Conformance Methodology (I)

Rule 13.2.4.2-4: The Backplane Slots intended for SOSA PICs that are conformant to ANSI/VITA 48.4 shall be 1.0" pitch or greater as per ANSI/VITA 48.4. Conformance Methodology (I)

Rule 13.2.4.2-5: When a SOSA PIC is liquid cooled, the PIC shall conform to ANSI/VITA 48.4 1.0" pitch requirements. Conformance Methodology (I)

Rule 13.2.4.2-6: The Chassis Slots intended for SOSA PICs that are conformant to ANSI/VITA 48.8 shall be 1.5" pitch or greater as per ANSI/VITA 48.8. Conformance Methodology (I)

Rule 13.2.4.2-7: The Backplane Slots intended for SOSA PICs that are conformant to ANSI/VITA 48.8, shall be 1.5" pitch or greater as per ANSI/VITA 48.8. Conformance Methodology (I)

Rule 13.2.4.2-8: When a SOSA PIC is air flow through cooled, the PIC shall conform to ANSI/VITA 48.8 1.5" pitch requirements. Conformance Methodology (I)

Rule 13.2.4.2-9: 100mm Conduction Cooled SOSA PICs shall be conformant to Table 13.2.4.2-1, Table 13.2.4.2-2, Figure 13.2.4.2-1, and Figure 13.2.4.2-2 showing VITA plug-in module requirements for 1.20" pitch. Conformance Methodology (I)

Observation 13.2.4.2-1: 1.2" conduction cooled pitch, for 3U sVPX, is currently specified in this document; however, when it is incorporated into ANSI/VITA 48.0/48.2 this document will be updated to reference the VITA specifications. Conformance Methodology (I)

Table 13.2.4.2-1: Primary Side Retainer Dimensions for 3U Conduction Cooled Cards

Primary Side Retainer	
Variable	1.20 in Pitch
*PSTI: Primary Side of Printed Circuit Board (PCB) to Thermal Interface	[3.35±0.13] 0.132±.005

Primary Side Retainer	
*PSRW: primary side of PCB to outer edge of relaxed retainer	[9.22±0.25] 0.363±.010
PIUW: Plug-In Unit Width	[29.72 MAX] 1.170 MAX
PS: Primary Side of PCB to front of plug-in unit	[21.84 MAX] 0.860 MAX
SS: primary side of PCB to back of plug-in unit	[7.87 MAX] 0.310 MAX

Table 13.2.4.2-2: Secondary Side Retainer Dimensions for 3U Conduction Cooled Cards

Secondary Side Retainer	
Variable	1.20 in Pitch
*PSTI: primary side of PCB to thermal interface	[9.98±0.13] 0.393±.005
*PSRW: primary side of PCB to outer edge of relaxed retainer	[2.59±0.25] 0.102±.010
PIUW: plug-in unit width	[29.72 MAX] 1.170 MAX
PS: primary side of PCB to front of plug-in unit	[21.84 MAX] 0.860 MAX
SS: primary side of PCB to back of plug-in unit	[7.87 MAX] 0.310 MAX

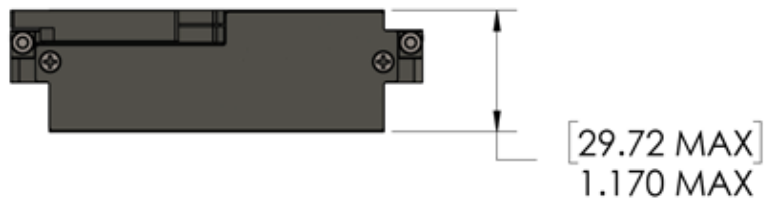


Figure 13.2.4.2-1: Module Width of 100mm 3U VPX Card

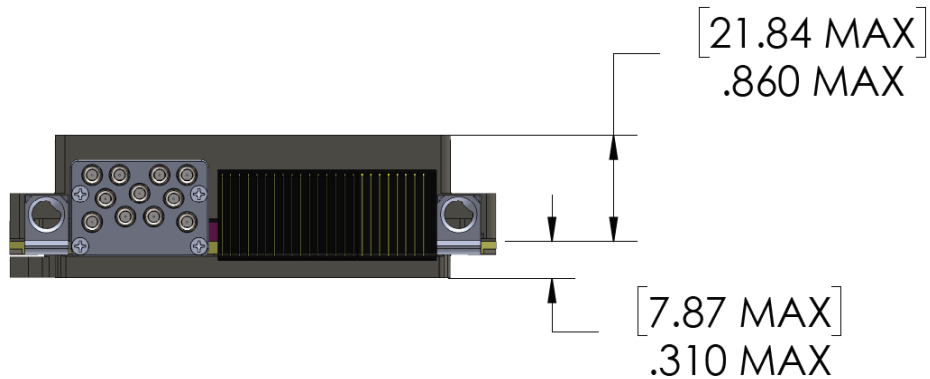


Figure 13.2.4.2-2: Wedge Lock Location of 100m 3U VPX Card

13.2.4.3 *PCB Dimension*

Rule 13.2.4.3-1: 100mm depth 3U VPX cards shall conform to the dimensions in Table 13.2.4.2-1 and Table 13.2.4.2-2. Conformance Methodology (I)

Observation 13.2.4.3-1: 100mm PCB depth is currently specified in this document; however, when it is incorporated into ANSI/VITA 48.0/48.2 this document will be updated to reference the VITA specifications. Conformance Methodology (I)

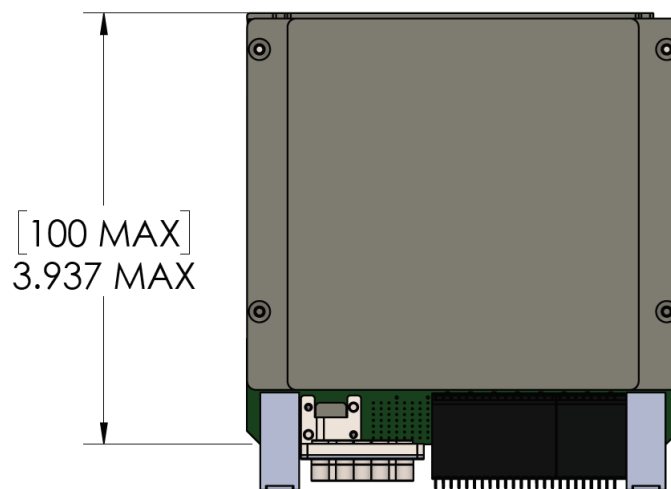


Figure 13.2.4.3-1: PCB Depth of 100mm 3U VPX Card

13.2.4.4 *Connector Family*

Rule 13.2.4.4-1: SOSA PICs shall use backplane interface connectors that are designed to ANSI/VITA 46.0, 46.30, 46.31, 66.x, and/or 67.x. Conformance Methodology (I, T)

Observation 13.2.4.4-1: ANSI/VITA 46.30 and 46.31 connectors intermate with ANSI/VITA 46.0 connectors but can operate at a higher signaling rate.

13.2.4.5 *Keying*

This document references ANSI/VITA 46.0 §4.4 for Alignment and Keying. Specifically, reference ANSI/VITA 46.0 §4.4.3 for Keying Rules applying to 6U and 3U modules. Reference

ANSI/VITA 65.0 §4.3 for keying requirements specific to ANSI/VITA 6U modules and backplanes.

13.2.4.6 *Rear Transition Modules (RTM)*

Rule 13.2.4.6-1: SOSA chassis shall not have Rear Transmission Modules (RTMs). Conformance Methodology (I)

13.2.5 Cooling Methods

Reference ANSI/VITA 48.2 for conduction cooled module requirements. Reference ANSI/VITA 48.8 for air flow through module requirements. Reference ANSI/VITA 48.4 for liquid cooled module requirements. For SOSA slot pitch requirements, see Section 13.2.4.2.

Rule 13.2.5-1: The SOSA PICs shall be designed to one of the cooling methods of ANSI/VITA 48.2 Type 1, ANSI/VITA 48.8 Type 1, or ANSI/VITA 48.4 Class A. Conformance Methodology (I, A, T (for 48.4 only))

Observation 13.2.5-1: ANSI/VITA 48.2 and ANSI/VITA 48.8 Type 1 have Electrostatic Discharge (ESD) protection, whereas Type 2 does not. With ANSI/VITA 48.4, Class A designates a latching, tolerance compensating insertion/extraction lever. Class B designates a non-latching insertion/extraction lever.

Recommendation 13.2.5-1: SOSA PICs should use extended covers to protect the ANSI/VITA 46.0 connectors. Conformance Methodology (I)

Permission 13.2.5-1: Adapter frames may be used to convert ANSI/VITA 48.2 to ANSI/VITA 48.8 form factor.

Observation 13.2.5-2: SOSA PICs might want to use the following cooling method guideline table (see Table 13.2.5-1), using a method more capable than the immediate need, in order to prepare for future power growth.

Observation 13.2.5-3: The chassis could be designed to accommodate multiple cooling methods (ANSI/VITA 48.2, ANSI/VITA 48.4, ANSI/VITA 48.8).

Observation 13.2.5-4: 1.0-inch pitch ANSI/VITA 48.2 conduction, ANSI/VITA 48.4 liquid flow through PICs, and 1.5-inch ANSI/VITA 48.8 air flow through PICs are not intermateable at the chassis slot level.

Observation 13.2.5-5: 1.0-inch pitch ANSI/VITA 48.2 conduction in a 1.5-inch air flow through adapter is intermateable with a 1.5-inch pitch ANSI/VITA 48.8 air flow through a PIC.

Observation 13.2.5-6: With proper planning, an ANSI/VITA 48.2 conduction, ANSI/VITA 48.8 air flow through, and ANSI/VITA 48.4 liquid flow through frames could accommodate common design ANSI/VITA 46.0 Circuit Card Assemblies.

Table 13.2.5-1: SOSA PIC Cooling Methods

SOSA PIC Form Factor and Cooling Method	3U Heat Load	6U Heat Load	System Integration Impact Rationale
ANSI/VITA 48.2 conduction to air cooled chassis	Low	Low	Host platform-agnostic air cooling

SOSA PIC Form Factor and Cooling Method	3U Heat Load	6U Heat Load	System Integration Impact Rationale
ANSI/VITA 48.8 air flow through	Medium	Medium	
ANSI/VITA 48.2 conduction to liquid cooled chassis	Medium	Medium	Dependent on host platform-supplied liquid cooling infrastructure with condensation mitigation
ANSI/VITA 48.4 liquid flow through	N/A	High	

13.2.6 Power Supply Card (PSC) General Rules

Rule 13.2.6-1: SOSA PSCs shall conform to Section 13.2.6 if they are installed into a monolithic backplane containing SOSA PICs. Conformance Methodology (T)

Recommendation 13.2.6-1: SOSA PSCs should conform to Section 13.2.6 and Section 13.2.3.1 even if they are part of a separate power supply backplane. Conformance Methodology (A)

Rule 13.2.6-2: Where 3U PSCs provide final power to SOSA PICs, the PSCs shall follow the profile as described in Table 13.2.6-1. Conformance Methodology (I)

Rule 13.2.6-3: Where 6U PSCs provide final power to SOSA PICs, the PSCs shall follow the profile as described in Table 13.2.6-2 and Table 13.2.6-3. Conformance Methodology (I)

Observation 13.2.6-1: Table 13.2.6-1, Table 13.2.6-2, and Table 13.2.6-3 describe all pin assignments for 3U and 6U PSCs that are intended to provide final power to SOSA PICs; not all functions need to be implemented by the PSC, but it is assumed that backplane slots will be connected to accommodate all functions.

Rule 13.2.6-4: Unless a 3U or 6U PSC implements a function, the 3U or 6U PSC shall leave those function pins unconnected. Conformance Methodology (I)

Rule 13.2.6-5: 3U PSCs shall have an Alignment Key 1 set based on its expected input voltage in accordance with ANSI/VITA 62.0, Table 4.3.1-1. Conformance Methodology (I)

Rule 13.2.6-6: Where 3U PSCs provide final power to SOSA PICs, the PSC's Alignment Key 2 shall be set to 135°. Conformance Methodology (I)

Rule 13.2.6-7: 6U PSCs shall have an Alignment Key 1 set based on its expected input voltage in accordance with ANSI/VITA 62.0, Table 4.3.2-1. Conformance Methodology (I)

Rule 13.2.6-8: 6U PSCs shall have an Alignment Key 2 set based on its expected input voltage type in accordance with ANSI/VITA 62.0, Table 4.3.2-2. Conformance Methodology (I)

Rule 13.2.6-9: Where 6U PSCs provide final power to SOSA PICs, the PSC's Alignment Key 3 shall be set to 45°. Conformance Methodology (I)

Table 13.2.6-1: 3U P0 Connector Pin Out

3U P0 CONNECTOR PIN OUT			
PIN NUMBER	RATED CURRENT	Pin Name	12V Only
P1	40A	-DC_IN/ACN	-DC_IN/ACN
P2	40A	+DC_IN/ACL	+DC_IN/ACL
LP1	20A	CHASSIS	CHASSIS
A1	<1A	UD1	SYNC_OUT
B1	<1A	UD2	NVMRO
C1	<1A	UD3	GA2*
D1	<1A	UD4	Reserved
A2	<1A	VBAT	VBAT
B2	<1A	FAIL*	FAIL*
C2	<1A	INHIBIT*	INHIBIT*
D2	<1A	ENABLE*	ENABLE*
A3	<1A	UD0	SYNC_IN
B3	<1.5A	+12V_AUX	Reserved
C3	<1A	NED	NED
D3	<1A	NED_RETURN	NED_RETURN
A4	<1.5A	3.3V_AUX	Reserved
B4	<1.5A	3.3V_AUX	Reserved
C4	<1.5A	3.3V_AUX	Reserved
D4	<1.5A	3.3V_AUX	Reserved
A5	<1A	GA0*	GA0*
B5	<1A	GA1*	GA1*
C5	<1A	SM0	SM0
D5	<1A	SM1	SM1
A6	<1A	SM2	SM2

3U P0 CONNECTOR PIN OUT			
PIN NUMBER	RATED CURRENT	Pin Name	12V Only
B6	<1A	SM3	SM3
C6	<1.5A	-12V_AUX	Reserved
D6	<1A	SYSRESET*	SYSRESET*
A7	<1A	SHARE_1	SHARE_1
B7	<1A	SHARE_2	SHARE_2
C7	<1A	SHARE_3	SHARE_3
D7	<1A	SIGNAL RETURN	SIGNAL RETURN
A8	<1A	PO1_SENSE	SENSE, +12VDC
B8	<1A	PO2_SENSE	SENSE, 3.3V_AUX
C8	<1A	PO3_SENSE	SENSE, +12VDC
D8	<1A	SENSE RETURN	SENSE RETURN
P3	40A	PO3	+12VDC (Vs1)
P4	40A	POWER RETURN	POWER RETURN
P5	40A	POWER RETURN	POWER RETURN
LP2	20A	PO2	3.3V_AUX
P6	40A	PO1	+12VDC (Vs1)
Key 2			135°

Table 13.2.6-2: 6U P0 Connector Pin Out

6U P0 CONNECTOR PIN OUT					
PIN NUMBER	RATED CURRENT	PIN NAME	DC Input	AC 10	AC 30
P7	40A	+DCIN/ACL/L1	+DCIN	ACL	0A
P6	40A	+DC_IN/L2	+DCIN	N/C	0B
P5	40A	-DC_IN/L3	-DCIN	N/C	0C
P4	40A	-DC_IN/ACN	-DCIN	ACN	ACN

6U P0 CONNECTOR PIN OUT					
PIN NUMBER	RATED CURRENT	PIN NAME	DC Input	AC 10	AC 30
P3	40A	POS_FILT_OUT	POS_FILT_OUT	POS_FILT_OUT	POS_FILT_OUT
P2	40A	NEG_FILT_OUT	NEG_FILT_OUT	NEG_FILT_OUT	NEG_FILT_OUT
P1	40A	CHASSIS	CHASSIS	CHASSIS	CHASSIS
Key 2			0°	45°	90°

Table 13.2.6-3: 6U P1 Connector Pin Out

6U P1 CONNECTOR PIN OUT			
PIN NUMBER	RATED CURRENT	Pin Name	12V Only
P10	40A	PO1	+12VDC (Vs1, Vs2)
P9	40A	PO2	+12VDC (Vs1, Vs2)
A9	<1A	PO1_SENSE	SENSE, +12VDC
B9	<1A	PO2_SENSE	SENSE, +12VDC
C9	<1A	PO3_SENSE	SENSE, +12VDC
D9	<1A	UD0	SYNC_IN
A8	<1A	PO1_SENSE_RTN	SENSE_RTN, +12VDC
B8	<1A	PO2_SENSE_RTN	SENSE_RTN, +12VDC
C8	<1A	PO3_SENSE_RTN	SENSE_RTN, +12VDC
D8	<1A	UD1	SYNC_OUT
A7	<1A	SHARE_1	SHARE_1
B7	<1A	SHARE_2	SHARE_2
C7	<1A	SHARE_3	SHARE_3
D7	<1A	SIGNAL_RETURN	SIGNAL_RETURN
P8	40A	POWER_RETURN	POWER_RETURN
P7	40A	POWER_RETURN	POWER_RETURN
A6	<1A	SM2	SM2

6U P1 CONNECTOR PIN OUT			
PIN NUMBER	RATED CURRENT	Pin Name	12V Only
B6	<1A	SM3	SM3
C6	<1.5A	-12V_AUX	Reserved
D6	<1A	SYSRESET*	SYSRESET*
A5	<1A	GAP*	GAP*
B5	<1A	GA4*	GA4*
C5	<1A	SM0	SM0
D5	<1A	SM1	SM1
A4	<1A	GA3*	GA3*
B4	<1A	GA2*	GA2*
C4	<1A	GA1*	GA1*
D4	<1A	GA0*	GA0*
A3	<1A	UD2	NVMRO
B3	<1.5A	+12V_AUX	Reserved
C3	<1A	NED	NED
D3	<1A	NED_RETURN	NED_RETURN
P6	40A	PO3	+12VDC, (Vs1, Vs2)
P5	40A	PO3	+12VDC, (Vs1, Vs2)
P4	40A	POWER_RETURN	POWER_RETURN
P3	40A	POWER_RETURN	POWER_RETURN
A2	<1A	VBAT	VBAT
B2	<1A	FAIL*	FAIL*
C2	<1A	INHIBIT*	INHIBIT*
D2	<1A	ENABLE*	ENABLE*
A1	<1A	UD3	Reserved
B1	<1A	UD4	SHARE_4

6U P1 CONNECTOR PIN OUT			
PIN NUMBER	RATED CURRENT	Pin Name	12V Only
C1	<1A	UD5	3.3V_AUX SENSE
D1	<1A	UD6	3.3V_AUX_SENSE_RT N
P2	40A	3.3V_AUX	3.3V_AUX
P1	40A	POWER_RETURN	POWER_RETURN
Key 3			45°

13.2.6.1 PSC Input Rules

Rule 13.2.6.1-1: When a 3U PSC accepts DC Input Power, the 3U PSC shall have the more positive input on the +DC_IN/ACL pin. Conformance Methodology (I)

Rule 13.2.6.1-2: When a 3U PSC accepts DC Input Power, the 3U PSC shall have the more negative input on the -DC_IN/ACN pin. Conformance Methodology (I)

Rule 13.2.6.1-3: When a 3U PSC accepts single phase AC Input Power, the 3U PSC shall have the line input on the +DC_IN/ACL pin. Conformance Methodology (I)

Rule 13.2.6.1-4: When a 3U PSC accepts single phase AC Input Power, the 3U PSC shall have the neutral input on the -DC_IN/ACN pin. Conformance Methodology (I)

Rule 13.2.6.1-5: When a 6U PSC accepts DC Input Power, the 6U PSC shall have the more positive input on the +DC_IN/ACL/L1 and +DC_IN/L2 pins. Conformance Methodology (I)

Rule 13.2.6.1-6: When a 6U PSC accepts DC Input Power, the 6U PSC shall have the more negative input on the -DC_IN/L3 and -DC_IN/ACN pins. Conformance Methodology (I)

Rule 13.2.6.1-7: When a 6U PSC accepts single phase AC Input Power, the 6U PSC shall have the line input on the +DC_IN/ACL/L1 pin. Conformance Methodology (I)

Rule 13.2.6.1-8: When a 6U PSC accepts single phase AC Input Power, the 6U PSC shall have the neutral input on the -DC_IN/ACN pin. Conformance Methodology (I)

Rule 13.2.6.1-9: When a 6U PSC accepts three phase AC Input Power, the 6U PSC shall have the Phase A input on the +DC_IN/ACL/L1 pin. Conformance Methodology (I)

Rule 13.2.6.1-10: When a 6U PSC accepts three phase AC Input Power, the 6U PSC shall have the Phase B input on the +DC_IN/L2 pin. Conformance Methodology (I)

Rule 13.2.6.1-11: When a 6U PSC accepts three phase AC Input Power, the 6U PSC shall have the Phase C input on the -DC_IN/L3 pin. Conformance Methodology (I)

Rule 13.2.6.1-12: When a 6U PSC accepts three phase AC Input Power and utilizes the neutral connection, the 6U PSC shall have the neutral input on the -DC_IN/ACN pin. Conformance Methodology (I)

13.2.6.2 *PSC Power Outputs*

Rule 13.2.6.2-1: When 3U PSCs provide final power to SOSA PICs, the 3U PSCs shall output 12V Final Power intended for connection to Vs1 on the PO1 and PO3 pins. Conformance Methodology (I)

Rule 13.2.6.2-2: When 3U PSCs provide final power to SOSA PICs, the 3U PSCs shall output 3.3V_AUX Final Power intended for connection to 3.3V_AUX on the PO2 pin. Conformance Methodology (I)

Rule 13.2.6.2-3: When 6U PSCs provide final power to SOSA PICs, the 6U PSCs shall output 12V Final Power intended for connection to Vs1 and Vs2 on the PO1 and PO2 pins. Conformance Methodology (I)

Permission 13.2.6.2-1: When 6U PSCs provide final power to SOSA PICs, the 6U SOSA PSCs may output 12V Final Power intended for connection to Vs1 and Vs2 on the PO3 pin. Conformance Methodology (I)

Rule 13.2.6.2-4: When 6U PSCs provide final power to SOSA PICs, the 6U PSCs shall output 3.3V_AUX intended for connection to 3.3V_AUX on the 3.3V_AUX pin. Conformance Methodology (I)

Rule 13.2.6.2-5: PSCs shall utilize the POWER_RETURN pins as the return path for output current. Conformance Methodology (I)

Rule 13.2.6.2-6: Backplanes utilizing PSCs shall connect all POWER_RETURN and SIGNAL_RETURN pins of all like PSCs together on the backplane. Conformance Methodology (T)

Observation 13.2.6.2-1: This document requires that PICs do not draw power from Vs2, Vs3, or +/-12V Aux for 3U PICS and VS3 or +/-12V Aux for 6U PICS; therefore, SOSA PSCs do not need to provide these voltages.

13.2.6.3 *PSC 3U Output Support*

Rule 13.2.6.3-1: When 3U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 12V Power output, the 3U PSCs shall utilize the PO1_SENSE and SENSE_RETURN pins for this function. Conformance Methodology (I)

Permission 13.2.6.3-1: When 3U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 12V Power output, the 3U PSCs may utilize the PO3_SENSE and SENSE_RETURN pins for this function. Conformance Methodology (I)

Rule 13.2.6.3-2: When 3U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 3.3V_AUX Power output, the 3U PSCs shall utilize the PO2_SENSE and SENSE_RETURN pins for this function. Conformance Methodology (I)

Rule 13.2.6.3-3: 3U PSCs that implement Active Current Sharing shall utilize the SHARE_1, SHARE_2, and SHARE_3 pins. Conformance Methodology (I)

Rule 13.2.6.3-4: Backplanes utilizing 3U PSCs shall buss SHARE_1, SHARE_2, and SHARE_3 among all power supplies slots of the same type.

13.2.6.4 *PSC 6U Output Support*

Rule 13.2.6.4-1: When 6U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 12V Power output, the 6U PSCs shall utilize the PO1_SENSE and PO1_SENSE_RETURN pins for this function. Conformance Methodology (I)

Permission 13.2.6.4-1: When 6U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 12V Power output, the 6U PSCs may utilize the PO2_SENSE, PO3_SENSE, PO2_SENSE_RETURN, and PO3_SENSE_RETURN pins for this function. Conformance Methodology (I)

Rule 13.2.6.4-2: When 6U PSCs which provide final power to SOSA PICs implement Remote Sensing on the 3.3V_AUX Power output, the 6U PSCs shall utilize the 3.3V_AUX_SENSE and 3.3V_AUX_SENSE_RETURN pins for this function. Conformance Methodology (I)

Rule 13.2.6.4-3: 6U PSCs that implement Active Current Sharing shall utilize the SHARE_1, SHARE_2, SHARE_3, and SHARE_4 pins. Conformance Methodology (I)

Rule 13.2.6.4-4: Backplanes utilizing 6U PSCs shall buss SHARE_1, SHARE_2, SHARE_3, and SHARE_4 among all power supplies slots of the same type. Conformance Methodology (T)

13.2.6.5 *PSC Utility Plane Signals*

Rule 13.2.6.5-1: PSCs shall implement an IPMC using the SM[3:0] pins. Conformance Methodology (I)

Rule 13.2.6.5-2: 3U PSCs shall implement GA0* and GA1*. Conformance Methodology (I)

Rule 13.2.6.5-3: When a 3U PSC implements GA2*, the 3U PSC shall use the pin assigned in Table 13.2.6-1 to increase the number of PSCs which can be addressed from four to eight. Conformance Methodology (I)

Rule 13.2.6.5-4: 6U PSCs shall implement the complete geographical addressing. Conformance Methodology (I)

Rule 13.2.6.5-5: When PSCs are capable of sourcing VBAT, the PSCs shall provide a voltage between 2.55V and 3.50V. Conformance Methodology (T)

Rule 13.2.6.5-6: When PSCs draw power from VBAT, the PSCs shall draw no more than 1mA. Conformance Methodology (I)

Rule 13.2.6.5-7: PSCs shall provide details on the operation of the SYSRESET* pin. Conformance Methodology (I)

Rule 13.2.6.5-8: When PSCs provide final power to SOSA PICs, the PSCs shall implement ENABLE* and INHIBIT* such that the state of the PSC outputs follow those shown in Table 13.2.6.5-1. Conformance Methodology (I)

Table 13.2.6.5-1: ENABLE* and INHIBIT* Values

Control Inputs		Power Outputs	
ENABLE*	INHIBIT*	3.3V_AUX	+12V Output
High	High	Off	Off

Control Inputs		Power Outputs	
High	Low	Off	Off
Low	High	On	On
Low	Low	On	Off

Rule 13.2.6.5-9: When PSCs implement Nuclear Event Detection, the PSCs shall use the NED and NED_RETURN pins for this function. Conformance Methodology (I)

Rule 13.2.6.5-10: PSCs shall utilize SIGNAL_RETURN as the return path for ENABLE*, INHIBIT*, FAIL*, SYSRESET*, VBAT, GAx*, and SM[0:3]. Conformance Methodology (I)

13.2.6.6 PSC 3U and 6U SYNC Signals

Rule 13.2.6.6-1: When PSCs implement SYNC_IN, the PSCs shall use the SYNC_IN pin to input the synchronization signal. Conformance Methodology (I)

Rule 13.2.6.6-2: When 3U and 6U PSCs implement SYNC_OUT, the PSCs shall use the SYNC_OUT pin to output the synchronization signal. Conformance Methodology (I)

Rule 13.2.6.6-3: SOSA PSCs shall provide details on the operation and signal requirements of the SYNC_IN and SYNC_OUT pins. Conformance Methodology (I)

Rule 13.2.6.6-4: When any output voltage is out of specification, the PSC shall assert the FAIL* signal. Conformance Methodology (T)

Rule 13.2.6.6-5: The PSC CHASSIS pin shall connect to PSC front panel and covers. Conformance Methodology (T)

Rule 13.2.6.6-6: The PSC CHASSIS pin shall be isolated from the SIGNAL_RETURN pin. Conformance Methodology (T)

Rule 13.2.6.6-7: The PSC CHASSIS pin shall be isolated from the POWER_RETURN pins. Conformance Methodology (T)

Rule 13.2.6.6-8: The PSC CHASSIS pin shall be isolated from the –DC/ACN pin. Conformance Methodology (T)

Rule 13.2.6.6-9: PSCs outputting an intermediate power shall explicitly define the nominal output voltage and the output voltage range, for the intermediate power. Conformance Methodology (I)

Rule 13.2.6.6-10: PSCs having intermediate power as an input shall explicitly define the nominal input voltage and the input voltage range, for the intermediate power. Conformance Methodology (I)

Rule 13.2.6.6-11: Energy Storage Modules shall accept an input of the intermediate voltage in accordance with ANSI/VITA 62.0 §4.5. Conformance Methodology (I)

Rule 13.2.6.6-12: Energy Storage Modules shall output the intermediate voltage in accordance with ANSI/VITA 62.0 §4.5. Conformance Methodology (T)

Rule 13.2.6.6-13: 6U Single-Stage Power Modules shall route the intermediate voltage to the ANSI/VITA 62.0 pins labeled “POS_FILT_OUT” and “NEG_FILT_OUT” in accordance with ANSI/VITA 62.0 §6.5.2. Conformance Methodology (A)

Rule 13.2.6.6-14: 3U PSCs shall conform to the mechanical requirements of ANSI/VITA 48.2 for 3U conduction cooled modules except where specified herein. Conformance Methodology (I)

Rule 13.2.6.6-15: 6U PSCs shall conform to the mechanical requirements of ANSI/VITA 48.2 for 6U conduction cooled modules except where specified herein. Conformance Methodology (I)

13.2.7 Mezzanine Cards

Permission 13.2.7-1: Non-conformant SOSA Mezzanine Cards may be used.

Rule 13.2.7-1: XMC Mezzanine Cards that do not require utilization of all available user I/O signals shall leave the remaining unused signals as no connects. Conformance Methodology (A)

Recommendation 13.2.7-1: The higher-priority I/O signals of the XMC Mezzanine Card should populate pins in the following order of ANSI/VITA 46.9 patterns: Conformance Methodology (A)

- X12d
- X8d
- X16s
- X24s

Observation 13.2.7-1: Any XMC module (SOSA Mezzanine Cards or otherwise) will be expected to be subject to qualification testing while installed on a target Payload Module within the constraints of the target system deployed configuration and environment, including all hardware and accessories.

Rule 13.2.7-2: If a Payload PIC has an XMC Mezzanine Card site, the Payload PIC shall route the ANSI/VITA 42.0-defined I²C connections from the XMC Mezzanine Card site to the IPMC of the Payload PIC. Conformance Methodology (A)

13.2.8 Maintenance Console Port

The Maintenance Console Port is intended to be a consistently implemented port providing a console for low-level access to the attached processor. It is not intended to be an “operational” port; that is, not intended to communicate to some device as part of the normal operation of the system. It is intended strictly as a part of the board maintenance functions.

The basic use-cases for the maintenance console port can be classed as described below.

13.2.8.1 *Vendor Board Bring Up, Board Support Package (BSP) Development, etc.*

This implies access to low-level firmware, Basic Input/Output System (BIOS), Extensible Firmware Interface (EFI) shell, etc. The typical case is for an operator to attach to the maintenance console port of a single PIC using a terminal or PC. There is also a case where the operator could attach to a relatively limited set of boards at one time.

13.2.8.2 *Integrator Application Development and Debug*

This also implies access to low-level firmware, BIOS, EFI shell, etc. This will typically be performed in a lab environment with the target PIC installed in either an “open” lab chassis or a target deployable chassis. The operator could attach to a relatively limited set of boards at one time, but there could be cases where the operator could need to attach to every maintenance console port in the system.

13.2.8.3 *Deployed System*

In this case the target PIC is installed in a deployed system. Whether or not the maintenance console ports on the individual boards are accessible in a deployed system is up to the system integrator, but assuming the ports are accessible, it can be assumed that most, if not all, of the individual PIC maintenance console ports can be attached. It is also assumed that some sort of port aggregation mechanism is implemented within the system to provide this access.

13.2.8.4 *Maintenance Depot*

The maintenance depot use-case can be characterized by the need to access the maintenance console ports of an individual fieldable PIC in a lab test fixture. The port will facilitate debug and perhaps upgrade/updates of the PIC.

The SOSA Maintenance Console Port is defined to operate at Low Voltage Complementary Metal Oxide Semiconductor (LVCMOS) levels rather than traditional Telecommunications Industrial Association (TIA) 232 levels. The reason is that there is a desire in SOSA platforms to support an aggregator function for the various Maintenance Console Ports, giving system designers the ability to access any Maintenance Console Port in the system from a single interface (or, perhaps, a limited number). The use of LVCMOS rather than traditional TIA 232 levels allows the aggregator to be generally smaller and simpler – often implemented with an FPGA or Complex Programmable Logic Device (CPLD).

Note: Board designers are not prohibited from supporting TIA 232 levels for these ports, so long as they provide a mechanism to support the requirements documented here.

These ports all share a common implementation defined as follows.

Rule 13.2.8.4-1: The Maintenance Console Port shall be a two-pin serial interface implementing the Universal Asynchronous Receiver/Transmitter (UART) protocol. Conformance Methodology (I)

Rule 13.2.8.4-2: The Maintenance Console Port shall use LVCMOS signaling non-inverted (active high) with the following levels (see Table 13.2.8.4-1). Conformance Methodology (A, T)

Table 13.2.8.4-1: Maintenance Console Port Signal Levels

Description	Maintenance Console Voltage	LVCMOS Serial ANSI/VITA 65.0	GPIO ANSI/VITA 65.0
Vcc	3.3V +/- 0.3V	N/A	N/A
Vih	1.7V	2.0	2.0
Vil	0.7V	0.8	0.8

Description	Maintenance Console Voltage	LVC MOS Serial ANSI/VITA 65.0	GPIO ANSI/VITA 65.0
Voh	2.0V	2.4@2ma	2.4@8ma
Vol	0.4V	0.4@2ma	0.4@8ma

Observation 13.2.8.4-1: The Maintenance Console Port non-inverted (active high) signaling permits the addition of an external TIA 232 transceiver to provide a proper signal polarity to TIA 232 devices.

Rule 13.2.8.4-3: The Maintenance Console Port shall support, at a minimum, 115,200 bits/sec, 57,600 bits/sec, and 9600 bits/sec (H/M/L speed), 8 bits, no parity, one stop bit. Conformance Methodology (I)

Permission 13.2.8.4-1: Maintenance Console Ports are permitted to support additional speeds and protocol settings.

13.2.9 Overlays

There are several Slot Profiles that allow the use of undefined pins or defined pins with undefined function.

The 3U and 6U I/O Intensive Slot Profiles support XMC module pin mapping to the backplane.

To limit the number of PICPs that are largely redundant, the concept of a pin out “overlay” is introduced. This allows the creation of various functional uses of these otherwise undefined pins to be codified within this document.

SOSA systems could need to support NSA Type 1-approved high-assurance security functions for applications that could process classified information. These implementations generally require special functions and interfaces to support their high-assurance services. This overlay defines those special interfaces and where they map to the 3U I/O Intensive Slot Profile and the XMC-enabled 6U Payload Card backplane connections.

It should be noted that while there is a Radial AUXCLK/REFCLK Slot Profile for 3U, no such Slot Profile exists for 6U PICs. However, this can be implemented using an overlay.

Figure 13.2.9-1 depicts a notional security overlay with special purpose signaling for distributing REF_CLK and AUX_CLK to the backplane and other PIC slots.

Note: The requirements associated with the Security Module Overlay are contained in Appendix C.

Plug-in module	Row G	Row F	Row E		Row D	Row C	Row B		Row A
			Even	Odd			Even	Odd	
Bplane J5	Row i	Row h	Row g	Row f	Row e	Row d	Row c	Row b	Row a
1	MPO2-TD	GND	GND-J5	REFCLK14_L1	REFCLK14_L0	GND	GND-J5	REFCLK15_L1	REFCLK15_L0
2	GND	REFCLK00_L1	REFCLK00_L0	GND-J5	GND	REFCLK01_L1	REFCLK01_L0	GND-J5	GND
3	MPO2-RD	GND	GND-J5	REFCLK02_L1	REFCLK02_L0	GND	GND-J5	REFCLK03_L1	REFCLK03_L0
4	GND	REFCLK04_L1	REFCLK04_L0	GND-J5	GND	REFCLK05_L1	REFCLK05_L0	GND-J5	GND
5	GPI005	GND	GND-J5	REFCLK06_L1	REFCLK06_L0	GND	GND-J5	REFCLK07_L1	REFCLK07_L0
6	GND	REFCLK08_L1	REFCLK08_L0	GND-J5	GND	REFCLK09_L1	REFCLK09_L0	GND-J5	GND
7	GPI006	GND	GND-J5	REFCLK10_L1	REFCLK10_L0	GND	GND-J5	REFCLK11_L1	REFCLK11_L0
8	GND	REFCLK12_L1	REFCLK12_L0	GND-J5	GND	REFCLK13_L1	REFCLK13_L0	GND-J5	GND
9	GPI007	GND	GND-J5	AUXCLK14_L1	AUXCLK14_L0	GND	GND-J5	AUXCLK15_L1	AUXCLK15_L0
10	GND	AUXCLK00_L1	AUXCLK00_L0	GND-J5	GND	AUXCLK01_L1	AUXCLK01_L0	GND-J5	GND
11	GPI008	GND	GND-J5	AUXCLK02_L1	AUXCLK02_L0	GND	GND-J5	AUXCLK03_L1	AUXCLK03_L0
12	GND	AUXCLK04_L1	AUXCLK04_L0	GND-J5	GND	AUXCLK05_L1	AUXCLK05_L0	GND-J5	GND
13	GPI009	GND	GND-J5	AUXCLK06_L1	AUXCLK06_L0	GND	GND-J5	AUXCLK07_L1	AUXCLK07_L0
14	GND	AUXCLK08_L1	AUXCLK08_L0	GND-J5	GND	AUXCLK09_L1	AUXCLK09_L0	GND-J5	GND
15	GPI010	GND	GND-J5	AUXCLK10_L1	AUXCLK10_L0	GND	GND-J5	AUXCLK11_L1	AUXCLK11_L0
16	GND	AUXCLK12_L1	AUXCLK12_L0	GND-J5	GND	AUXCLK13_L1	AUXCLK13_L0	GND-J5	GND

Figure 13.2.9-1: AUXCLK/RECLK Distribution Overlay

Rule 13.2.9-1: The XMC map definition for the Payload Slot Profile SLT3-PAY-1F1F2U1TU1T1U1T-14.2.16 shall be selected from the Alternate Module Profile Scheme (AMPS) Protocol Table for XMC Type A Overlay (Table 13.2.9-1) Conformance Methodology (I)

Rule 13.2.9-2: The XMC map definition for the Payload Slot Profile SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n shall be selected from AMPS Protocol Table for XMC Type B Overlay (Table 13.2.9-2). Conformance Methodology (I)

Table 13.2.9-1: SLT3-PAY-1F1F2U1TU1T1U1T-14.2.16 Overlay Description

XMC Type A Overlay (SOSA Only)		ANSI/VITA 65.0 Sections for Electrical Protocols
N	Not Connected	N/A
XA0	User-defined: X12d+X8d+X16s	N/A
XA1	GPIO/GPLVDS: X12d+X8d+X16s	5.15.1/5.15.2
XA2	Security	N/A

Table 13.2.9-2: SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n Overlay Description

XMC Type B Overlay (SOSA Only)		ANSI/VITA 65.0 Sections for Electrical Protocols
N	Not Connected	N/A
XB0	User-defined: X12d+X8d+X24s	N/A
XB1	GPIO/GPLVDS: X12d+X8d+X24s	5.15.1/5.15.2
XB2	Security	N/A

13.2.10 Certificate of Volatility (CoV)

A Certificate of Volatility (CoV), sometimes referred to as a Letter or Statement of Volatility, is a common piece of user documentation provided by hardware vendors in the SOSA marketplace. This document describes the different types of memory found on a hardware element, how to write to and clear the memory, and if there are any mechanisms to prevent memories from being written (e.g., a jumper that, when installed, prohibits anything from writing to a memory). Some memory could be embedded within a non-memory component (such as non-volatile storage in an FPGA). A CoV is expected to describe all non-volatile (NVM) memory located on a hardware element, even if that memory is embedded within another component. It should also describe any discrete volatile memory.

Rule 13.2.10-1: Each conformable hardware element shall include as a part of the user documentation package a CoV. Conformance Methodology (I)

Observation 13.2.10-1: The intention of the CoV is to document, for the user of the hardware element, the memories provided by the hardware element along with their volatility and NVMRO protection.

Observation 13.2.10-2: Hardware element vendors could require a Non-Disclosure Agreement (NDA) to be in place before providing a CoV.

Observation 13.2.10-3: Components might have internal undocumented NVM, which is outside the scope of what is covered in a CoV.

Rule 13.2.10-2: The hardware element CoV, shall, at a minimum, include the following: Conformance Methodology (I)

- Name of PIC vendor
- Product(s) covered by documentation (e.g., product name, family name, part number, as appropriate)

For each memory on the hardware element:

- Memory manufacturer and part number (note that “or equivalent” could be used in the case of multiple parts on an Approved Vendor List (AVL))
- Volatile memory type (SRAM, SDRAM, etc.)
- Non-volatile memory type (NAND Flash, NOR Flash, MRAM, optical, NVMe, etc.)
- Memory size
- Memory functionality (Boot Flash, Interface Chip Firmware, user memory, etc.)
- How memory can be written (e.g., application code, JTAG, etc.)
- Write protection mechanism, if present (including the NVMRO signal, user-settable jumpers, or switches, etc.)

For volatile memories:

- Declare any internal power source (e.g., battery, supercap) that allows it to retain its contents once removed from main power

- A statement that “memory is cleared when power removed” or similar is acceptable if there is no internal power source

13.2.11 3U SOSA PICPs – General

A SOSA PICP defines the connector type and how each pin, or pair of pins, is allocated. The allocation of pins with a prescribed set of communication protocols is accomplished via AMPS. (See Section 13.3 for a complete description of AMPS.) Single pins are generally allocated to the Utility Plane for power, grounds, system discrete signals, and system management. Differential pin/pairs are generally allocated for the three communication planes called Control, Data, and Expansion. Differential paired pins are grouped together to form “pipes”. Finally, PICPs also determine which pins are user-defined. SOSA PICPs are categorized as either Payload or Switch. As an example, payload PICs are further divided into sub-categories such as, but not limited to, RF Payload, RF Switch, and I/O Single Board Computer (SBC).

Rule 13.2.11-1: When a PIC is an ANSI/VITA 65.0 3U PIC, it shall be designed to one of the following ANSI/VITA 65.0 Slot Profiles:

- SLT3-PAY-1F1F2U1TU1T1U1T-14.2.16
- SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n, where allowable dash options for –n are specified in Table 13.2.11.2-1
- SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n, where allowable dash options for –n are specified in Table 13.2.11.2-2
- SLT3-SWH-6F8U-14.4.15
- SLT3-SWH-6F1U7U-14.4.14
- SLT3-SWH-4F1U7U1J-14.8.7-n, where allowable dash options for –n are specified in Table 13.2.11.4-1
- SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n, where allowable dash options for –n are specified in Table 13.2.11.5-1
- SLT3-PAY-2U2U-14.2.17
- SLT3-PAY-1F1U1S1S1U1U1K-14.6.14-n, where allowable dash options for –n are specified in Table 13.2.11.7-1

As defined in ANSI/VITA 65.0, a SOSA PICP which references an ANSI/VITA Slot Profile is giving the physical mapping of connector pins to ports. In the case of a SOSA PICP which references ANSI/VITA 65.0 Slot Profiles with apertures for coax and optical contacts, there is a dash option at the end of an ANSI/VITA 65.0 Slot Profile name, which is an index into a table of dash options, for the ANSI/VITA 65.0 Slot Profile, as shown in ANSI/VITA 65.1. When ANSI/VITA 65.0 Slot Profiles are referred to, without reference to a particular dash option, a “-n” is used to indicate this. An example of an ANSI/VITA 65.0 Slot Profile name without specifying the loading of the aperture is:

- SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n

For this Slot Profile, a dash option of 4 indicates the aperture is filed with an RF Connector module with 14 SubMiniature Push-on Micro (SMPM) contacts, in which case the Slot Profile name is:

- SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-4

For examples, see Table 13.2.11.2-1.

To fully specify SOSA PICPs, AMPS Strings are used. AMPS Strings specify both the Slot Profile, including the Slot Profile dash option and the protocols assigned to the Slot Profile ports. See Section 13.3 for a description of AMPS.

13.2.11.1 3U I/O Intensive Single Board Computer (SBC) PICP

This ANSI/VITA Slot Profile in Figure 13.2.11.1-1 is intended for Payload PICs with lots of standard I/O, such as USB, DisplayPort, serial ports, etc. with the option for an XMC. This type of PIC is frequently referred to as an SBC. For compute-intensive applications with no standard I/O, use the Payload Profiles of Section 13.2.11.2.

The XMC site on this PIC is intended to be used for system-specific interfaces. For systems needing interfaces not available as part of SOSA Profiles, XMCs are how additional I/Os can be added beyond those defined by the standard SOSA PICPs. This VITA Slot Profile makes a subset of the XMC pins available to the backplane: the ANSI/VITA 46.9 P1w9-X12d, X8d, and X16s mappings.

The use of an XMC enables logic that is system-specific to be on the XMC, so that it can be upgraded less often than the SBC carrier on which it is sitting. This methodology also localizes the system-specific logic to the XMC, possibly making the XMC a custom (or customized) board, while the carrier can be a COTS SBC. If this does not provide enough I/O pins to meet the needs for system-specific signals, a less desirable option is to use the PIC of Section 13.2.11.6.

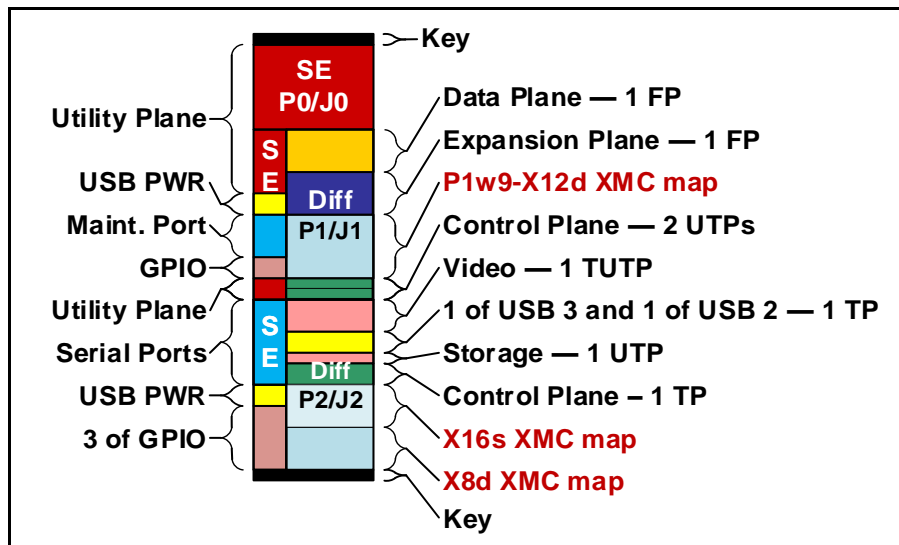


Figure 13.2.11.1-1: ANSI/VITA 65.0 3U I/O-Intensive SBC Slot Profile SLT3-PAY-1F1F2U1TU1T1U1T-14.2.16

Rule 13.2.11.1-1: The backplane shall not route GPIO signals between slots intended for SOSA PICs. Conformance Methodology (I)

Rule 13.2.11.1-2: Unless signals from XMC are from an XMC Overlay Profile, the backplane shall not route XMC signals between slots intended for SOSA PICs. Conformance Methodology (A)

Observation 13.2.11.1-1: An XMC can be used to customize the I/O for a system or platform.

13.2.11.2 3U Payload PICPs

The PICPs of Figure 13.2.11.2-1 or Figure 13.2.11.2-2 are intended to be used as the workhorse of the system. They are intended for, but not limited to, SBCs that are computationally intensive, FPGAs, and RF transceivers. Figure 13.2.11.2-1 is the primary choice *versus* Figure 13.2.11.2-2. If additional Expansion Planes are needed, then the VITA Slot Profile of Figure 13.2.11.2-2 can be used. Notice that if the P2A connector of the VITA Slot Profile of Figure 13.2.11.2-2 is not present and there is no RF/optical present, a PIC adhering to this Slot Profile can go into a slot adhering to the VITA Slot Profile of Figure 13.2.11.2-1.

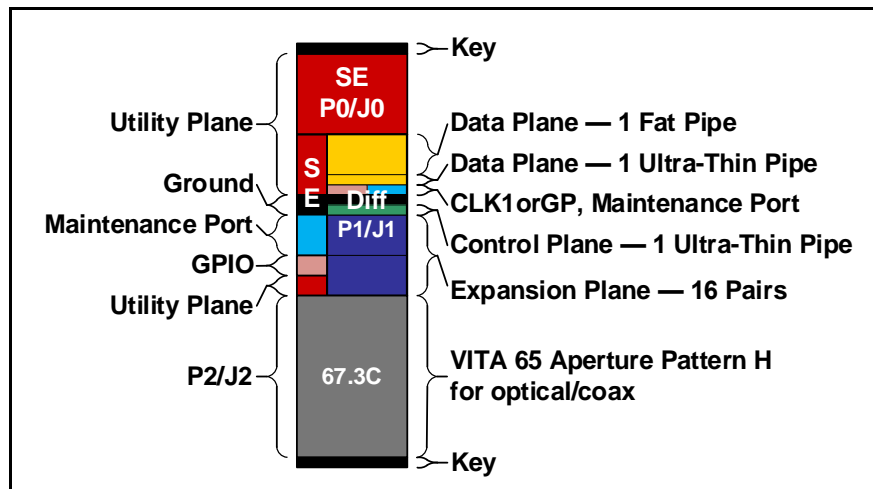


Figure 13.2.11.2-1: ANSI/VITA 65.0 Payload Slot Profile SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n

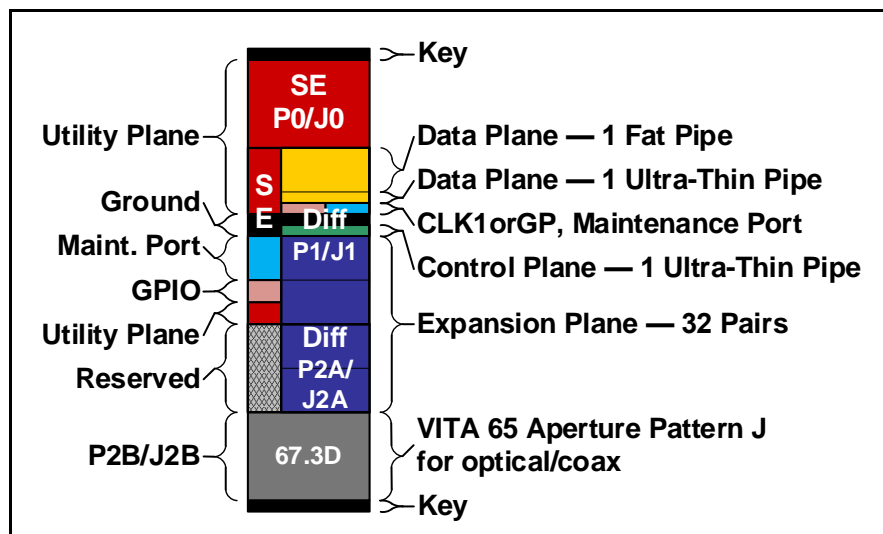


Figure 13.2.11.2-2: ANSI/VITA 65.0 Payload Slot Profile SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n

Recommendation 13.2.11.2-1: Suppliers that use ANSI/VITA 65.1 Slot Profile SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n should provide a build option to not populate the ANSI/VITA 46.0 connector in P2A so that the card can also be used in a backplane adhering to SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n. Conformance Methodology (A)

Recommendation 13.2.11.2-2: SOSA 3U Payload PICs that do not require RF or optical should conform to ANSI/VITA 65.1 module profile MOD3-PAY-1F1U1S1S1U1U2F1H-16.6.11-11. Conformance Methodology (I)

Observation 13.2.11.2-1: SOSA 3U Payload PICs can include, but are not limited to, SBCs that are computationally intensive, FPGAs, and RF transceivers.

Observation 13.2.11.2-2: The meaning of optical interface codes used in the following tables is defined by ANSI/VITA 65.0 and referred to by ANSI/VITA 65.0 as Optical Profiles. The Optical Profiles shown in the last column of Table 13.2.11.2-1 and Table 13.2.11.2-2 have this meaning: MT = Fiber Interface, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

Table 13.2.11.2-1: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT3-PAY-1F1U1S1S1U1U2F1H-14.6.11-n , where n is a "Dash Num" from this table.							
Dash Num	STD Date	Connector Modules				P2A/J2A	P2B/J2B
		P1B/J1B	P2A/J2A	P2B/J2B	P2A/J2A		
		VITA 46	Aperture H			MT loading and Optical	
0	2017-05	VITA 46	Empty				
1*	2017-05	VITA 46	Hybrid_66.4+67.1-6.4.5.6.1				
2*	2019-11	VITA 46	10_SMPM_contacts-6.4.5.6.3				
4	2019-11	VITA 46	14_SMPM_contacts-6.4.5.6.4				
5	Ready	VITA 46	19 SMPS contacts-6.4.5.6.6				
6	Ready	VITA 46	2 Style C inserts and 10 NanoRF contacts - 6.4.5.6.8			MT-MM12-1F-6.5.2.2	
10	Ready	VITA 46	1 Style C insert and 14 NanoRF contacts – 6.4.5.6.9			MT-MM12-1F-6.5.2.2	
12	Ready	VITA 46	2 Style C insert and 20 NanoRF contacts – 6.4.5.6.10			MT-MM12-1F-6.5.2.2	
14	Ready	VITA 46	2 Style D inserts – 6.4.5.6.11			MTA-MM12-3F-6.5.2.2, MTB - MM24 - 6.5.3.5, MTC - MM24 - 6.5.3.5	
* These Slot Profile dash options are legacy.							

Table 13.2.11.2-2: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n , where n is a "Dash Num" from this table.					
Dash Num	STD Date	Connector Modules			
		P1B/J1B	P2A/J2A	P2B/J2B	P2B/J2B
		VITA 46	VITA 46	Aperture H	MT loading and Optical Pipes
0	2019-11	VITA 46	VITA 46	Empty	
1	Ready	VITA 46	VITA 46	9 NanoRF contacts - 6.4.5.7.2	
2	Ready	VITA 46	VITA 46	1 Style C insert and 5 NanoRF contacts – 6.4.5.7.3	MT-MM12-1F-6.5.2.2
4	Ready	VITA 46	VITA 46	1 Style C insert and 10 NanoRF contacts – 6.4.5.7.4	MT-MM12-1F-6.5.2.2
8	Ready	VITA 46	VITA 46	1_Style_D_insert-6.4.5.7.6	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5 MTC-MM24-3F-6.5.3.5
* These Slot Profile dash options are legacy.					

13.2.11.3 3U Expansion Plane/Control Plane Switch PICP

The VITA Slot Profile of Figure 13.2.11.3-1 is intended to be used as an Expansion Plane. The version of the Slot Profile at the top of the figure is as it is documented in ANSI/VITA 65.0. In this document, what ANSI/VITA 65.0 has as the Data Plane is being used to switch the Expansion Plane instead, as shown in the bottom half of the figure. (This is allowed by ANSI/VITA 65.0, Permission 6.2.6-1.) Additionally, this Profile can be used to switch the Control Plane.

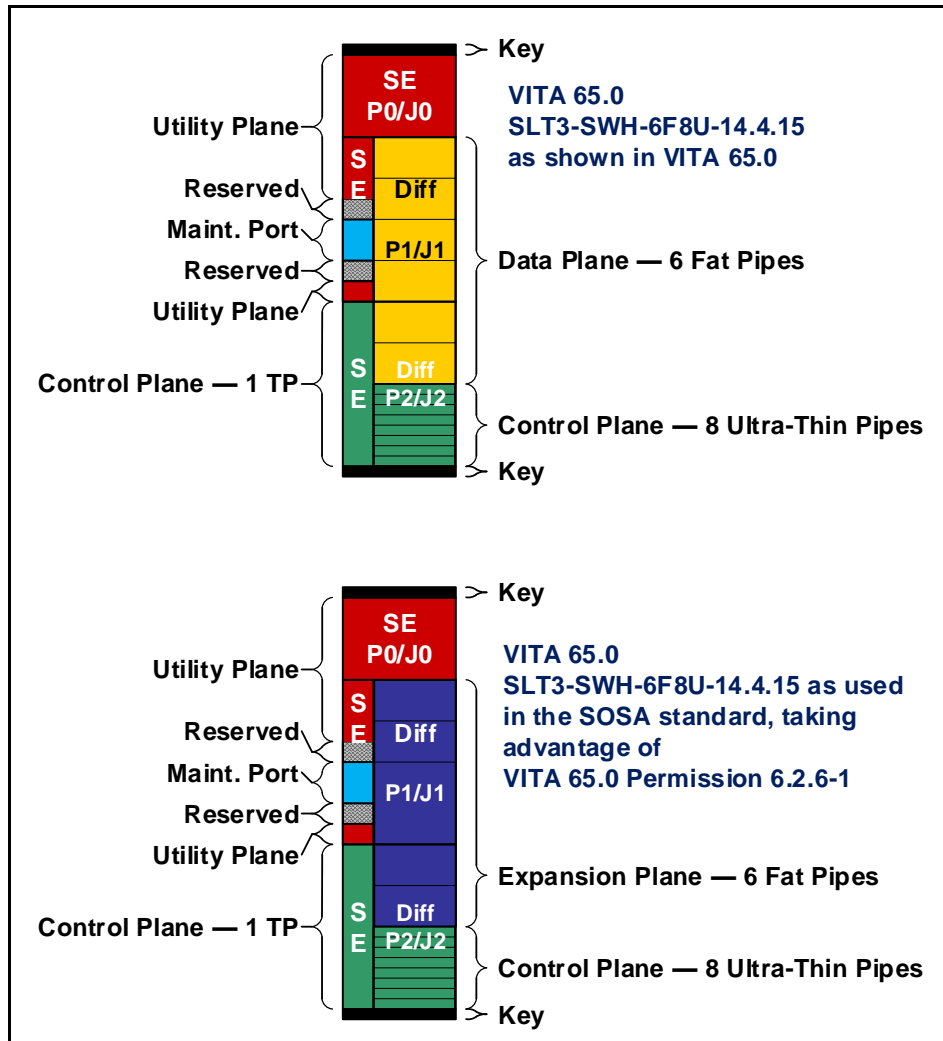


Figure 13.2.11.3-1: ANSI/VITA 65.0 Switch Slot Profile SLT3-SWH-6F8U-14.4.15

Observation 13.2.11.3-1: This 3U SOSA switch might not be required in smaller chassis as the Expansion Plane can be connected directly between payload cards. The requirement for this switch increases as the chassis size grows if there is a need to maintain Expansion Plane connectivity amongst all of the payload cards. This will probably be more common in compute-intensive systems where data is offloaded to an FPGA or General-Purpose Graphics Processing Unit (GPGPU).

13.2.11.4 3U Data/Control Plane Switch PICP

The VITA Slot Profiles of Figure 13.2.11.4-1 and Figure 13.2.11.4-2 are used for switching the Data and Control Planes. If optical connections are needed, the Slot Profile of Figure 13.2.11.4-1 is recommended; otherwise, the Slot Profile of Figure 13.2.11.4-2 is recommended. The Slot Profile in Figure 13.2.11.4-1 has two more Data Plane FPs than the one of Figure 13.2.11.4-2. Although the Data Plane of these Slot Profiles is shown as FPs, ANSI/VITA 65.0 has permissions for them to be repartitioned into Ultra-Thin Pipes (UTPs). Notice that the Payload Profiles of this section have both an FP and a UTP. Repartitioning some of the FPs of these Switch Profiles enables them to switch both Data Plane FPs and UTPs.

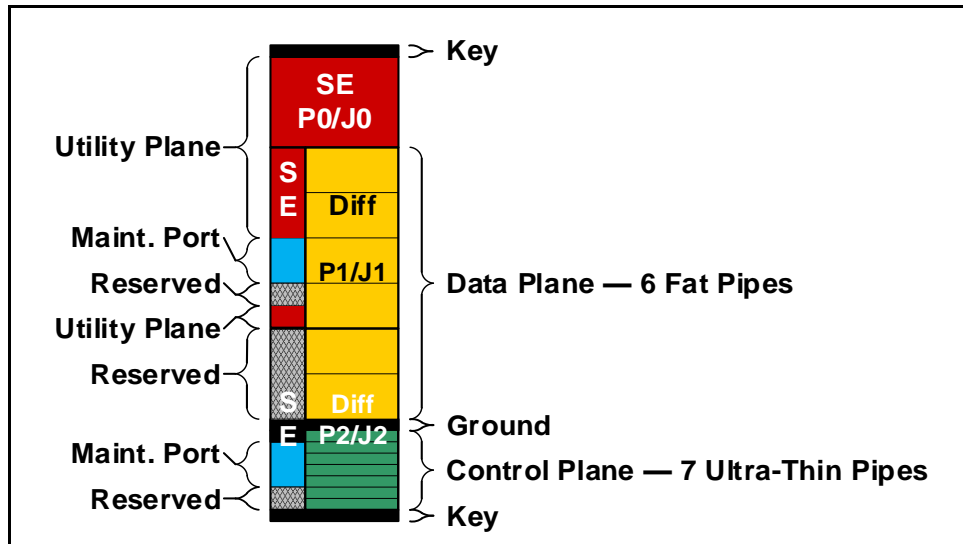


Figure 13.2.11.4-1: ANSI/VITA 65.0 Data/Control Plane Switch Slot Profile SLT3-SWH-6F1U7U-14.4.14

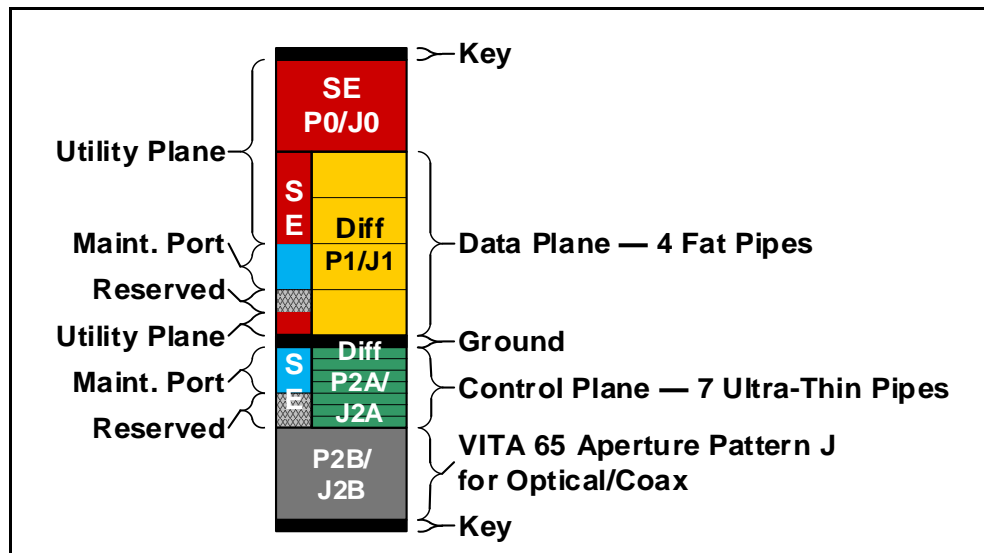


Figure 13.2.11.4-2: ANSI/VITA 65.0 Data/Control Plane Switch Slot Profile SLT3-SWH-4F1U7U1J-14.8.7-n

Permission 13.2.11.4-1: The Control Plane pipes in ANSI/VITA 65.1 Slot Profiles SLT3-SWH-6F1U7U-14.4.14 and SLT3-SWH-4F1U7U1J-14.8.7-n may be repurposed to provide a second Data Plane switch fabric.

Permission 13.2.11.4-2: Fiber connections on the front of the ANSI/VITA 65.1 SLT3-SWH-6F1U7U-14.4.14 and the SLT3-SWH-4F1U7U1J-14.8.7-n Slot Profiles may be used for Ethernet in/out of the chassis if blind-mate fiber connections are not available or practical.

Recommendation 13.2.11.4-1: Suppliers of a card based on the ANSI/VITA 65.1 Slot Profile SLT3-SWH-6F1U7U-14.4.14 should offer a variant of this card that can be used in a backplane with a Switch Slot for SLT3-SWH-4F1U7U1J-14.8.7-0 (i.e., P2B is empty). Conformance Methodology (A)

Observation 13.2.11.4-1: The meanings of optical interface codes used in Table 13.2.11.4-1 are defined by ANSI/VITA 65.0 and are referred to by ANSI/VITA 65.0 as Optical Profiles. The Optical Profiles shown in the last column of Table 13.2.11.4-1 have the meaning: MT = Fiber Interface, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

Table 13.2.11.4-1: ANSI/VITA 65.1 Slot Profiles for SLT3-PAY-1F1U1S1S1U1U4F1J-14.8-7-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT3-SWH-4F1U7U1J-14.8.7-n , where n is a "Dash Num" from this table.					
Dash Num	STD Date	Connector Modules			MT loading and Optical Pipes
		P1B/J1B	P2A/J2A	P2B/J2B	
		VITA 46	VITA 46	Aperture J	
0	2017-05	VITA 46	VITA 46	Empty	
1*	2017-05	VITA 46	VITA 46	66.4 in_67.3D-6.4.5.7.1	
4	Ready	VITA 46	VITA 46	1 Style D insert - 6.4.5.7.6	MTA-MM12-1F - 6.5.2.2, MTB-MM24-3F - 6.5.3.5, MTC-MM24-3F - 6.5.3.5
5	Ready	VITA 46	VITA 46	1 Style D insert - 6.4.5.7.6	MT-MM24-3F - 6.5.3.5

* These Slot Profile dash options are legacy.

13.2.11.5 3U Radial Clock PICP

The Radial Clock VITA Slot Profile of Figure 13.2.11.5-1 is intended for driving radial clocks over the backplane. This Profile can also drive on-board bussed REF_CLK and AUX_CLK signals. In addition to the external inputs for REF_CLK and AUX_CLK, coax inputs are available for higher-quality clock signals. Lastly, this Profile is available as a Position Time Navigation (PNT) PIC if necessary. There are Slot Profile dash options, which specify Connector modules for use in the Slot Profile’s aperture. AMPS Strings can be used to assign coax connections for GPS antenna inputs as well as coax versions of REF_CLK and AUX_CLK inputs and outputs; see Section 13.3.8.

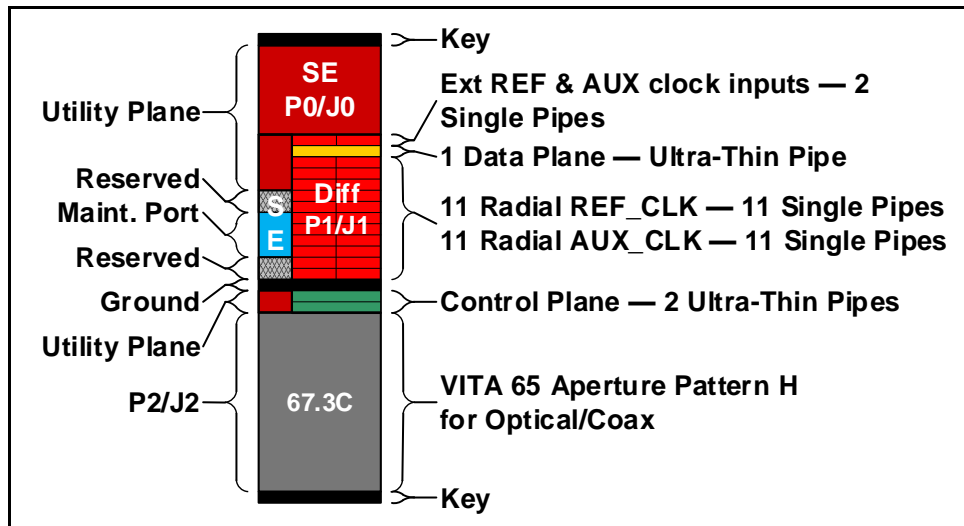


Figure 13.2.11.5-1: ANSI/VITA 65.0 Radial Clock Slot Profile SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n

Rule 13.2.11.5-1: While the SYS_CON* input is grounded, the Radial Clock PIC shall be capable of driving the bussed REF_CLK+/- . Conformance Methodology (D)

Observation 13.2.11.5-1: ANSI/VITA 65.0 §6.2.2 requires the lower-numbered ports to be the ones that are used if there are unused ports. The lower-numbered ports are the ones closest to P0/J0; hence if backplanes follow this requirement, the option of using SLT3x-TIM-4S16S1U2U1H-14.9.1-n for eight or fewer REF_CLK/AUX_CLK pairs will be accommodated.

Observation 13.2.11.5-2: See Section 13.2.3 for higher VBAT current for this ANSI/VITA Slot Profile; i.e., the 3U Radial Clock Profile.

Table 13.2.11.5-1: ANSI/VITA 65.1 Slot Profiles for SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SSLT3x-TIM-2S1U22S1U2U1H-14.9.2-n, where n is a "Dash Num" from this table.								
Dash Num	STD Date	Connector Modules			MT Loading and Optical Pipes			Comments
		P1B/J1B	P2A/J2A	P2B/J2B	P1B/J1B	P2A/J2A	P2B/J2B	
		VITA 46	Aperture H		VITA 46	Aperture H		
0	2019-11	VITA 46	Empty					
1*	2019-11	VITA 46	10 SMPM 67.3 contacts – 6.4.5.6.3					
2	Ready	VITA 46	14 SMPM 67.3 contacts – 6.4.5.6.4					
3	Ready	VITA 46	19 SMPS 67.3 contacts – 6.4.5.6.6					

* These Slot Profile dash options are legacy.

Rule 13.2.11.5-2: The Radial Clock PIC shall implement the rules from ANSI/VITA 65.0 delineated in §14.9.2. Conformance Methodology (T)

Rule 13.2.11.5-3: SOSA PICs containing resources to drive the Utility Plane bussed REF_CLK+/- signals shall provide a mechanism to permit application software or system management to reassign the identity of the SYS_CON module, regardless of the logic level of the backplane SYS_CON* contact, in order to control these signal drivers once the backplane power rails are all at minimum operating voltages as defined in ANSI/VITA 46.0 §4.8.12.4. Conformance Methodology (A, D)

Table 13.2.11.5-2: Selected Rules from ANSI/VITA 65.0

ANSI/VITA 65.0 Rule	SOSA Rule	Topic	ANSI/VITA 65.0 Conformance Method	SOSA Conformance Method
3.5.4.1-1	13.2.11.5-4	REF_CLK Duty Cycle	T,A	T
3.5.4.1-2	13.2.11.5-5	REF_CLK Center Frequency Accuracy	T,A	T
3.5.4.2-1	13.2.11.5-6	1 PPS Duty Cycle	T,A	T
3.5.4.2-2	13.2.11.5-7	1 PPS Accuracy	T,A	T
3.5.4.3-2	13.2.11.5-8	Differential Voltage Swing	T,A	T
3.5.4.3-3	13.2.11.5-9	Common Mode Voltage Range	T,A	T
3.5.4.3-4	13.2.11.5-10	Symmetry	T,A	T

ANSI/VITA 65.0 Rule	SOSA Rule	Topic	ANSI/VITA 65.0 Conformance Method	SOSA Conformance Method
3.5.4.7-3	13.2.11.5-11	Clock Trace Length Matching	T,A	A
3.5.4.7-4	13.2.11.5-12	AUX_CLK and REF_CLK Matching	Missing	A

13.2.11.6 3U External I/O PICP

The VITA Slot Profile of Figure 13.2.11.6-1 is intended to be used for system-specific interfaces in the case where the XMC mapping of the profiles of Section 13.2.11.1 does not provide enough signal pins. It is intended that PICs implemented with this Slot Profile be used following one or both of the following models:

- Subserving to up to two other PICs using the Expansion Plane to receive commands and send back status/results
- Able to receive commands from many PICs via the Control Plane

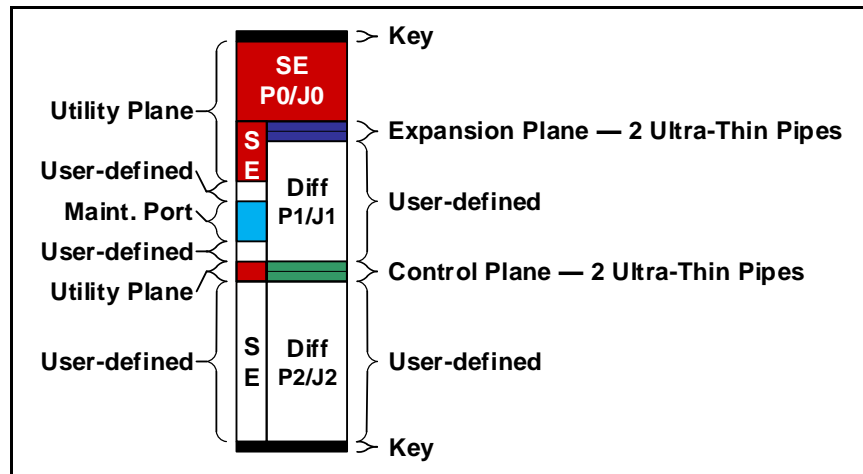


Figure 13.2.11.6-1: ANSI/VITA 65.0 3U External I/O Slot Profile SLT3-PAY-2U2U-14.2.17

Rule 13.2.11.6-1: The backplane shall not route user-defined signals between slots intended for SOSA PICs. Conformance Methodology (A)

Observation 13.2.11.6-1: Instead of routing platform-specific I/O to non-standard payloads, integrators can utilize the SOSA 3U External I/O PIC as the platform I/O “data center” where a single PIC (or multiple if required) can interface with the platform over platform-specific connections and the rest of the payload PICs over standard Expansion or Control Plane interfaces.

Recommendation 13.2.11.6-1: The SOSA 3U I/O-Intensive SBC PIC profile should be used instead of the SOSA 3U External I/O PICP if platform-specific I/O can be accommodated by a single XMC. Conformance Methodology (A)

13.2.11.7 3U Payload PICP

The P1/J1 portion of the VITA Slot Profile (Figure 13.2.11.7-1) is like that of Section 13.2.11.2. The additional UTP makes connector P1A/J1A on this VITA Slot Profile the same as the Payload VITA Slot Profiles of Section 13.2.11.1.

In addition to being used as an RF or optical switch, this Slot Profile is available to implement RF transceivers and other PICs that require more of coax and/or optical connections than is available on other SOSA PICPs. These are a new class of Profile with limited deployment and operation as the type of connection and its intended use is still new architecturally.

Observation 13.2.11.7-1: The meanings of optical interface codes used in Table 13.2.11.7-1 are defined by ANSI/VITA 65.0 and are referred to by ANSI/VITA 65.0 as Optical Profiles. The Optical Profiles shown in the last column of Table 13.2.11.7-1 have the meaning: MT = Fiber Interface, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

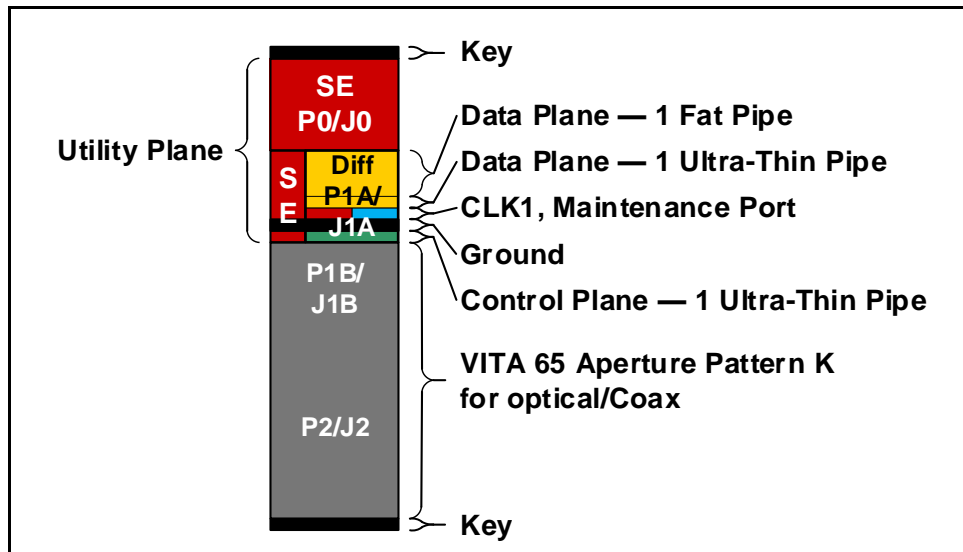


Figure 13.2.11.7-1: ANSI/VITA 65.0 3U Payload Slot Profile SLT3-PAY-1F1U1S1S1U1U1K-14.6.14-n

Table 13.2.11.7-1: ANSI/VITA 65.1 Slot Profile for SLT3-PAY-1F1U1S1S1U1U1K-14.6.14-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SSLT3-PAY-1F1U1S1S1U1U1K-14.6.14-n , where n is a "Dash Num" from this table.							
Dash Num	STD Date	Connector Modules			MT loading and Optical Pipes		
		P1B/J1B	P2A/J2A	P2B/J2B	P1B/J1B	P2A/J2A	P2B/J2B
		Aperture K			Aperture K		
0	2019-11	Empty					
6	Ready	31 SMPS 67.3 contacts - 6.4.5.8.4					
11	Ready	1_Style_D_insert_and_14_SMPM_contacts-6.4.5.8.7			MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5		
12	Ready	1_Style_D_insert_and_19_SMPS_contacts-6.4.5.8.8			MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5		
13	Ready	3_Style D_inserts-6.4.5.8.9			MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5		

13.2.12 6U SOSA PICPS – General

Rule 13.2.12-1: When a PIC is an ANSI/VITA 65.0 6U PIC, it shall be designed to one of the following ANSI/VITA 65.0 Slot Profiles:

- SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n, where allowable dash options for –n are specified in Table 13.2.12.1-2
- SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n, where allowable dash options for –n are specified in Table 13.2.12.1-1
- SLT6-SWH-14F16U1U15U1J-10.8.1-n, where allowable dash options for –n are specified in Table 13.2.12.2-1
- SLT6-PAY-4U2U-10.2.8
- SLT6-PAY-4F2Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n, where allowable dash options for –n are specified in Table 13.2.12.4-1

13.2.12.1 6U Payload PICPs

Given that VITA 6U Slot Profiles have a lot more connector area available than 3U, the VITA Slot Profiles of Figure 13.2.12.1-1 and Figure 13.2.12.1-2 combine features of the I/O-intensive VITA 3U Slot Profile of Section 13.2.11.1 and the Payload Slot Profiles of Section 13.2.11.2. Both VITA Slot Profiles have standard I/O like that of Section 13.2.11.1 and apertures for optical/coax connections like the VITA Slot Profiles of Section 13.2.11.2. The difference between the two is that the VITA Slot Profiles of Figure 13.2.12.1-2 have an XMC mapping, while the VITA Slot Profiles of Figure 13.2.12.1-1 have an additional Expansion Plane, on the P5/J5 connector, instead of the XMC mapping.

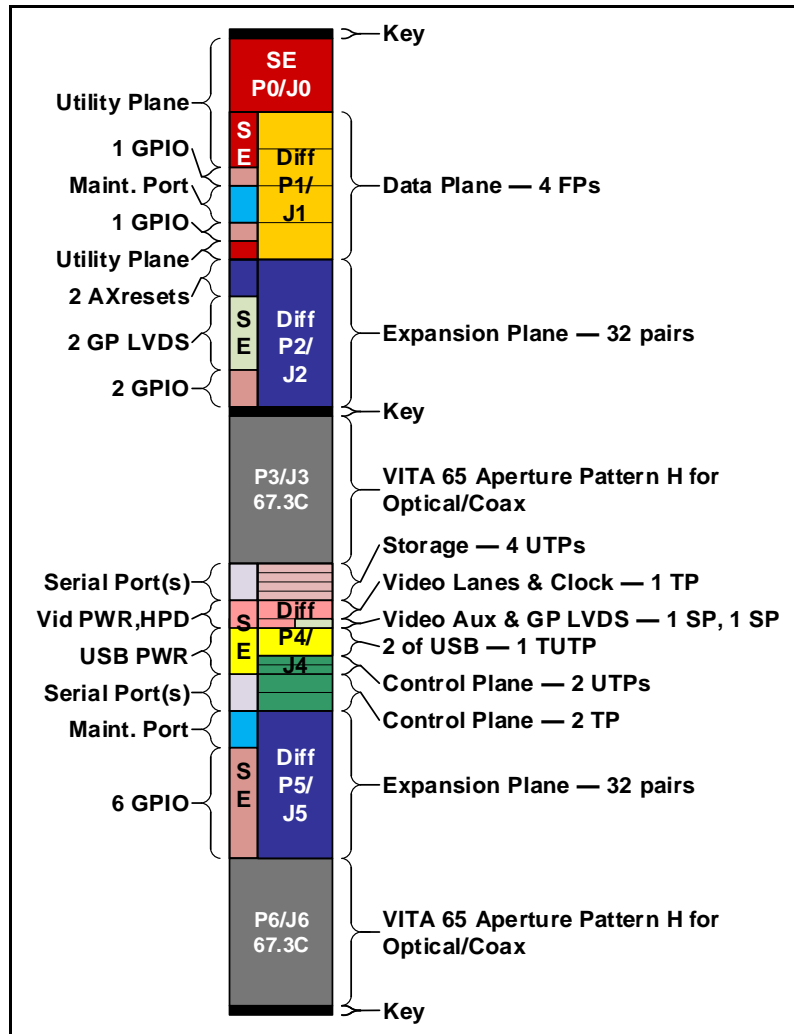


Figure 13.2.12.1-1: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n

The XMC site of PICs implemented using the Slot Profiles of Figure 13.2.12.1-2 are intended to be used for system-specific interfaces. For systems needing interfaces not available as part of SOSA Profiles, an XMC can be used. These VITA Slot Profiles make a subset of the XMC pins available to the backplane, the ANSI/VITA 46.9 P5w1-X24s+X8d+X12d mapping. The use of an XMC enables logic that is system-specific to be on the XMC, so that it can be upgraded less often than the SBC carrier on which it is sitting. This methodology also localizes the system-specific logic to the XMC, possibly making the XMC a custom (or customized) board, while the carrier can be a COTS SBC. If this does not provide enough I/O pins, to meet the needs for system-specific signals, a less desirable option is to use the PIC of Section 13.2.12.3.

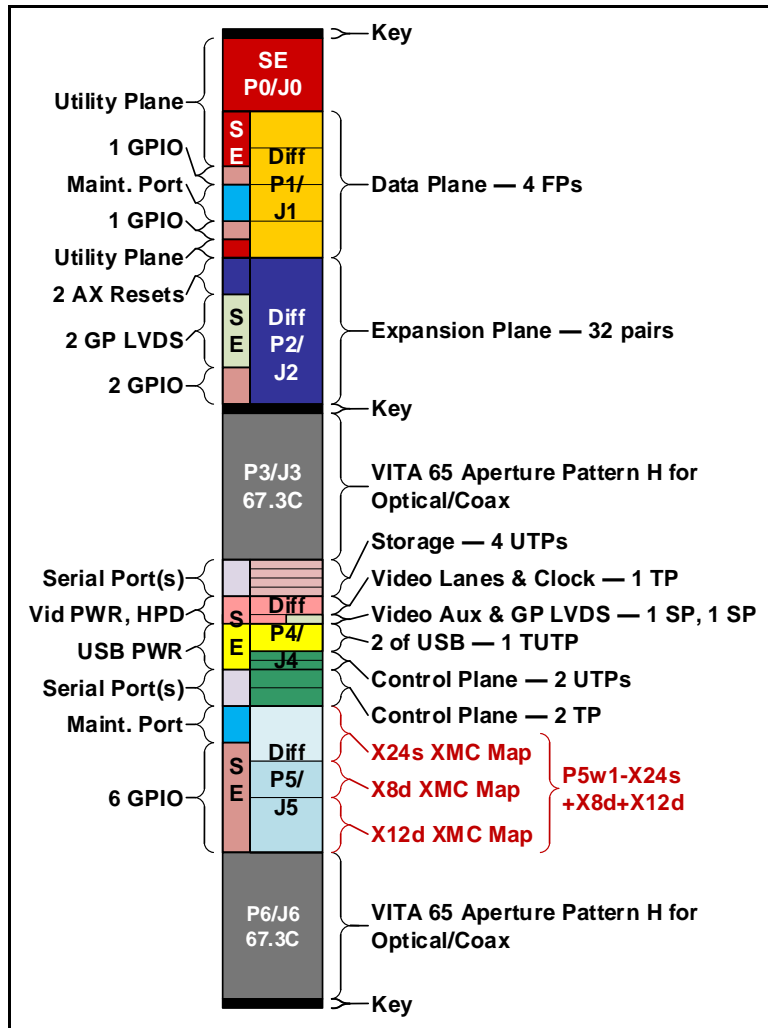


Figure 13.2.12.1-2: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n

Rule 13.2.12.1-1: Unless signals from XMC are from an XMC Overlay Profile, the backplane shall not route XMC signals between slots intended for SOSA PICs. Conformance Methodology (A, T)

Rule 13.2.12.1-2: The backplane shall not route Control Plane Thin Pipes between slots intended for SOSA PICs. Conformance Methodology (T)

Observation 13.2.12.1-1: Payload PICs can include, but are not limited to, SBCs that are I/O-intensive, SBCs that are computationally-intensive, FPGAs, and RF transceivers.

Recommendation 13.2.12.1-1: Payload PICs should conform to ANSI/VITA 65.1 Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n if they don't require an XMC. Conformance Methodology (I)

Observation 13.2.12.1-2: SOSA systems will likely only contain one or two PICs that support ANSI/VITA 65.1 Slot Profile SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n. These slots can use an XMC to customize I/O for a system or platform. The remaining PICs will use

ANSI/VITA 65.1 Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n to support processing for the various sensor modalities.

Observation 13.2.12.1-3: The meanings of optical interface codes used in Table 13.2.12.1-1 and Table 13.2.12.1-2 are defined by ANSI/VITA 65.0 and are referred to by ANSI/VITA 65.0 as Optical Profiles. The Optical Profiles shown in the last columns in Table 13.2.12.1-1 and Table 13.2.12.1-2 have the meaning: MT = Fiber Interface, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

Table 13.2.12.1-1: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT6-PAY-4F2Q1H4U1T1S1S1TU2U2T1H-10.6.4-n , where n is a "Dash Num" from this table.							
Dash Num	STD Date	Connector Modules				MT loading and Optical Pipes	
		P1/J1, P2/J2	P3/J3	P4/J4, P5/J5	P6/J6	P3/J3	P6/J6
		VITA 46	Aperture H	VITA 46	Aperture H	Aperture H	Aperture H
0	2019-11	VITA 46	Empty	VITA 46	Empty		
1*	2019-11	VITA 46	9_SMPM_contacts-6.4.5.6.2	VITA 46	9_SMPM_contacts-6.4.5.6.2		
2	2019-11	VITA 46	14_SMPM_contacts-6.4.5.6.4	VITA 46	14_SMPM_contacts-6.4.5.6.4		
3	Ready	VITA 46	19 SMPS contacts-6.4.5.6.6	VITA 46	19 SMPS contacts-6.4.5.6.6		
8	Ready	VITA 46	1 Style C insert and 14 NanoRF contacts –6.4.5.6.8	VITA 46	1 Style C insert and 14 NanoRF contacts –6.4.5.6.8	MT-MM12-1F-6.5.2.2	MT-MM12-1F-6.5.2.2
12	Ready	VITA 46	2_Style_D_inserts-6.4.5.6.11	VITA 46	2_Style_D_inserts-6.4.5.6.11	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5
* These Slot Profile dash options are legacy.							

Table 13.2.12.1-2: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT6-PAY-4F1Q1H4U1T1S1S1TU2U2T1H-10.6.3-n , where n is a "Dash Num" from this table.							
Dash Num	STD Date	Connector Modules				MT loading and Optical Pipes	
		P1/J1, P2/J2	P3/J3	P4/J4, P5/J5	P6/J6	P3/J3	P6/J6
		VITA 46	Aperture H	VITA 46	Aperture H	Aperture H	Aperture H
0	2019-11	VITA 46	Empty	VITA 46	Empty		
1*	2019-11	VITA 46	9_SMPM_contacts-6.4.5.6.2	VITA 46	9_SMPM_contacts-6.4.5.6.2		
2	2019-11	VITA 46	14_SMPM_contacts-6.4.5.6.4	VITA 46	14_SMPM_contacts-6.4.5.6.4		
3	Ready	VITA 46	19 SMPS contacts-6.4.5.6.7	VITA 46	19 SMPS contacts-6.4.5.6.7		
4	Ready	VITA 46	2 Style C inserts and 10 NanoRF contacts-6.4.5.6.8	VITA 46	2 Style C inserts and 10 NanoRF contacts-6.4.5.6.8	MT-MM12-1F-6.5.2.2	MT-MM12-1F-6.5.2.2
8	Ready	VITA 46	1 Style C insert and 14 NanoRF contacts –6.4.5.6.9	VITA 46	1 Style C insert and 14 NanoRF contacts –6.4.5.6.9	MT-MM12-1F-6.5.2.2	MT-MM12-1F-6.5.2.2
12	Ready	VITA 46	2_Style_D_inserts-6.4.5.6.11	VITA 46	2_Style_D_inserts-6.4.5.6.11	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5

13.2.12.2 6U Data/Control Plane Switch PICP

The VITA Slot Profiles of Figure 13.2.12.2-1 are for PICs which switch both the Data and Control Planes. The Data Plane is composed of both FPs and UTPs. The Data Plane can be repartitioned to give different combinations of FPs and UTPs. See ANSI/VITA 65.0 for details. There are also two Data Plane Thin Pipes and one Control Plane UTP intended for going outside the chassis. The Data Plane Thin Pipes are a BASE-T Ethernet Protocol. See Table 13.3.5-1 for possible protocols. The Control Plane UTP intended for going outside the chassis is the one located on the Single-Ended (SE) pins of P6A/J6A and is 100BASE-T.

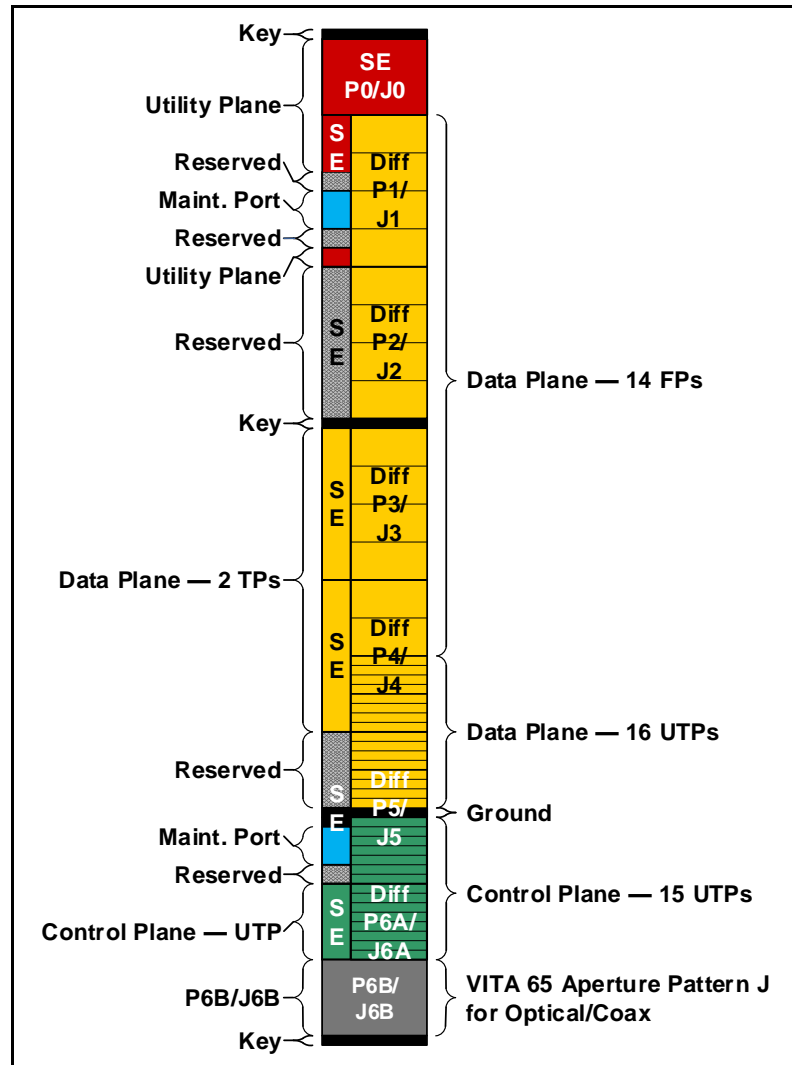


Figure 13.2.12.2-1: ANSI/VITA 65.0 6U Data/Control Switch Slot Profile SLT6-SWH-14F16U1U15U1J-10.8.1-n

Observation 13.2.12.2-1: The meanings of optical interface codes used in Table 13.2.12.2-1 are defined by ANSI/VITA 65.0 and are referred to by ANSI/VITA 65.0 as Optical Profiles. The MT loading and Optical Pipes string shown in the last column of Table 13.2.12.2-1 has this meaning: MT = Fiber Interface, the letter (A or B, if it is present) is the Optical Fiber Interface number, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

Table 13.2.12.2-1: ANSI/VITA 65.1 Slot Profiles for SLT6-SWH-14F16U1U15U1J-10.8.1-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT6-SWH-14F16U1U15U1J-10.8.1-n , where n is a "Dash Num" from this table.				
Dash Num	STD Date	Connector Modules		
		P1/J1 - P1A/J6A	P6B/J6B	P6B/J6B
		VITA 46	Aperture J	Aperture J
0	2019-11	VITA 46	Empty	
3	2021-10	VITA 46	1 Style D insert – 6.4.5.7.6	MTA-MM12-1F-6.5.2.2, MTB-MM24-3F-6.5.3.5, MTC-MM24-3F-6.5.3.5

13.2.12.3 *6U External I/O PICP*

The VITA Slot Profile of Figure 13.2.12.3-1 is intended to be used for system-specific interfaces in the case where the XMC mapping of the profiles of Figure 13.2.12.3-1 does not provide enough signal pins. It is intended that PICs implemented with this VITA Slot Profile be used following one or both of the following models:

- Subservient to up to four other PICs using the Expansion Plane to receive commands and send back status/results
- Able to receive commands from many PICs via the Control Plane

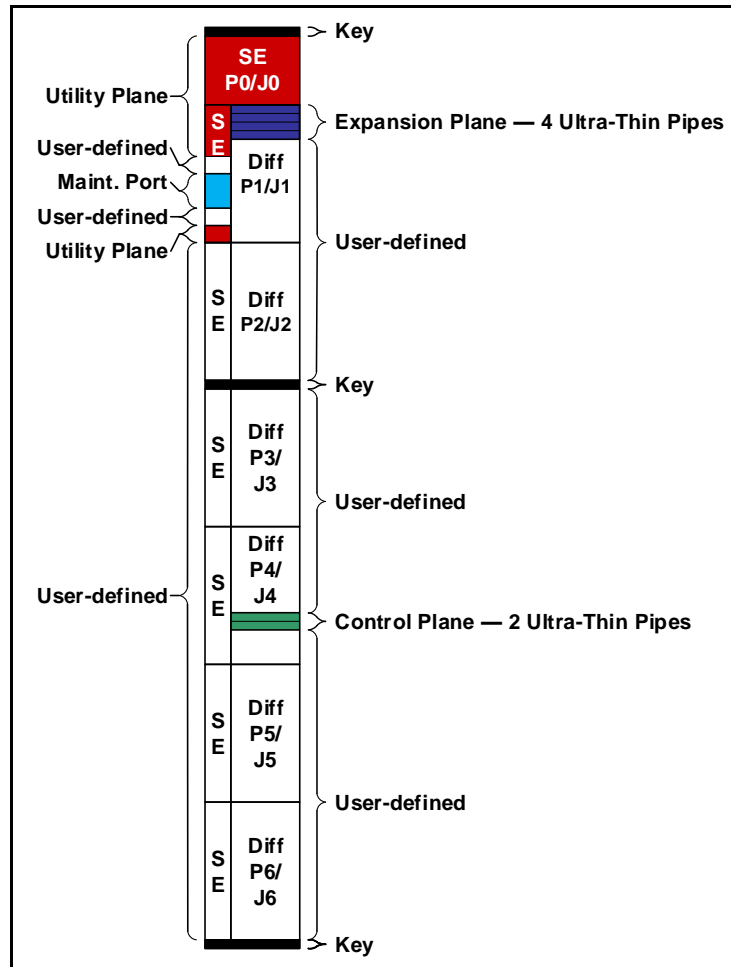


Figure 13.2.12.3-1: ANSI/VITA 65.0 6U External I/O Slot Profile SLT6-PAY-4U2U-10.2.8

Rule 13.2.12.3-1: The backplane shall not route user-defined signals between slots intended for SOSA PICs. Conformance Methodology (T)

Observation 13.2.12.3-1: Instead of routing platform-specific I/O to non-standard payloads, integrators can utilize the SOSA 6U External I/O PIC as the platform I/O “data center” where a single PIC (or multiple if required) can interface with the platform over platform-specific connections and the rest of the payload modules over standard Expansion or Data Plane interfaces.

Recommendation 13.2.12.3-1: The SOSA 6U Payload PICP should be used instead of the SOSA 6U External I/O PICP if platform-specific I/O cannot be accommodated by a single XMC. Conformance Methodology (A)

13.2.12.4 6U RF/Optical Switch PICP

In addition to being used as an RF or optical switch, this ANSI/VITA 65.0 Slot Profile, shown in Figure 13.2.12.4-1, is available to implement RF transceivers and other PICs that require more of coax and/or optical connections than is available on other SOSA PICPs. These are a new class of Profile with limited deployment and operation as the type of connection and its intended use is still new architecturally.

Observation 13.2.12.4-1: The meanings of optical interface codes used in Table 13.2.12.4-1 are defined by ANSI/VITA 65.0 and are referred to by ANSI/VITA 65.0 as Optical Profiles. The MT loading and Optical Pipes string shown in the last column of Table 13.2.12.4-1 has this meaning: MT = Fiber Interface, the letter (A or B, if it is present) is the Optical Fiber Interface number, MM = Optical Fiber type, after the MM the # of Optical Fiber, the # of Pipes, and the type of Pipe; e.g., Fat Pipe (FP). For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

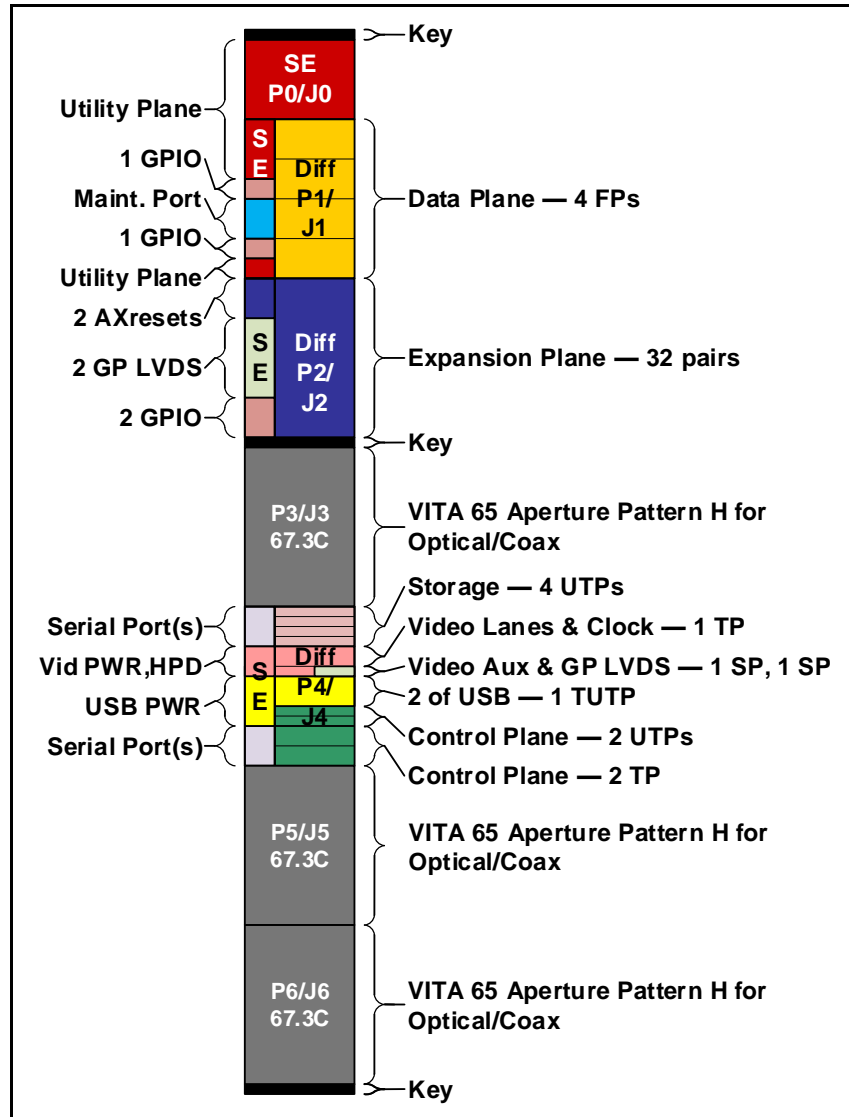


Figure 13.2.12.4-1: ANSI/VITA 65.0 6U Payload Slot Profile SLT6-PAY-4F2Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n

Table 13.2.12.4-1: ANSI/VITA 65.1 Slot Profiles for SLT6-PAY-4F2Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n

ANSI/VITA 65.0 and 65.1 Slot Profile names: SLT6-PAY-4F1Q1H4U1T1S1S1T1U2U2T2H-10.6.5-n , where n is a "Dash Num" from this table.									
Dash Num	STD Date	Connector Modules					MT loading and Optical Pipes		
		P1/J1, P2/J2	P3/J3	P4/J4	P5/J5	P6/J6	P3/J3	P5/J5	P6/J6
		VITA 46	Aperture H	VITA 46	Aperture H	Aperture H	Aperture H	Aperture H	Aperture H
0	2019-11	VITA 46	Empty	VITA 46	Empty	Empty			
9	2019-11	VITA 46	14 SMPM contacts-6.4.5.6.4	VITA 46	2_Style_D_inserts-6.4.5.6.11	14 SMPM contacts-6.4.5.6.4		MTA1-MM12-1F-6.5.2.2, MTB1-MM24-3F-6.5.3.5, MTC1-MM24-3F-6.5.3.5, MTA2-MM12-1F-6.5.2.2, MTB2-MM24-3F-6.5.3.5, MTC2-MM24-3F-6.5.3.5	
10	2019-11	VITA 46	19 SMPS contacts-6.4.5.6.7	VITA 46	2_Style_D_inserts-6.4.5.6.11	19 SMPS contacts-6.4.5.6.7		MTA1-MM12-1F-6.5.2.2, MTB1-MM24-3F-6.5.3.5, MTC1-MM24-3F-6.5.3.5, MTA2-MM12-1F-6.5.2.2, MTB2-MM24-3F-6.5.3.5, MTC2-MM24-3F-6.5.3.5	

13.2.13 Legacy

As this document evolves, an established definition (and process) is necessary to differentiate between newer SOSA hardware elements, in this case SOSA PICPs, and older ones whose current interface sets are obsolete, overcome by a need for additional or different interface types, or use in SOSA conformant products is waning.

Important: The term introduced here is a **Legacy PICP**.

Motivating the SOSA Consortium to this course of action is a desire and need to maintain a minimum viable set of SOSA PICPs for use by SOSA Consortium members. This minimizes flexibility and maximizes hardware interchangeability and portability.

The agreed upon process for flagging legacy PICPs and eventually deprecating legacy PICPs is described below. The legacy PICP label placed next to a SOSA PICP indicates an intention of the SOSA Consortium to remove the PICP form this document in a future version.

The date that these legacy PICPs shall be removed from this document will be determined by the SOSA Consortium, typically at the next release of this document. An 18-month grace period after the legacy PICP has been removed from this document shall be provided to allow submission of a sensor component for certification against the legacy PICP that has been removed.

Any sensor component built to a legacy PICP that is submitted after the 18-month grace period for certification shall not be able to proceed through the certification process.

The following sections list existing SOSA PICPs, based on ANSI/VITA 65.0 Slot Profiles, which are currently labeled legacy.

13.2.13.1 3U Legacy PIC – 3U Payload

This was a very popular ANSI/VITA 65.0 Slot Profile, shown in Figure 13.2.13.1-1, before the effort to come up with VITA Slot Profiles with no user-defined pins. Except for the second FP being Data Plane instead of Expansion Plane, PICs meeting the requirements of the I/O-intensive VITA Slot Profile will also meet the requirements of this VITA Slot Profile. The large number of user-defined pins means that this VITA Slot Profile leads to interoperability problems.

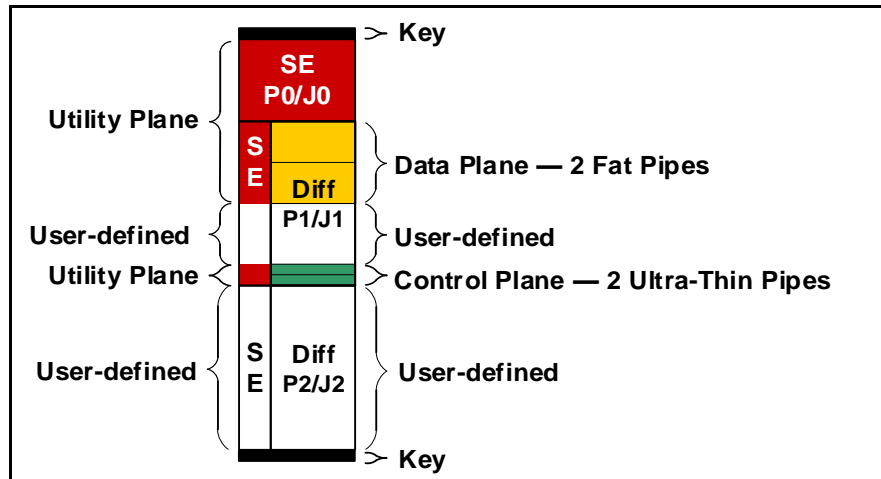


Figure 13.2.13.1-1: ANSI/VITA 65.0 Payload Slot Profile for SLT3-PAY-2F2U-14.2.3

Rule 13.2.13.1-1: SOSA 3U Legacy Payload PICs shall conform to ANSI/VITA 65.0 Slot Profile SLT3-PAY-2F2U-14.2.3. Conformance Methodology (I)

Rule 13.2.13.1-2: SOSA 3U Legacy Payload PICs shall conform to one of the following ANSI/VITA 65.1 module profiles: (Conformance Methodology (A, T))

- MOD3-PAY-2F2U-16.2.3-3
- MOD3-PAY-2F2U-16.2.3-5
- MOD3-PAY-2F2U-16.2.3-11

Recommendation 13.2.13.1-1: It is anticipated that the SLT3-PAY-2F2U-14.2.3 ANSI/VITA Slot Profile will be deprecated from the next version of this document and consequently should not be used for new systems. Conformance Methodology (I)

13.2.13.2 6U Legacy PIC – Switch

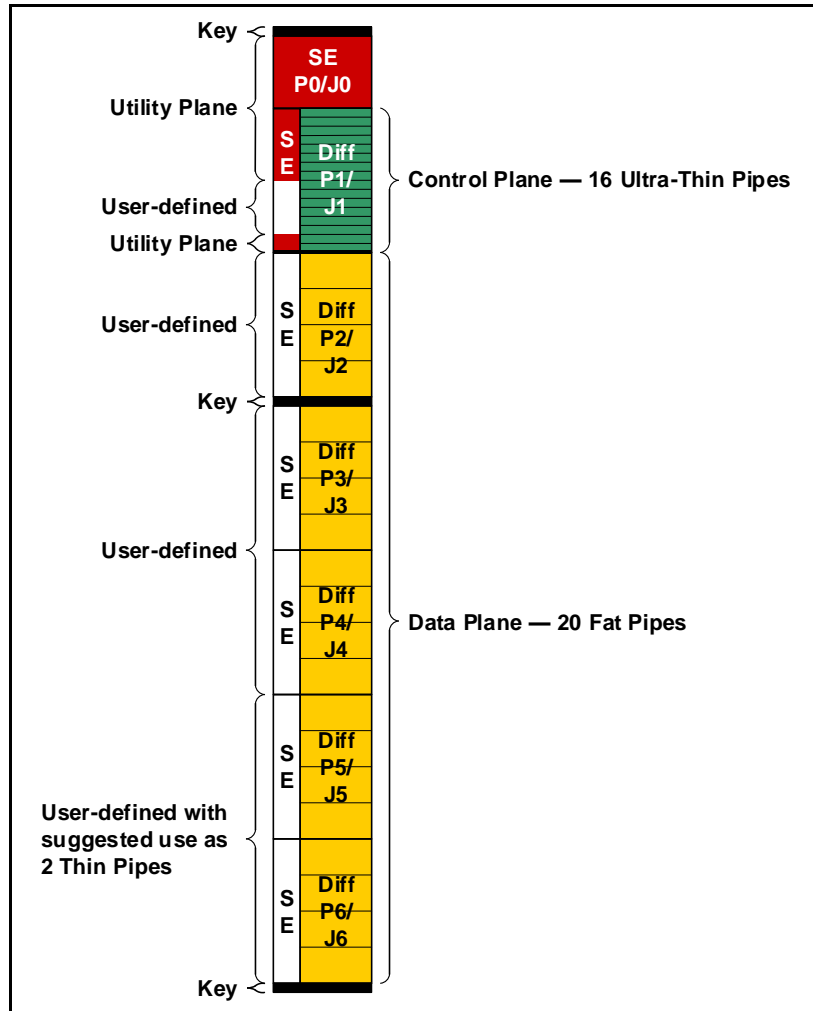


Figure 13.2.13.2-1: ANSI/VITA 65.0 Switch Slot Profile for SLT6-SWH-16U20F-10.4.2

Rule 13.2.13.2-1: SOSA 6U Legacy Switch PICs shall conform to ANSI/VITA 65.0 Slot Profile SLT6-SWH-16U20F-10.4.2, shown in Figure 13.2.13.2-1. Conformance Methodology (I)

Rule 13.2.13.2-2: SOSA 6U Legacy Switch PICs shall conform to one of the following ANSI/VITA 65.1 module profiles per: Conformance Methodology (I)

- MOD6-SWH-16F20U-12.4.2-3
- MOD6-SWH-16F20U-12.4.2-5
- MOD6-SWH-16F20U-12.4.2-11
- MOD6-SWH-16F20U-12.4.2-15

Recommendation 13.2.13.2-1: It is anticipated that the SLT6-SWH-16U20F-10.4.2 profile will be deprecated from the next version of this document and consequently should not be used for new systems. Conformance Methodology (I)

13.2.13.3 3U Legacy SMPM-10 (-1 Option) Radial Clock PICP

The ANSI/VITA 65.0 3U Radial Clock Slot Profile SLT3x-TIM-2S1U22S1U2U1H-14.9.2-1, as shown in Figure 13.2.11.5-1, is designated legacy. No other SLT3x-TIM-2S1U22S1U2U1H-14.9.2-n dash option, other than -1 for SMPM-10, is designated legacy.

13.3 Alternate Module Profile Scheme (AMPS)

13.3.1 SOSA AMPS Definitions

Alternate Module Profile Scheme (AMPS)

A method that defines the characteristics of a PICP via the construction of a protocol field string instead of an enumerated list of protocol field combinations.

AMPS String

A range of protocol fields enumerated in a specified manner meant to replace the use of module profile tables.

Alternate Naming Structure (ANS)

The PICP string created with a series of protocol fields. The ANS specifies which Slot Profile is to be used, not including the Slot Profile dash option, and assigns the protocol fields to the ports of the PICP. The ANS is also specifying the order of the protocol fields within an AMPS String and each protocol field specifies the protocol for its corresponding port.

Protocol Field

A field within an AMPS String used to specify the protocol on one or more ports. For example, in the SOSA PICP 14.6.11 profile, “Data Plane 1” would be a protocol field.

Protocol Modifier

Additional specific characters added to a given protocol field.

13.3.2 SOSA AMPS Introduction

Note: This section contains excerpts from language in ANSI/VITA 65.0.

In ANSI/VITA 65.0 there are two different naming schemes for module profiles – first the older method, which is referred to as “classic module profile” naming, and second the newer method referred to as AMPS. The classic method of naming and cataloging has been in use since ANSI/VITA 65-2010 and up to Edition 1.0 of the SOSA Technical Standard, Version 3.0 (Snapshot). It uses tables of dash options in ANSI/VITA 65.1 to specify the protocols on the various ports. This classic module profile naming construct is described in ANSI/VITA 65.0 §1.3.3.3.1. The second module profile naming scheme (AMPS) was created in response to the inclusion of new optical and RF blocks that subsequently precipitated an explosion in protocol and optical/RF combinations because of how ANSI/VITA 65.0 catalogs module profiles with the classic naming construct. The classic module profile naming construct is also a limitation on its

utility. The profile designation, with dash options, restricts the range of protocol types and rates based on choice. This limitation is essentially the reason for the explosion noted above and hence the genesis of AMPS. ANSI/VITA 65.0 added AMPS. The SOSA Technical Standard switched to using AMPS beginning with Edition 1.0.

The AMPS String fully defines an ANSI/VITA 65.0 module profile and all its features, what this document refers to as a PICP. The AMPS String provides all relevant information to the user and assists in the maximization of this document's interoperability and portability quality attributes. Protocol fields within an AMPS String specify protocols and parameters for those protocols, such as baud rate, whether they auto-negotiate, etc.

It is important to note that AMPS uses an additional construct from ANSI/VITA 65.0: the ANS. The ANS specifies which Slot Profile is to be used, not including the Slot Profile dash option, and assigns the protocol fields to the Slot Profile's ports. The ANS is also specifying the order of the protocol fields within an AMPS String. Each protocol field specifies the protocol for its corresponding port.

An example of an ANS construct is shown below in Table 13.3.2-1. This is an excerpt from ANSI/VITA 65.0.

Table 13.3.2-1 is a combination of the classic method for expressing the VITA 65 module profiles, in this case MOD3-PAY-1F1U1S1S1U1U4F1J-16.6.13-1, while the highlighted text (the last line in the table) is the ANS MODA3-16.6.13-1, which specifies how to build an AMPS String that can express the functionality of the VITA 65 module profile MOD3-PAY-1F1U1S1S1U1U4F1J-16.6.13-1, as well as many others. For details concerning the use of ANS see ANSI/VITA 65.0 §8.10.1.

In Table 13.3.2-1, going through the columns of MODA3-16.6.13-1:

- There is a Slot Profile column, specifying the Slot Profile to be a dash option of SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n
- There are two columns for specifying two protocol fields of the Data Plane, enclosed by “()”; one of these protocol fields is for the FP DP01 and the other for the UTP DPutp01
- There are two columns for specifying two protocol fields for the Expansion Plane; the first of these is for lanes EP00 to EP07 and the second is for lanes EP08 to EP15 – these two protocol fields are also enclosed by “()”
- There is a single column for specifying a protocol field for the Control Plane port CPutp01; this protocol field is also enclosed by “()”
- The last column is for any protocol implemented on the aperture for optical and/or coax

ANS ports do not need to be the same as the column's headings in the part of the VITA 65 module profile table for current VITA 65 module profile dash options – this is the reason for listing ports again in the ANS portion of the table. As an example, the Expansion Plane ports shown in Table 13.3.2-1 could change:

- From: (EP00 – EP07 EP08 – EP15)
- To: (EP00 – EP03 EP04 – EP15)

Each lane in the former, and the latter, are assigned a protocol in AMPS.

Table 13.3.2-1: ANS Example Using VITA 65 MOD3-PAY-1F1U1S1S1U1U4F1J-16.6.13-n

Module Profile names			Protocols for Copper Planes					Protocols for Optical/Coax
	Dash Num	Slot Profile	Data Plane	Data Plane	Expansion Plane	Expansion Plane	Control Plane	
MOD3-PAY-1F1U1S1S1U1U4F1J-16.6.13-			DP01	DPutp01	EP00 - EP07	EP08 - EP15	CPutp01	P2B
MOD3p-PAY-1F1U1S1S1U1U4F1J-16.6.13-	1	SLT3p-PAY-1F1U1S1S1U1U4F1J-14.6.13-0	40GBASE-KR4 -- 5.1.8	10GBASE-KR -- 5.1.7	PCIe Gen 3 -- 5.3.3.3	PCIe Gen 3 -- 5.3.3.3	10GBASE-KR -- 5.1.7	
MODA3-16.6.13-			Protocols for Copper Planes					Protocols for Optical/Coax
MODA3-16.6.13- 1		SLT3-PAY-1F1U1S1S1U1U4F1J-14.6.13-n	(DP01)	(DPutp01)	(EP00 - EP07)	(EP08 - EP15)	(CPutp01)	[P2B]
Last line								

In early 2020, the SOSA Hardware SC agreed to a transition from the current VITA 65 module profile naming construct, which uses dash numbers for each VITA 65 module profile, to AMPS (with ANS), which is described in ANSI/VITA 65.0 §1.3.3.3. The new AMPS naming convention was necessary to manage the unwieldy number of VITA 65 module profile dash options.

As a result of this transition, all SOSA PICPs will use AMPS, which uses high-level summary tables instead of the VITA 65 module profile tables with dash options. The summary profile tables of protocols that can be used in protocol fields for SOSA AMPS Strings are given in Table 13.3.2-2.

Important Note: This document does not allow all possible protocols as does VITA 65 and has down selected to the options shown in Table 13.3.2-2, and further down selected to the protocols for specific ports indicated by Table 13.3.3-2, Table 13.3.3-3, and Table 13.3.3-4. This document also expands on the VITA 65 AMPS scheme by adding some SOSA specific fields onto the end of the AMPS String such as RF pin outs, XMC overlay, and Switch Front Panel Fiber I/O.

Table 13.3.2-2: SOSA Protocol Summary

Copper High Speed Serial Protocols			
Protocol Description	lanes	Name	ANSI/VITA 65.0 Section #
N	N/A	Not connected	N/A
J	N/A	Joined with previous protocol field	N/A
A3F	4	Aurora-10Gbaud-64B/66B	5.7.3
D1	4	Display Port 1.2	5.11.1
E1	1	Ethernet-1000BASE-BX	5.1.1
E2	1	Ethernet-1000BASE-KX	5.1.2

Copper High Speed Serial Protocols			
Protocol Description	lanes	Name	ANSI/VITA 65.0 Section #
E7	1	Ethernet-10GBASE-KR	5.1.7
E5	4	Ethernet-10GBASE-KX4	5.1.5
E15	1	Ethernet-25GBASE-KR	5.1.15
E8	4	Ethernet-40GBASE-KR4	5.1.8
E18	4	Ethernet-100GBASE-KR4	5.1.18
P2F	4	PCIe-Gen 2 (x4)	5.3.3.2
P3U	1	PCIe-Gen 3 (x1)	5.3.3.3
P3F	4	PCIe-Gen 3 (x4)	5.3.3.3
P3D	8	PCIe-Gen 3 (x8)	5.3.3.3
P3Q	16	PCIe-Gen 3 (x16)	5.3.3.3
P4U	1	PCIe-Gen 4 (x1)	5.3.3.4
P4F	4	PCIe-Gen 4 (x4)	5.3.3.4
P4D	8	PCIe-Gen 4 (x8)	5.3.3.4
P4Q	16	PCIe-Gen 4 (x16)	5.3.3.4
S2	1	SATA Gen 2	5.6.2
S3	1	SATA Gen 3	5.6.3
U2	1	USB 3.0 G1	5.9.2
U3	1	USB 3.0 G2	5.9.3
Z3F	4	sFPDP-Gen3-10Gbaud-64B/67B	5.16.3

Optical High Speed Serial Protocols			
Protocol Description	lanes	Name	ANSI/VITA 65.0 Section #
A5F	4	Aurora-10Gbaud-64B/66B	5.7.5
A6F	4	Aurora-25Gbaud-64B/66B	5.7.6

Optical High Speed Serial Protocols			
Protocol Description	lanes	Name	ANSI/VITA 65.0 Section #
E11	1	Ethernet-10GBASE-SR	5.1.11
E17	1	Ethernet-25GBASE-SR	5.1.17
E12	4	Ethernet-40GBASE-SR4	5.1.12
E19	4	Ethernet-100GBASE-SR4	5.1.19
Z5F	4	sFPDP-Gen3-10Gbaud-64B/67B	5.16.5
Z6F	4	sFPDP-Gen3-25Gbaud-64B/67B	5.16.6

Differential Protocols			
Protocol Description	pairs	Name	ANSI/VITA 65.0 Section #
M4	2	TIA 422	5.13.4
M5	2	TIA 485	5.13.5
U1	1	USB 2.0	5.9.1
G2	1	LVDS-<1.25Gbps	5.15.2
G5	1	Radial Clock	5.15.5
E3	4	1000BASE-T	5.1.3
E14	2	100BASE-TX	5.1.14

Single Ended Protocols			
Protocol Description	signals	Name	ANSI/VITA 65.0 Section #
G1	1	GPIO	5.15.1
M3	2	TIA 232	5.13.3

RF Pin Outs (SOSA Only)		ANSI/VITA 65.0 Section #
N	Not connected	N/A
RF0	User-defined pin out	N/A

XMC Type A Overlay (SOSA Only)		ANSI/VITA 65.0 Section #
N	Not connected	N/A
XA0	XMC-defined: X12d+X8d+X16s	N/A
XA1	GPIO/GPLVDS: X12d+X8d+X16s	5.15.1/5.15.2
XA2	Security	N/A

XMC Type B Overlay (SOSA Only)		ANSI/VITA 65.0 Section #
N	Not connected	N/A
XB0	User-defined: X12d+X8d+X24s	N/A
XB1	GPIO/GPLVDS: X12d+X8d+X24s	5.15.1/5.15.2
XB2	Security	N/A
XB3	AUXCLK/RECLK Dist.	3.5.4.3

Note: The Serial Front Panel Data Port (sFPDP) (ANSI/VITA 17.3) protocol is expected to be added to a future version of ANSI/VITA 65.0. The proposal to add §5.16 to ANSI/VITA 65.0 has been accepted by the ANSI/VITA 65 Working Group. §5.16 is in the latest draft of ANSI/VITA 65.0 and is expected to be present in then next ANSI/VITA version of ANSI/VITA 65.0 (post-ANSI/VITA 65.0-2021).

There can be multiple protocols in the same protocol field, in which case they are separated by one of the following:

- “/” if the port(s) are required to be configurable among the protocols – the “/”, which is separating the protocols, can double as the last character of a protocol modifier (see ANSI/VITA 65.0 §8.10.2.1.3)
- “:” if the ports are required to auto-negotiate among the protocols

13.3.3 Alternate Module Profile Scheme (AMPS) String Construct

The focus of this section is the AMPS name construct and the ANS construct. Details concerning AMPS are in ANSI/VITA 65.0 §1.3.3.3.2 and §8.10, including a detailed description of the protocol field used within the AMPS String. An ANS description is included in ANSI/VITA 65.0 §8.10.

Figure 13.3.3-1 gives the construction of the AMPS naming string. Table 13.3.3-2, Table 13.3.3-3, and Table 13.3.3-4 define ANS protocol fields.

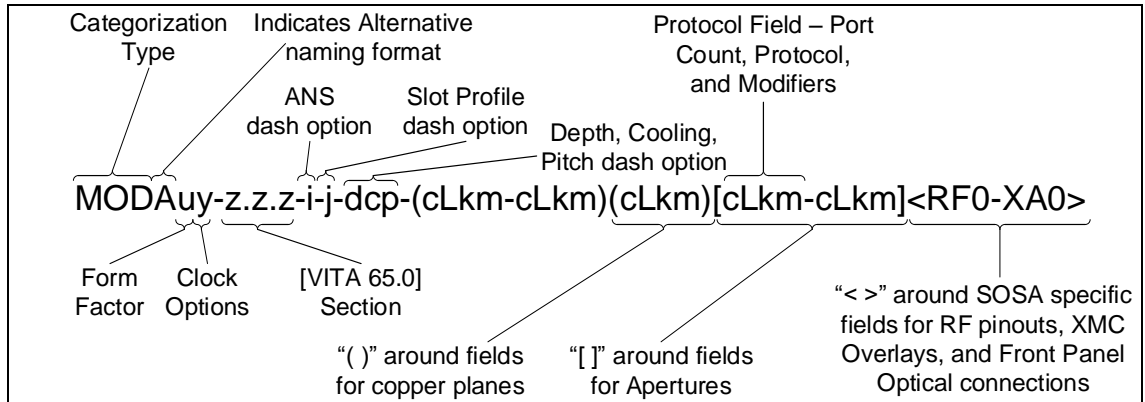


Figure 13.3.3-1: Alternative Module Profile Scheme (AMPS) String Construct

Table 13.3.3-1: AMPS Parameters

MODA	Module Profile Using AMPS	Notes
u	Form Factor {3 6}	Where: 3 = 3U VPX 6 = 6U VPX
y	Clock Options {p s x "} See ANSI/VITA 65.0 §3.5.5.1	Where: p = radial with parallel termination s = radial with series termination x = radial but termination type not specified " " = omitted indicates bussed or able to receive radial clocks with series termination
z.z.z	OpenVPX (VITA 65) Module Profile Section Number	
i	Dash option of ANS	Always "1" in this document
j	VITA 65 Slot Profile dash option	j specifies the dash option of the Slot Profile. When the Slot Profile has no dash options, this field is omitted. Note: Slot Profiles with no apertures do not have dash options.

MODA	Module Profile Using AMPS	Notes
cLkm	Protocol Field	
c	Count of ports, for ANS field in question	<p>When a single port of the protocol field of the ANS is fully utilized by a single port of the protocol, this field is omitted. This count is used two different ways:</p> <ul style="list-style-type: none"> • When the ANS field defines multiple ports This is the count of ports of the original pipe size, without any repartitioning. If the ANS field is for 4 FPs, then a value of 3 for c says there are 3 FPs used whether the pipe size stays as an FP or not, it is 3 FPs, each of which can be repartitioned into something smaller, using a port modifier. If only a single port of the four is used, then a value of 1 for the port count is still used as opposed to omitting the port count. • When the ANS field defines a single port Assuming the Slot Profile permits the port to be repartitioned, the “c” along with the pipe size expressed by Lkm can be used to express a repartitioning. For example, if there are 16 lanes of Expansion Plane, and the port width as defined by either the protocol or a protocol and port modifier is repartitioning it into FPs, “c” becomes the number of FPs. 3P3F would indicate the 16-lane port is being split into 3 of PCIe G3 with 4 lanes for a total of 12 lanes used and 4 lanes unused. There is more on repartitioning in ANSI/VITA 65.0 §8.10.2.1.2.
Lkm	Protocol description	See Table 13.3.2-2.
L	Protocol type	Example: Ethernet <i>versus</i> PCIe
k	Represents the protocol specifics	Example: speed
m	Protocol modifier	Primarily used for pipe diameter, see ANSI/VITA 65.0 §8.10.2.1. Example: FP (4 lanes) <i>versus</i> Double FP (8 lanes).
MODA	Module Profile using AMPS	
dcp	Depth, cooling, and pitch description	See Table 13.3.3-5 and Table 13.3.3-6.

Table 13.3.3-2: Protocol Field Examples Where ANS Specifies One Fat Pipe

Protocol Field	What the Field Indicates
E8	40GBASE-KR4; required to auto-negotiate to 10GBASE-KX4, 10GBASE-KR, and 1000BASE-KX.
E18	100GBASE-KR4; required to auto-negotiate to 40GBASE-KR4, 10GBASE-KX4, 25GBASE-KR, 25GBASE-KR-S, 10GBASE-KR, and 1000BASE-KX.
E18/	100GBASE-KR4; not required to auto-negotiate speed and other attributes, such as number of lanes.
E18/E8	Configurable between 100GBASE-KR4 and 40GBASE-KR4; not required to auto-negotiate speed, etc.
E18:E8	100GBASE-KR4; required to auto-negotiate to 40GBASE-KR4; but not 10GBASE-KX4, 25GBASE-KR, 25GBASE-KR-S, 10GBASE-KR, and 1000BASE-KX.
E18~	The port is meeting the electrical requirements of 100GBASE-KR4 but is dormant.
P4D	PCIe G4 with 8 lanes.
A3F	Aurora at up to 10.3 Gbaud with 4 lanes bonded together.
E18/E8/P4F/A4F	Configurable among 100GBASE-KR4, 40GBASE-KR4, PCIe G4 with 4 lanes, and Aurora with 4 lanes at up to 25.8 Gbaud. Not required to auto-negotiate among any of these.

Table 13.3.3-3: Protocol Field Examples Where ANS Specifies Four Fat Pipes

Protocol Field	What the Field Indicates
4P3U	4 FPs of PCIe G3 are implemented as 16 UTPs, 4 UTPs per FP.
4P3U1	4 FPs of PCIe G3 are implemented as 4 UTPs, 1 UTP per FP.
3P3U1	3 FPs of PCIe G3 are implemented as 3 UTPs, 1 UTP per FP.
3P3U2	3 FPs of PCIe G3 are implemented as 6 UTPs, 2 UTP per FP.
3E18/E8	Only 3 of the 4 FPs are implemented; they are configurable between 3 FPs of 100GBASE-KR4 and 3 FPs of 40GBASE-KR4, and not required to auto-negotiate among these speeds, or other speeds.

Table 13.3.3-4: Protocol Field Examples Where ANS Specifies 8 Lanes

Protocol Field	What the Field Indicates
2P3F	8 lanes are repartitioned into 2 FPs of PCIe G3 (2 of x4 PCIe).

Protocol Field	What the Field Indicates
4P3U	8 lanes are repartitioned into 4 UTPs of PCIe G3 with 4 unused lanes. If we assume the ANS MODA6-12.6.3-1, the Slot Profile specifies ANSI/VITA 65.0, Table 6.2.4.2-3 for how to divide the Expansion Plane into UTPs. For the 8 lanes of EP1, looking at the last column of ANSI/VITA 65.0, Table 6.2.4.2-3, for lanes EP00 – EP07 we have the odd UTPs, taking the lowest 4 of these we get UTP1, UTP3, UTP5, and UTP7 – lanes EP00, EP04, EP02, and EP06. For the 8 lanes of EP2, which are lanes EP08 – EP15, it is the 4 lower, even UTPs, which are used; they fall on lanes: EP08, EP12, EP10, and EP14.
2E18	Two FPs of 100GBASE-KR4 using all 8 of the lanes.
1E18	One FP of 100GBASE-KR4 using 4 lanes, leaving another 4 lanes unused.

Table 13.3.3-5: Examples of Depth, Cooling, and Pitch

Depth (mm)	Cooling (VITA 48.2)	Pitch (in)
F:Full(160)	1: Air	A:0.80
S:Short(100)	2: Conduction	B:0.85
	4: Liquid	C:1.00
	8: Air Flow Through	D:1.10
		E:1.20
		F:1.30
		G:1.40
		H:1.50
		J:1.60

Table 13.3.3-6: Depth, Cooling, and Pitch Combination Supported in This Document

AMPS	Depth	Cooling	Pitch
F2C	160mm	48.2 Conduction Cooled	1” pitch
F4C	160mm	48.4 Liquid Cooled	1” pitch
F8H	160mm	48.8 Air Flow Through Cooled	1.5” pitch
S2E	100mm	48.2 Conduction Cooled	1.2” pitch

13.3.4 SOSA 3U/6U Payload AMPS Format

Table 13.3.4-1 and Table 13.3.4-2 summarize all SOSA Payload PICPs. These tables give the ANS for each SOSA Payload PICP, specifying the order of the protocol fields, the ports to which they correspond, and the protocols which are legal for the ports. To construct an AMPS String for the Slot Profile in question, an item from the section of each column, corresponding to the Slot Profile, is chosen, independent of the value chosen from other columns (it is not a row of the table that is chosen). The copper backplane parts of the string are represented by “()”. The optical protocol fields are delimited by “[]” as defined in ANS. At the end of the string is the SOSA only portion which includes VITA 67 RF pin outs and XMC overlay each delimited by “<>”.

Please see the AMPS String construct diagram in Figure 13.3.3-1 and the appropriate ANS subsection within ANSI/VITA 65.1. This format is identical to ANSI/VITA 65.1, except for the SOSA only portion at the end of the string.

Note: The protocol values in Table 13.3.3-2, Table 13.3.3-3, and Table 13.3.3-4 are only examples to show the format.

Table 13.3.4-1: Summary of 3U Payload Plug-In Card Profiles (PICPs)

Payload Card Type	Physical Definition			Backplane Copper Protocol/Speed/Width Definition																		VITA 66/67		XMC										
	VITA 65 Slot Profile	VITA 65 Alternate Naming Structure	Depth, Cooling, Pitch	Data Plane		Expansion Plane			Control Plane		CPU Interface/Misc						VIT A 66	SOSA ONLY		XMC Overlay														
				FP	UTP	EP1	EP2	UTP	UTP	TP	STR	VID 01	USB 01	USB 02	SER 01	GP IO		CLK1 orGP	GP LVDS		1	VITA 67 RF Pinout												
																						1	2	A										
I/O intensive	14.2.16	-	16.2.15-1	F2C	(P2F*	X	(P2F	X	X	X	(2E1*	E3	(S2	D1	U1	U1	M3	G1	X	X	(X	<	X	X	XA0	>				
				F4C	(P3F*	X	(P3F	X	X	X	(2E2	X	(S3	N	U2	N	M4	N	X	X	X	(X	<	X	X	XA1	>			
				F8H	(E8	X	(P4F	X	X	X	(2E7	X	(N	X	N	X	M5	X	X	X	(X	<	X	X	XA2	>				
				S2E	(E18	X	(N	X	X	X	(E15	X	(X	X	X	X	N	X	X	X	(X	<	X	X	N	>				
External I/O	14.2.17	-	16.2.16-1	F2C	(X	X	(X	X	X	X	(2E1*	X	(X	X	X	X	X	X	X	X	(X	<	X	X	X	>				
				F4C	(X	X	(X	X	X	X	(2E2	X	(X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>			
				F8H	(X	X	(X	X	X	N	X	(2E7	X	(X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>		
				S2E	(X	X	(X	X	X	X	X	(N	X	(X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>		
Payload (Full-P V66/V67)	14.6.11	-	16.6.11-1	F2C	(E8	-	E1*	(P3F	-	P3F	X	(E1*	X	(X	X	X	X	N	G2	X	(P3F	<	RF0	X	>	X				
				F4C	(E18	E2	(A3F	-	A3F	X	(E2	X	(X	X	X	X	X	X	X	G5	X	(P4F	<	RFx	X	>	X			
				F8H	(N	E7	(Z3F	-	Z3F	X	(E7	X	(X	X	X	X	X	X	X	G6	X	(E12	<	N	X	>	X			
				S2E	(X	E15	(G2	-	G2	X	(E15	X	(X	X	X	X	X	X	X	N	X	(E19	<	X	X	X	>	X		
				X	(X	N	(P4F	-	P4F	X	(N	X	(X	X	X	X	X	X	X	X	X	X	(A5F	<	X	X	X	>	X	
				X	(X	X	(P3F/E8	-	P3F/E8	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(A6F	<	X	X	X	>	X	
				X	(X	X	(P3F/E18	-	P3F/E18	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(Z5F	<	X	X	X	>	X	
				X	(X	X	(P3D-J		X	(X	X	(X	X	X	X	X	X	X	X	X	X	X	(Z6F	<	X	X	X	>	X	
				X	(X	X	(P4D-J		X	(X	X	(X	X	X	X	X	X	X	X	X	X	X	(N	<	X	X	X	>	X	
				X	(X	X	(P3D-J/2E8		X	(X	X	(X	X	X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>	X	
				X	(X	X	(P3D-J/2E18		X	(X	X	(X	X	X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>	X	
				X	(X	X	(N	N	X	(X	X	(X	X	X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>	X	
Payload (Half-P V66/V67)	14.6.13	-	16.6.13-1	F2C	(E8	-	E1*	(2P3F	-	2P3F	X	(E1*	X	(X	X	X	X	X	G2	X	(P3F	<	RF0	-	RF0	>	X			
				F4C	(E18	E2	(P3D	-	P3D	X	(E2	X	(X	X	X	X	X	X	X	G5	X	(P4F	<	RFx	X	>	X			
				F8H	(N	E7	(2A3F	-	2A3F	X	(E7	X	(X	X	X	X	X	X	X	G6	X	(E12	<	N	X	>	X			
				S2E	(N	E15	(2P4F	-	2P4F	X	(E15	X	(X	X	X	X	X	X	X	N	X	(E19	<	X	X	X	>	X		
				X	(X	N	(2Z3F	-	2Z3F	X	(N	X	(X	X	X	X	X	X	X	X	X	X	(A5F	<	X	X	X	>	X	
				X	(X	X	(P4D	-	P4D	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(A6F	<	X	X	X	>	X	
				X	(X	X	(2P3F/2E8		G2	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(Z5F	<	X	X	X	>	X	
				X	(X	X	(2P3F/2E18		-	2P3F/2E8	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(Z6F	<	X	X	X	>	X
				X	(X	X	(P3D/2E8		-	2P3F/2E18	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(N	<	X	X	X	>	X
				X	(X	X	(P3D/2E18		-	P3D/2E8	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>	X
				X	(X	X	(N	-	P3D/2E18	X	(X	X	(X	X	X	X	X	X	X	X	X	X	(X	<	X	X	X	>	X	
				RF/Optical Switch	14.6.14	-	16.6.14-1	F2C	(E8	-	E1*	(X	X	X	(E1*	X	(X	X	X	X	X	X	G2	X	(P3F	<	RF0	-	RF0	>
F4C	(E18	E2	(X	X	X	(E2	X	(X	X	X	X	X	X	X	X	G5	X	(P4F	<	RFx	-	RFx	>	X		
F8H	(N	E7	(X	X	X	(E7	X	(X	X	X	X	X	X	X	X	G6	X	(E12	<	N	N	>	X			
S2E	(X	E15	(X	X	X	(E15	X	(X	X	X	X	X	X	X	X	N	X	(E19	<	X	X	X	>	X		
X	(X	N	(X	X	X	(N	X	(X	X	X	X	X	X	X	X	X	X	X	(A5F	<	X	X	X	>	X	
Radial Clock	14.9.2	-	16.9.2-1	F2C	(X	E1*	(X	X	X	(2E1*	X	(X	X	X	X	X	X	X	X	X	(E12	<	RF0	X	>	X				
				F4C	(X	E2	(X	X	X	(2E2	X	(X	X	X	X	X	X	X	X	X	X	(E19	<	RFx	X	>	X			
				F8H	(X	E7	(X	X	X	(2E7	X	(X	X	X	X	X	X	X	X	X	X	(A5F	<	N	X	>	X			
				S2E	(X	E15	(X	X	X	(2E15	X	(X	X	X	X	X	X	X	X	X	X	(A6F	<	X	X	X	>	X		
X	(X	N	(X	X	X	(N	X	(X	X	X	X	X	X	X	X	X	X	X	(N	<	X	X	X	>	X					

"X" - Not Applicable

*-Legacy

Footnotes for sFPDP

- Z3F full description: ANSI/VITA 17.3 with 64B/67B encoding (up to 10.3125 gbaud signaling over copper)
- Z5F full description: ANSI/VITA 17.3 with 64B/67B encoding (up to 10.3125 gbaud signaling over multi-mode optical fiber)
- Z6F full description: ANSI/VITA 17.3 with 64B/67B encoding (up to 25.78125 gbaud signaling over multi-mode optical fiber)
- The Z6F protocol will use SOSA PICs that are configurable to operate with signaling up to a nominal rate of 25.78125 gbaud over multi-mode optical fiber [VM = T, D, A]
- SOSA PICs using Z6F will follow the Physical Medium Dependent (PMD) requirements for 25GBASE-SR in IEEE 802.3 §112, except for the nominal baud rate [VM = T, D, A]
- SOSA PICs using Z5F are configurable to operate with signaling up to a nominal rate of 10.3125 gbaud over multi-mode optical fiber [VM = T, D, A]
- The Z5F protocol will use SOSA PICs which follow the PMD requirements for 10GBASE-SR in IEEE 802.3 §52, except for the nominal baud rate [VM = T, D, A]
- The sFPDP (ANSI/VITA 17.3) protocol is expected to be added to a future version of ANSI/VITA 65.0; the proposal is underway to add a new protocol §5.16 (sFPDP) to ANSI/VITA 65.0

13.3.5 SOSA 3U/6U Switch AMPS Format

Table 13.3.5-1 and Table 13.3.5-2 summarize all SOSA Switch PICPs. These tables give the ANS for each SOSA Payload PICP, specifying the order of the protocol fields, the ports to which they correspond, and the protocols which are legal for the ports. To construct an AMPS String for the Slot Profile in question, an item from the section of each column, corresponding to the Slot Profile, is chosen, independent of the value chosen from other columns (it is not a row of the table that is chosen). The copper backplane parts of the string are represented by “()”. The backplane optical protocol fields are delimited by “[]”, as defined in ANS. At the end of the string is the SOSA only portion which includes front panel optical protocol fields, which are appended to the AMPS String after the backplane optical protocol fields and delimited by “< >”. Please see the AMPS String construct diagram in Figure 13.3.3-1 and the appropriate ANS subsection within ANSI/VITA 65.1. This format is identical to ANSI/VITA 65.1, except for the SOSA only portion at the end of the string.

Note: The protocol values in Table 13.3.5-1 and Table 13.3.5-2 are only examples to show the format.

Table 13.3.5-1: Summary of Switch Plug-In Card Profiles (PICPs)

Payload Card Type		Physical Definition			Backplane Copper								VITA 66	Front Panel Optical										
					Data Plane			Exp. Plane	Control Plane			SOSA ONLY												
		VITA 65 Slot Profile	VITA 65 Alternate Naming Structure	Depth, Cooling, Pitch	FP	UTP	TP		EP	CP	TP	EXT	FP (MT)	Data Plane		Control Plane								
								FP (MPO)						UTP (LC)	FP (MPO)	UTP (LC)								
3U	DP Switch DP: 6 FP/Ethernet CP: 7 UTP/Ethernet	14.4.14	-	16.4.15-1	F2C	(E5)	E1*	X	(X)	(E1*)	X	X	X	X	<	E12	-	E11	-	E12	-	E11	>	
					F4C	(E8)	E2	X	(X)	(E2)	X	X	X	X	<	E19	-	E17	-	E19	-	E17	>	
					F8H	(E18)	E7	X	(X)	(E7)	X	X	X	X	<	N	-	N	-	N	-	N	>	
					S2E	(N)	E15	X	(X)	(E15)	X	X	X	X	<	X	-	X	-	X	-	X	>	
		X	(X)	N	X	(X)	(N)	X	X	X	X	<	X	-	X	-	X	-	X	>				
	EP Switch EP: 6 FP/PCIe CP: 8 UTP/Ethernet	14.4.15	-	16.4.16-1	F2C	(X)	X	X	(P2F)	(E1*)	E3	X	X	X	X	<	E12	-	E11	-	E12	-	E11	>
					F4C	(X)	X	X	(P3F)	(E2)	N	X	X	X	<	E19	-	E17	-	E19	-	E17	>	
					F8H	(X)	X	X	(P4F)	(E7)	X	X	X	X	<	P3F	-	N	-	P3F	-	N	>	
					S2E	(X)	X	X	(E8)	(E15)	X	X	X	X	<	P4F	-	X	-	P4F	-	X	>	
						X	(X)	X	(E18)	(N)	X	X	X	X	<	N	-	X	-	N	-	X	>	
		X	(X)	X	(N)	(X)	X	X	X	X	<	X	-	X	-	X	-	X	>					
	DP Switch/V66 DP: 4 FP/Ethernet CP: 7 UTP/Ethernet	14.8.7	-0-	16.8.7-1	F2C	(E5)	E1*	X	(X)	(E1*)	X	X	X	[E12]	<	E12	-	E11	-	E12	-	E11	>	
-4-			F4C		(E8)	E2	X	(X)	(E2)	X	X	X	[E19]	<	E19	-	E17	-	E19	-	E17	>		
-5-			F8H		(E18)	E7	X	(X)	(E7)	X	X	X	[N]	<	N	-	N	-	N	-	N	>		
X			S2E		(N)	E15	X	(X)	(E15)	X	X	X	[X]	<	X	-	X	-	X	-	X	>		
X					X	(X)	N	X	(X)	(N)	X	X	[X]	<	X	-	X	-	X	-	X	>		
6U DP: 18 FP/Ethernet CP: 15 UTP/Ethernet	10.8.1	-0-	12.8.1-1	F2C	(E5)	E1*	E3	(X)	(E1*)	X	-	E14	[E12]	<	E12	-	E11	-	E12	-	E11	>		
		-3-		F4C	(E8)	E2	N	(X)	(E2)	X	N	[E19]	<	E19	-	E17	-	E19	-	E17	>			
		X		F8H	(E18)	E7	X	(X)	(E7)	X	X	[N]	<	N	-	N	-	N	-	N	>			
		X			X	(N)	E15	X	(X)	(E15)	X	X	[X]	<	X	-	X	-	X	-	X	>		
		X			X	(X)	N	X	(X)	(N)	X	X	[X]	<	X	-	X	-	X	-	X	>		

Note: 14.4.15 profile specifies P1/P2A as Data Plane, but SOSA has re-defined these as Expansion Plane

"X"- Not Applicable *-Legacy

Table 13.3.5-2 gives examples of full AMPS Strings from the PICPs of Table 13.3.4-3. The right side of the table highlights in detail some examples of AMPS Strings. Refer to Table 13.3.3-1, Table 13.3.3-2, Table 13.3.3-3, and Table 13.3.3-4 for protocol field definitions and examples.

Table 13.3.5-2: Examples of Full AMPS Strings from SOSA PICPs

Payload Card Type		Physical Definition		Examples from AMPS string from ANS table
		VITA 65 Slot Profile	VITA 65 Alternate Naming Structure	
3U	DP Switch	14.4.14	- 16.4.15-1	MODA3-16.4.15-1-(E5-E1*)(E1*)<E12-E11-E12-E11>
	EP Switch	14.4.15	- 16.4.16-1	MODA3-16.4.16-1-(P2F)(E1*-E3)
	DP Switch/V66	14.8.7	-j- 16.8.7-1	MODA3-16.8.7-1-0-(E5-E1*)(E1*)[E12]<E12-E11-E12-E11>
6U	DP Switch	10.8.1	-j- 12.8.1-1	MODA6-10.8.1-0-(E5-E1*-E3)(E1*-E14)[E12]<E12-E11-E12-E11>

13.3.6 Portion of the AMPS String for VITA 66 Connectors

Slot Profile dash options specify:

- The location of Connector modules in the Slot Profile’s aperture; the Connector modules can each have one or more MTs for optical fibers
- An Optical Profile for each MT of each Connector module

Optical Profiles specify what kind of MT (e.g., MM12, MM24) is to be loaded and how the fibers are configured into pipes. For more on Optical Profiles, see ANSI/VITA 65.0 §6.5.

The protocol fields for VITA 66 Connector modules go toward the end of the AMPS String with “[]” around them, as indicated in the part of the AMPS String for apertures; see Table 13.3.6-1. In the case of VITA 66 Connector modules where the ANSI/VITA 65.1 ANS defines a single protocol field, the aperture portion of the AMPS String is constructed in one of two ways:

- A single protocol with no MTs skipped
A single protocol field which applies to all the MTs of a Connector module with no MTs skipped. The MTs are in the order of lowest to highest – MTA1, MTA2, ..., MTB1, MTB2, There must be no pipes of any of the MTs skipped; it is fine for one or more of the highest numbered MTs to be unused. There can be unused fibers skipped, if they are specified as unused by the Optical Profile, for the MT in question. The port count, within the protocol field, will indicate how many ports are used.
- Different protocols and/or MTs skipped
When there are different protocols used or portions of MTs skipped, then there is a protocol field for each MT.

The above options make it so that the same ANS can be used for different Slot Profile dash options, even if the number of MTs varies.

Table 13.3.6-1: Examples of Protocol Fields for VITA 66 Connectors

Examples assuming a Slot Profile dash option specifying a Connector module with 3 MTs – MTA1, MTB1, and MTC1 with Optical Profiles as follows:	
MTA1 – MTkk-MM12-1F-6.5.2.2 – 12 optical fibers where 8 are used for a FP and 4 are unused.	
MTB1 – MTkk-MM24-3F-6.5.3.5 – 24 optical fibers used as 3 FPs of 8 fibers each.	
MTC1 – MTkk-MM24-3F-6.5.3.5 – 24 optical fibers used as 3 FPs of 8 fibers each.	
Protocol Field	What the field indicates
[E18]	7 FP of 100GBASE-SR4 using 1 FP (8 fibers) of MTA1, 3 FP (24 fibers) of MTB1, and 3 FP of MTC1.
[4E18]	4 FP of 100GBASE-SR4 using 1 FP (8 fibers) of MTA1, 3 FP (24 fibers) of MTB1, and none of MTC1.
[N-3E18-3A6F]	MTA1 not used, MTB1 has 3 of 100GBASE-SR4, MTC1 has 3 FP of Aurora at up to 10 Gbaud.

13.3.7 SOSA AMPs Rules

Rule 13.3.7-1: Where a SOSA PIC has Low Voltage Differential Signal (LVDS) on its Expansion Plane, the SOSA PIC shall use the LVDS starting on the lowest lane of the highest numbered Expansion Plane port. Conformance Methodology (A)

Rule 13.3.7-2: A SOSA PIC's AMPS String must conform to the formats in either Table 13.3.4-1 or Table 13.3.4-2 for Payload PICPs and Table 13.3.5-1 for Switch PICPs. Conformance Methodology (A)

Rule 13.3.7-3: A PIC shall implement all the ports and all the lanes of those ports, for the associated protocols, specified by the AMPS String. Conformance Methodology (A, D)

Rule 13.3.7-4: A SOSA PIC with ports configurable for multiple protocols shall implement all the lanes of all the protocols specified by the AMPS String. Conformance Methodology (A, D)

Observation 13.3.7-1: As an example of what is required by Rule 13.3.7-4: if an FP is specified by the AMPS String to be configurable between 40GBASE-KR4 and 10GBASE-KR, using a protocol field of E8/E7 when it is configured for 10GBASE-KR, it must be repartitioned into four UTPs, all implementing 10GBASE-KR, unless the AMPS String were to specifically indicate that a subset of the lanes of the FP are to be implemented.

Permission 13.3.7-1: Expansion Plane ANS fields EP1 and EP2 may be combined for PCIe to allow for larger pipe sizes.

13.3.7.1 SOSA Non-Switch Plug-In Card Backplane Interfaces Supporting Inter-Module Interactions

This section discusses direction to SOSA PIC designers regarding backplane interface connections. Ensuring that connections used for SOSA inter-module interactions are connected to sufficiently intelligent processors is critical to the reusability and interchangeability of SOSA PICs.

While this document builds on ANSI/VITA 65.0 for much of the SOSA Technical Standard regarding PICP, the ANSI/VITA 65.0 "planes" terminology will be used only to refer to a collection of PIC pins. The ANSI/VITA 65.0 "planes" terminology implies backplane connectivity that is not relevant in many cases. As Ethernet is currently the only data link defined for inter-module interaction bindings, this section describes the mapping of these pins to two levels of Ethernet functionality:

- Support Level Ethernet 1 (SLE1): a SOSA PIC claiming SLE1 on one of its Ethernet interfaces can be expected to implement any level of network behavior required anywhere within the SOSA Technical Standard
- Support Level Ethernet 2 (SLE2): a SOSA PIC claiming SLE2 on one of its Ethernet interfaces is expected to implement a subset of network behavior that is described in this section's rule set

13.3.7.1.1 Backplane Interfaces to Ethernet Support Level Mapping

SLE1 is optimized for control and SLE2 is optimized for high bandwidth data. AMPS defines the rules for physical implementation of PIC backplane interfaces and/or whether they are implemented at all.

Table 13.3.7.2-1 describes the network behavior that can be expected to be available on the PIC backplane interfaces.

Observation 13.3.7.1.1-1: Specific behavior for AMPS protocols other than Ethernet is not defined in this document.

Rule 13.3.7.1.1-1: If a SOSA PIC implements an AMPS-defined physical backplane interface using Ethernet, at a minimum it shall support the protocol support level as called out in Table 13.3.7.2-1. Conformance Methodology (A)

13.3.7.1.2 Support Level for Ethernet Common Definition

Rule 13.3.7.1.2-1: A SOSA PIC's Ethernet interfaces shall support Address Resolution Protocol (ARP) packet generation for purposes of announcing its interface address to the network as specified in IETF RFC 5227. Conformance Methodology (D)

13.3.7.1.3 Support Level for Ethernet 1 (SLE1) Definition

Ethernet Support Level 1 (SLE1) is a generic capability "bin" targeted for use in devices that can run a full IP stack such as a general-purpose processor. Often these types of devices are the ones generating this lower bandwidth but potentially more complex data. "SLE1" will support the use of IEEE 802.3 TCP packets and include an IPv4 header.

Rule 13.3.7.1.3-1: A SOSA PIC's "SLE1" Ethernet interfaces shall support Hypertext Transfer Protocol (HTTP) GET and POST. Conformance Methodology (D)

Observation 13.3.7.1.3-1: Rule 13.3.7.1.3-1 is a test of the complexity of the underlying hardware connected to an SLE1 set of pins. It is intended to ensure that a processor running a "full Ethernet stack" is connected to that interface.

Observation 13.3.7.1.3-2: A SOSA PIC's "SLE1" Ethernet interfaces might be required to support VICTORY Data Bus (VDB) in a future version of this document.

Observation 13.3.7.1.3-3: A SOSA PIC's "SLE1" Ethernet interfaces might support "SLE2" Ethernet traffic.

Suggestion 13.3.7.1.3-1: When SLE1 is used, it is suggested that the SLE1 Control Plane UTP interface be used first.

13.3.7.1.4 Support Level for Ethernet 2 (SLE2) Definition

Ethernet Support Level 2 (SLE2) is a generic capability "bin" targeted for use in devices that could not be able to run a full IP stack such as an FPGA. Often these types of devices are the ones generating this high bandwidth data. "SLE2" would use IEEE 802.3 UDP packets and include an IPv4 header.

Rule 13.3.7.1.4-1: A SOSA PIC's "SLE2" Ethernet interfaces shall support jumbo Ethernet frames with a maximum transmission unit of 9,000 bytes. Conformance Methodology (D)

Observation 13.3.7.1.4-1: A SOSA PIC's "SLE2" Ethernet interfaces might be required to support MORA Low Latency Bus (ML2B) in a future version of this document.

Permission 13.3.7.1.4-1: A SOSA PIC's "SLE2" Ethernet interface could optionally implement more functionality than is required for "SLE2".

Observation 13.3.7.1.4-2: A SOSA PIC’s “SLE2” Ethernet interfaces can optionally support “SLE1” traffic even though not required to within the SOSA Technical Standard. It should be noted that there will be some SOSA conformant “SLE2” endpoints that will not be able to support “SLE1” traffic.

13.3.7.2 Ethernet Backplane Connectivity Methodology

Currently, Ethernet is the only approved protocol for SOSA modules and their interaction bindings. As defined in the SOSA quality attributes (Section 3.1), it is important to maximize interoperability at the system level and interchangeability (or portability) at the infrastructure (PIC) level. Providing more definition and guidance in using Ethernet accomplishes this maximization. There is an implicit assumption that not all backplanes (whether SOSA conformant or not) will support Ethernet on the Expansion Plane. To help provide clarity and guidance, the decision tree of Figure 13.3.7.2-1 was created to maximize interoperability and interchangeability by restricting the use of Ethernet on the Expansion Plane when a SOSA PIC’s Data Plane and Control Plane are oversubscribed. Oversubscription is a direct result of a system’s need for more bandwidth and lower latency requirements. The decision tree, shown below, illustrates the intent of the rules and suggestions and provides guidance for the user depending upon their information domain needs.

Note: The use of single UTPs and single FPs as shown in the decision tree neither implies a requirement nor precludes the use of other size pipes.

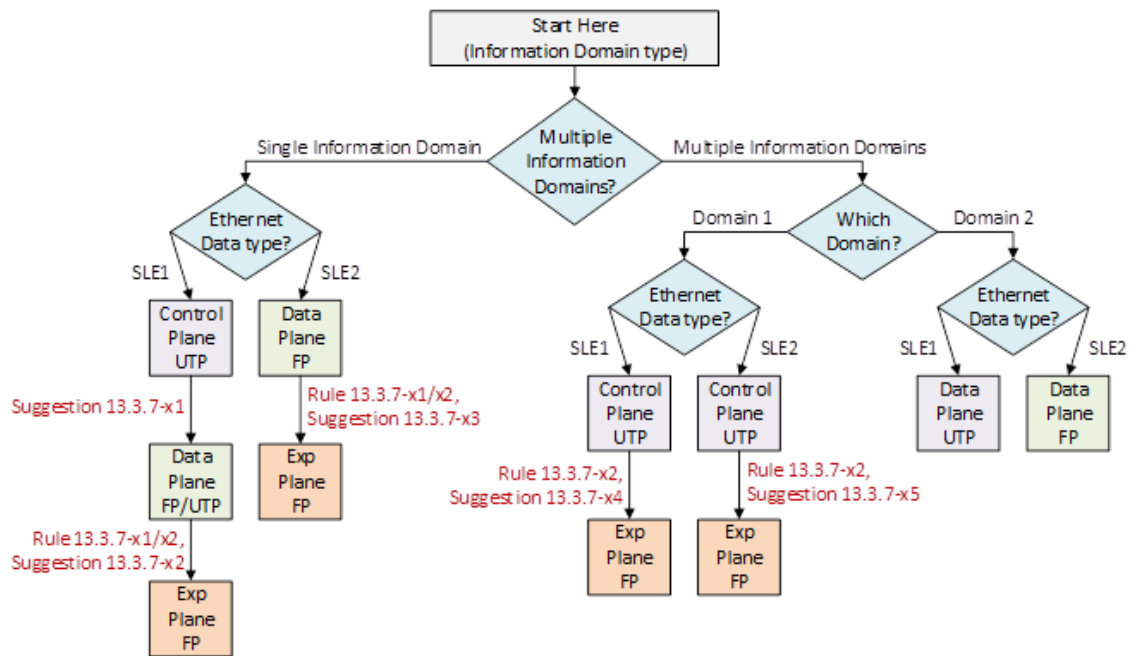


Figure 13.3.7.2-1: Ethernet Backplane Connectivity Decision Tree

Note: Although single UTPs and FPs are shown in the decision tree in Figure 13.3.7.2-1, there can be more than one.

Rule 13.3.7.2-1: For a SOSA PIC in a single information domain, the Expansion Plane shall only be used for Ethernet (i.e., contains Ethernet protocol for EP1/EP2 in the AMPS String), if the Data Plane FP is implemented via an AMPS String (i.e., does not contain an “N” for DP1 in the AMPS String). Conformance Methodology (I)

Rule 13.3.7.2-2: For a SOSA PIC, the Expansion Plane shall only be used for Ethernet (i.e., contains Ethernet protocol for EP1/EP2 in the AMPS String), if the Control Plane is implemented via the AMPS String (i.e., does not contain an “N” for CP1 in the AMPS String). Conformance Methodology (I)

Suggestion 13.3.7.2-1: It is suggested that for a SOSA PIC in a single information domain, the Data Plane not be used for SLE1 Ethernet traffic unless all Control Plane bandwidth is consumed and/or latency requirements cannot be met.

Suggestion 13.3.7.2-2: It is suggested that for a SOSA PIC in a single information domain, the Expansion Plane not be used for SLE1 Ethernet traffic unless all Control and Data Plane bandwidth is consumed and/or latency requirements cannot be met.

Suggestion 13.3.7.2-3: It is suggested that for a SOSA PIC in a single information domain, the Expansion Plane not be used for SLE2 Ethernet traffic unless all Data Plane bandwidth is consumed and/or latency requirements cannot be met.

Suggestion 13.3.7.2-4: It is suggested that for a SOSA PIC in multiple information domains, the Expansion Plane not be used for SLE1 Ethernet traffic unless all Control Plane bandwidth is consumed and/or latency requirements cannot be met.

Suggestion 13.3.7.2-5: It is suggested that for a SOSA PIC in multiple information domains, the Expansion Plane not be used for SLE2 Ethernet traffic unless all Control Plane bandwidth is consumed and/or latency requirements cannot be met.

Observation 13.3.7.2-1: Rule 13.3.7-1 and Rule 13.3.7-2 make it so that if a PIC implements Ethernet over the Expansion Plane, it must also implement the Control and Data Plane ports. At the system level, it is intended that the Expansion Plane only be used for Ethernet if the Control Plane or Data Plane ports are already consumed. In these sorts of cases, the Expansion Plane can frequently be thought of as an extension of either the Data Plane or the Control Plane depending on how SOSA modules are mapped to the PICs in question.

Observation 13.3.7.2-2: With Suggestion 13.3.7.2-5, it is intended that SOSA modules use the Control Plane before the Expansion Plane whenever possible for SLE2 Ethernet traffic when the Control Plane and Expansion Plane are in a separate information domain from the Data Plane. The suitability of this is based on whether the Control Plane provides sufficient bandwidth and a minimization of latency for a given SOSA module. The expectation is that SLE2 Ethernet traffic will use the Expansion Plane when a SOSA module’s application use of bandwidth and latency requirements exceed the stated capabilities of the SOSA PIC’s Control Plane.

Observation 13.3.7.2-3: With Suggestions 13.3.7.2-1, 13.3.7.2-2, and 13.3.7.2-4 it is intended that SOSA modules with SLE1 Ethernet traffic use the Control Plane first, then the Data Plane, if allowed, before the Expansion Plane. The suitability of this is based on whether the Control Plane provides sufficient bandwidth and a minimization of latency for a given SOSA module. It is important to note that only the Control Plane is required to support SLE1 traffic, so using the Data and/or Expansion Plane will result in reduced interoperability.

Table 13.3.7.2-1: Protocol Support Levels for SLE1 and SLE2

AMPS ANSI/VITA 65.0 Non-Switch Backplane Interface		Protocol Support Level	
		SLE1	SLE2
Data Plane	All		X
Control Plane	All	X	
Expansion Plane	All		X
Optical	4x		X

13.3.8 Backplane Apertures for Analog and Optical Fiber

Two aperture interface standards are utilized in VITA 65 Slot Profiles, used by this document: ANSI/VITA 67.3 and VITA 66.5 for the coax and fiber optics, respectively. The Slot Profiles in the previous subsections only define the physical interface of the aperture, whereas this section will further define the recommended signal to be placed on each interface; e.g., the RF channels for a tuner.

This information is intended to minimize the amount of re-cabling required when replacing capabilities within a slot but allowing customization when absolutely required. This balance is accomplished by focusing on the I/O channels while allowing the other connections to be used as required by the user.

13.3.8.1 Terminology, Signal Definitions, MORA Mapping, and Signal Orientation

Table 13.3.8.1-1 lists all relevant signal types from the MORA Specification, Version 2.4 used in the SOSA Technical Standard to define the selection of available coaxial pin assignments in the subsequent subsections of this document. A mapping of coaxial signal functions to MORA Signal Ports in the table provides guidance as to the type of port and its associated role viewed from a sensor system level. This, in turn, provides a connection to Figure 13.3.8.1-1 with example notional placement of SOSA PICs with ANSI/VITA 67.3 apertures providing analog signal I/O in a sensor system under their respective MORA Signal Port types; i.e., Receive RF Chain (ARX) and Transmit RF Chain (ATX).

It is worth noting that MORA establishes this naming convention for users to have control of some specific resources when necessary and then to release when control is no longer necessary.

Note: It is useful for the reader when reviewing Table 13.3.8.1-1 and connecting the MORA Signal Port types to coaxial signal assignments to also review and understand all relevant signal descriptions for context.

Note: The MORA Specification, Version 2.4 defines all signal types as seen in Table 13.3.8.1-1 in §3.2, §4.6.3.1.1, §4.6.3.1.2, §4.6.3.1.3, §4.6.3.3.1, §4.6.3.3.2, and §5.3.5.1 (Item 46 – Signal Port), respectively.

Table 13.3.8.1-1: Terminology, Signal Definitions, and MORA Mapping

Name	Description	RF Chain Location	MORA Signal Port Mapping		
			Port Type:	Sub Type:	Role (@ PIC):
CLKINn	High Frequency clock or LO input to PIC, typically in GHz range	N/A	ARI	OSC or CLK	Consumer
REFINn	Low Frequency clock or LO input to PIC, typically in MHz range	N/A	ARI	OSC or CLK	Consumer
TRIGINn	Trigger or 1 Pulse Per Second (1PPS) input to PIC	N/A	ARI	CLK	Consumer
CLKOUTn	High Frequency clock or LO output from PIC, typically in GHz range	N/A	ARO	OSC or CLK	Producer
REFOUTn	Low Frequency clock or LO output from PIC, typically in MHz range	N/A	ARO	OSC or CLK	Producer
TRIGOUTn	Trigger or 1 Pulse Per Second (1PPS) output from PIC	N/A	ARO	CLK	Producer
UDn	User Defined. Direction not defined	N/A	ARO or ARI	OSC or CLK	Producer or Consumer
AINn	Generic receive signal to PIC	End	ARX	RSC or ISC	Consumer
AOUTn	Generic transmit signal from PIC	End	ATX	RSC or ISC	Producer
USFINn	Upstream receive signal to PIC	Middle	ARX	RSC or ISC	Consumer
DSFOUTn	Downstream transmit signal from PIC	Middle	ARX	RSC or ISC	Producer
DSFINn	Downstream receive signal to PIC	Middle	ATX	RSC or ISC	Consumer
USFOUTn	Upstream transmit signal from PIC	Middle	ATX	RSC or ISC	Producer
RFn	RF signal (without direction specified)	Unknown	ARX or ATX or ATR	RSC or ISC	Producer, Consumer or Both
IFn	IF signal (without direction specified)	Unknown	ARX or ATX or ATR	ISC	Producer, Consumer or Both
GPSINn	GPS Antenna receive to PIC	End	ARX	RSC	Consumer

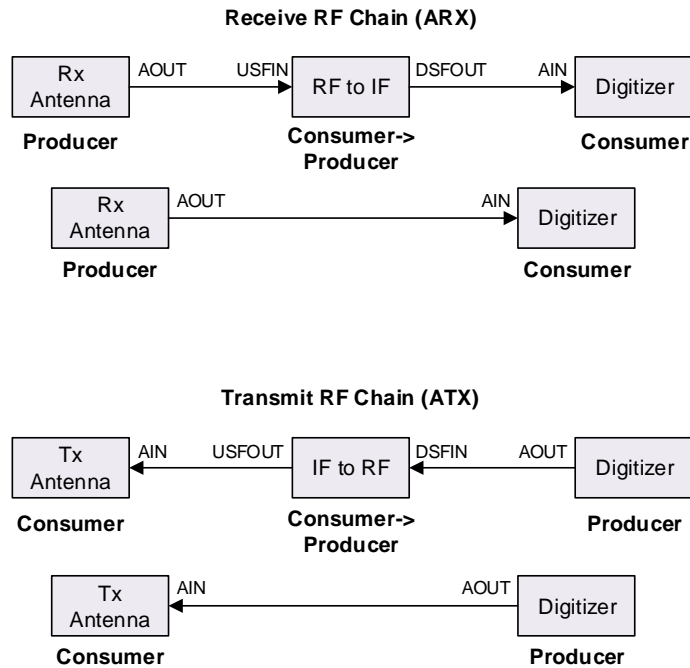


Figure 13.3.8.1-1: PIC Signal Chain Position

13.3.8.2 Backplane RF Pin Out Tables

The following section lists valid pin out definitions for ANSI/VITA 67.3 blocks using coaxial cable. Where applicable a decision tree is included to help minimize bifurcation in the market by guiding decisions, when possible, to use the same pin outs based on a use-case. It is not required to populate all the locations listed in the tables.

Rule 13.3.8.2-1: A SOSA PIC shall populate its ANSI/VITA 67.3 coaxial pin assignments starting with the lowest numbered element in a signal type from Table 13.3.8.1-1, except for user-defined signals.

Observation 13.3.8.2-1: The element number in Table 13.3.8.1-1 is designated with the letter “n”. For example, a PIC utilizing column B1 from Table 13.3.8.3-1 will first populate CLKOUT1, then CLKOUT2, and then the remaining CLKOUTn in numerical order.

Permission 13.3.8.2-1: The user-defined signals (i.e., UDx) in Table 13.3.8.1-1 may be populated in any order.

13.3.8.3 SMPM-10 Radial Clock Pin Out

This section describes the coaxial pin designations for the 3U Radial Clock Profile SLT3x-TIM-2S1U22S1U2U1H-14.9.2-1.

Figure 13.3.8.3-1 provides the ANSI/VITA 65.1 pin definition for the 10_SMPM_contacts-6.4.5.6.3 ANSI/VITA 67.3 aperture.

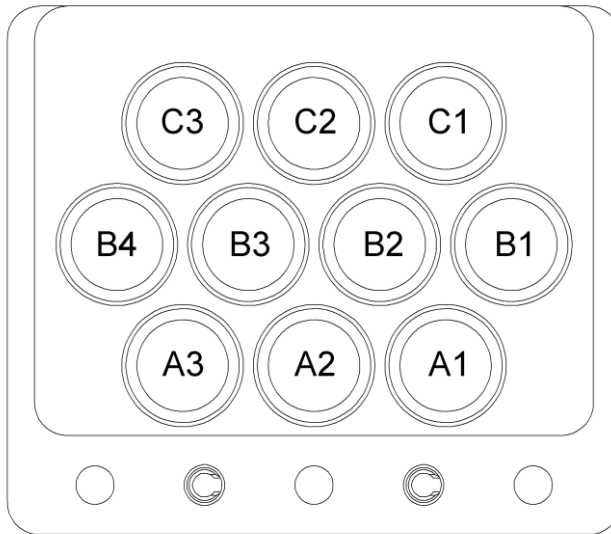


Figure 13.3.8.3-1: ANSI/VITA 67.3 10_SMPM_contacts-6.4.5.6.3 Coaxial Pin Locations (viewed from the PIC side of the backplane)

Table 13.3.8.3-1: ANSI/VITA 67.3 10_SMPM_contacts-6.4.5.6.3 Coaxial Pin Designations

Type		PNT	Clock Distribution	
Pinout/ID		PNT	Clock OUT	Ref OUT
Contact	Signal	A1	B1	B2
A1	1	REFOUT	CLKOUT1	REFOUT1
A2	2	TRIGOUT	CLKOUT2	REFOUT2
A3	3	RSVD	CLKOUT3	REFOUT3
B1	4	TRIGIN	TRIGIN	TRIGIN
B2	5	REFIN	REFIN/CLKIN	REFIN
B3	6	RSVD	CLKOUT4	REFOUT4
B4	7	RSVD	CLKOUT5	REFOUT5
C1	8	RSVD	CLKOUT6	REFOUT6
C2	9	GPSIN2	RSVD	RSVD
C3	10	GPSIN1	RSVD	RSVD
Supported VPX Slot Profiles		14.9.2-1	14.9.2-1	14.9.2-1
Use Case(s)		PNT	Full Rate Clock	Reference

Rule 13.3.8.3-1: A SOSA PIC with Slot Profile SLT3x-TIM-2S1U22S1U2U1H-14.9.2-1 shall select its ANSI/VITA 67.3 10_SMPM_contacts-6.4.5.6.3 coaxial pin assignment from Table 13.3.8.3-1. Conformance Methodology (I)

13.3.8.4 SMPM-14 Pin Designation and Usage

Figure 13.3.8.4-1 provides the ANSI/VITA 65.1 pin definition for the SMPM-14 ANSI/VITA 67.3 aperture.

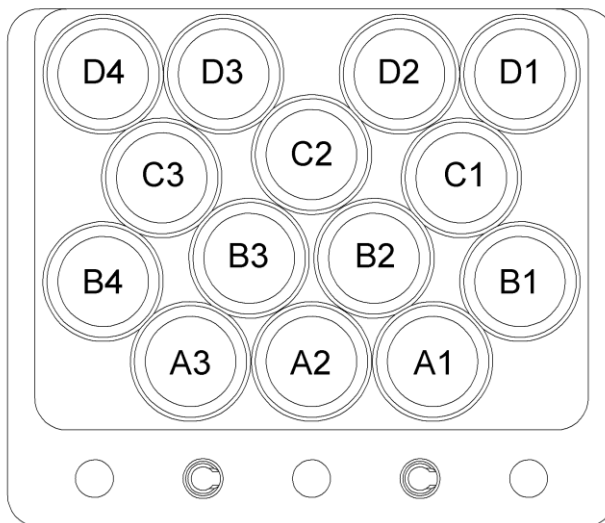


Figure 13.3.8.4-1: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Coaxial Pin Locations (viewed from the PIC side of the backplane)

Figure 13.3.8.4-1 portrays the 14_SMPM_contacts-6.4.5.6.4 contact designation from the front of the backplane perspective.

Table 13.3.8.4-1: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Coaxial Pin Designations

Type		unspecified	Digitizer					Signal Conditioning Cards			Clock Distribution	
RF Chain	location direction		End					Middle			N/A	
Pinout/ID		unspecified	RX	RX/TX		TX		RX	RX/TX	TX	N/A	
Contact	Signal	8RF or 4RF/4IF	8IN/2OUT	5IN/5OUT	4IN/4OUT	4IN/4OUT	8OUT/2IN	5IN/5OUT	Dual 2OUT/2IN	5OUT/5IN	Clock OUT	REF OUT
		A1	B1	C1	D1	F1	E1	C2	F2	G2	H1	H2
B1	1	RF1	AIN1	AIN1	AOUT1	AIN1	AOUT1	USFIN1	USFIN1	USFOUT1	CLKOUT1	REFOUT1
B4	2	RF2	AIN2	AIN2	AIN1	AIN2	AOUT2	USFIN2	USFIN2	USFOUT2	CLKOUT2	REFOUT2
D1	3	RF3	AIN3	AIN3	AOUT2	AOUT1	AOUT3	USFIN3	USFOUT1	USFOUT3	CLKOUT3	REFOUT3
D4	4	RF4	AIN4	AIN4	AIN2	AOUT2	AOUT4	USFIN4	USFOUT2	USFOUT4	CLKOUT4	REFOUT4
B2	5	RF5/IF1	AIN5	AOUT1	AOUT3	AOUT3	AOUT5	DSFOUT1	DSFOUT1	DSFIN1	CLKOUT5	REFOUT5
B3	6	RF6/IF2	AIN6	AOUT2	AIN3	AOUT4	AOUT6	DSFOUT2	DSFOUT2	DSFIN2	CLKOUT6	REFOUT6
D2	7	RF7/IF3	AIN7	AOUT3	AOUT4	AIN3	AOUT7	DSFOUT3	DSFIN1	DSFIN3	CLKOUT7	REFOUT7
D3	8	RF8/IF4	AIN8	AOUT4	AIN4	AIN4	AOUT8	DSFOUT4	DSFIN2	DSFIN4	CLKOUT8	REFOUT8
C1	9	UD1	AOUT1/UD1	AOUT5/UD1	UD1	UD1	AIN1/UD1	USFOUT1/UD1	UD1	USFIN1/UD1	CLKOUT9	REFOUT9
C2	10	UD2	AOUT2/UD2	AIN5/UD2	UD2	UD2	AIN2/UD2	DSFIN1/UD2	UD2	DSFOUT1/UD2	CLKOUT10	REFOUT10
C3	11	UD3	UD3	UD3	UD3	UD3	UD3	UD3	UD3	UD3	CLKOUT11	REFOUT11
A1	12	UD4	UD4	UD4	UD4	UD4	UD4	UD4	UD4	UD4	CLKIN	CLKIN
A2	13	UD5	UD5	UD5	UD5	UD5	UD5	UD5	UD5	UD5	TRIGIN	TRIGIN
A3	14	UD6	UD6	UD6	UD6	UD6	UD6	UD6	UD6	UD6	REFIN	REFIN
Supported VPX Slot Profiles	16.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.6.11-4	14.9.2-2	14.9.2-2
	16.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	14.6.14-11	X	X
	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	10.6.3-2	X	X
	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	10.6.4-2	X	X
	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	10.6.5-9	X	X
Use Case(s)	Input/Output	Lots of Inputs	Transceiver	Transceiver	Transceiver	Lots of Outputs	Downconverter	Transverter	Upconverter	Full Rate Clock	Reference	

Rule 13.3.8.4-1: A SOSA PIC shall select its ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 coaxial pin assignment from Table 13.3.8.4-1. Conformance Methodology (I)

Observation 13.3.8.4-1: If a single input clock is used, then utilizing UD3 allows for compatibility with pin outs using the extra RF on UD1 and UD2.

Suggestion 13.3.8.4-1: Given the location of a PIC in the signal chain, the selection of a suitable pin out for 14_SMPM_contacts-6.4.5.6.4 should be driven by the logic in the decision tree in Figure 13.3.8.4-2.

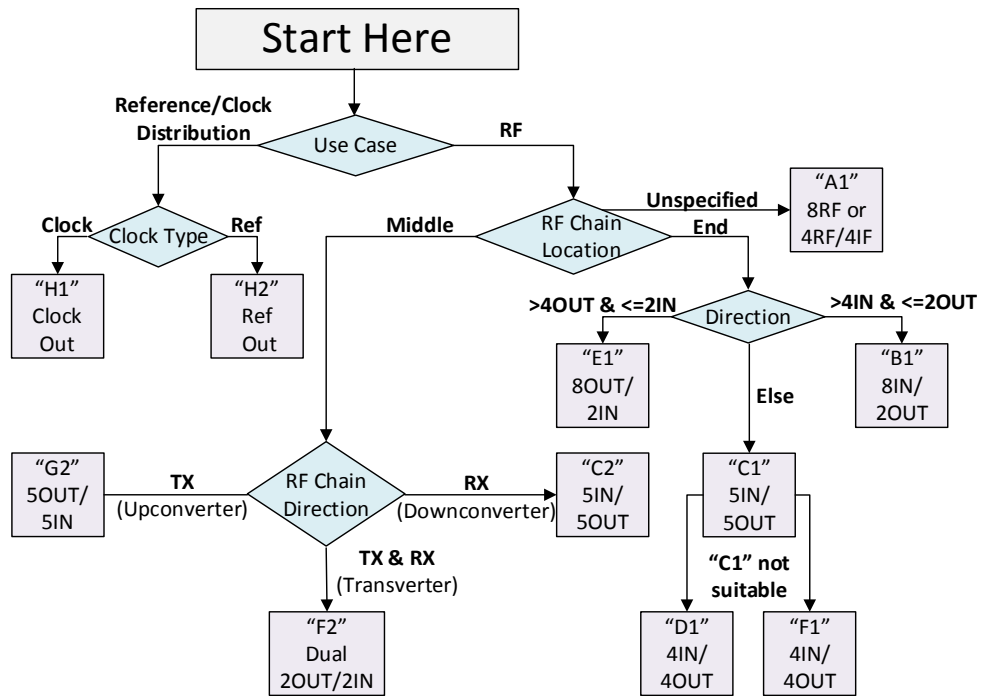


Figure 13.3.8.4-2: ANSI/VITA 67.3 14_SMPM_contacts-6.4.5.6.4 Decision Tree

13.3.8.5 10 and 20 NanoRF Designation and Usage

Figure 13.3.8.5-1 provides the ANSI/VITA 65.1 pin locations for the NanoRF contacts-6.4.5.6.10 ANSI/VITA 67.3 aperture.

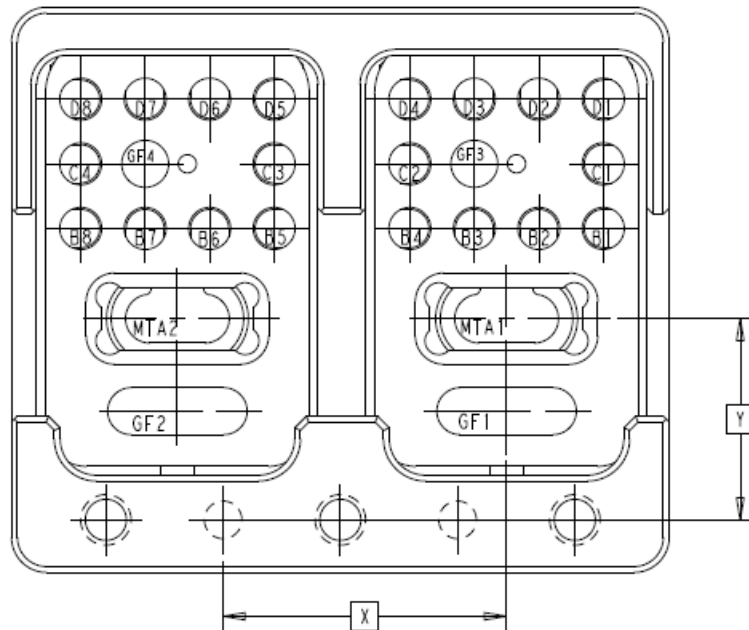


Figure 13.3.8.5-1: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Coaxial Pin Locations (viewed from the PIC side of the backplane)

Loc	Type		unspecified	Digitizer			Signal Conditioning Cards		
	RF Chain	location direction	unspecified	End			Middle		
	Chain	direction	unspecified	RX	RX/TX	TX	RX	RX/TX	TX
	Pinout/ID		8RF or 4RF/4IF	16IN	8IN/8OUT	16OUT	8IN/8OUT	Dual 4IN/4OUT	8OUT/8IN
	Contact	Signal	A1	B1	C1	E1	C2	F2	G2
P2B	D1	1	RF1	AIN1	AIN1	AOUT1	USFIN1	USFIN1	USFOUT1
	D2	2	RF2	AIN2	AIN2	AOUT2	USFIN2	USFIN2	USFOUT2
	D3	3	RF3	AIN3	AIN3	AOUT3	USFIN3	USFOUT1	USFOUT3
	D4	4	RF4	AIN4	AIN4	AOUT4	USFIN4	USFOUT2	USFOUT4
	B1	5	RF5/IF1	AIN5	AOUT1	AOUT5	DSFOUT1	DSFOUT1	DSFIN1
	B2	6	RF6/IF2	AIN6	AOUT2	AOUT6	DSFOUT2	DSFOUT2	DSFIN2
	B3	7	RF7/IF3	AIN7	AOUT3	AOUT7	DSFOUT3	DSFIN1	DSFIN3
	B4	8	RF8/IF4	AIN8	AOUT4	AOUT8	DSFOUT4	DSFIN2	DSFIN4
	C1	17	UD1	UD1	UD1	UD1	UD1	UD1	
	C2	18	CLKIN/UD2	CLKIN/UD2	CLKIN/UD2	CLKIN/UD2	CLKIN/UD2	CLKIN/UD2	
P2A	D5	9	RF9	AIN9	AIN5	AOUT9	USFIN5	USFIN3	USFOUT5
	D6	10	RF10	AIN10	AIN6	AOUT10	USFIN6	USFIN4	USFOUT6
	D7	11	RF11	AIN11	AIN7	AOUT11	USFIN7	USFOUT3	USFOUT7
	D8	12	RF12	AIN12	AIN8	AOUT12	USFIN8	USFOUT4	USFOUT8
	B5	13	RF13/IF5	AIN13	AOUT5	AOUT13	DSFOUT5	DSFOUT3	DSFIN5
	B6	14	RF14/IF6	AIN14	AOUT6	AOUT14	DSFOUT6	DSFOUT4	DSFIN6
	B7	15	RF15/IF7	AIN15	AOUT7	AOUT15	DSFOUT7	DSFIN3	DSFIN7
	B8	16	RF16/IF8	AIN16	AOUT8	AOUT16	DSFOUT8	DSFIN4	DSFIN8
	C3	19	UD3	UD2	UD2	UD2	UD2	UD2	
	C4	20	UD4	UD3	UD3	UD3	UD3	UD3	
Supported VPX Slot Profiles			14.6.11-12 14.6.13-4	14.6.11-12 14.6.13-4	14.6.11-12 14.6.13-4	14.6.11-12 14.6.13-4	14.6.11-12 14.6.13-4	14.6.11-12 14.6.13-4	
Use Case(s)			Input/Output	Lots of Inputs	Transceiver	Lots of Outputs	Downconverter	Transverter	Upconverter

Figure 13.3.8.5-2: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Coaxial Pin Designations

Figure 13.3.8.5-1: A SOSA PIC shall select its ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 coaxial pin assignment from Figure 13.3.8.5-2. Conformance Methodology (I)

Suggestion 13.3.8.5-1: Given the location of a PIC in the signal chain, the selection of a suitable pin out for NanoRF contacts-6.4.5.6.10 should be driven by the logic in the decision tree in Figure 13.3.8.5-3.

RF Pinout Decision Matrix (10/20 NanoRF/MT)

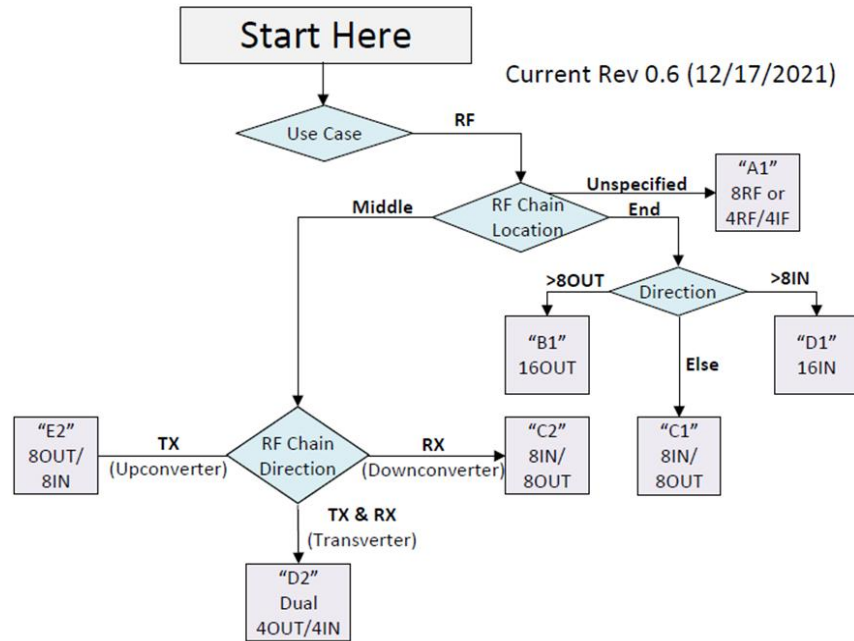


Figure 13.3.8.5-3: ANSI/VITA 67.3 NanoRF contacts-6.4.5.6.10 Decision Tree

13.3.8.6 AMPs RF Pin Out Designations

Each RF pin out choice depicted in each of the pin out tables has a unique Slot Profile identifier. Therefore, the column heading for each pin out can be used to associate the pin out choice with the designator in the associated AMPS String.

For example, the AMPS String for a 3U Compute Intensive Payload with the 14 SMPM aperture with eight inputs and two outputs could be:

- MODA3p-16.6.11-1-j-F2C-(E8-E7)(P3F-P3F)(E7)(G5)[E19]<RF1>

Where j = 4 (14 SMPM) and <RF1> would be <B1> (8 in / 2 out) so the final string would be:

- MODA3p-16.6.11-1-4-F2C-(E8-E7)(P3F-P3F)(E7)(G5)[E19]<B1>

13.4 SOSA Plug-In Cards (PICs) Using VNX

A subset of VNX+ has been selected as the baseline for a Small Form Factor (SFF) PIC standard to be used for current and future SOSA requirements. The specific SOSA VNX+ requirements will be refined in a future version of this document.

The contents of this section are intended to convey the initial SOSA VNX+ requirements as defined by the SOSA SFFSC.

Rule 13.4-1: The VNX+ form factor as defined in VITA 90.2 shall be used as the SOSA Technical Standard VNX+ PIC form factor. Conformance Methodology (I)

13.4.1 Glossary

Table 13.4.1-1: Glossary

Term	Definition
Large Aperture	An Aperture Fill beside the backplane connector with dimensions of 25.12mm x 12.99mm.
Module Height	Term used in place of “Slot Pitch” for VNX+ SFF applications.
Small Aperture	An Aperture Fill beside the backplane connector with dimensions of 12.54mm x 12.99mm.

13.4.2 VNX+ Module Heights

The VNX+ module heights as balloted and approved by the SOSA SFFSC are shown in Figure 13.5.2.4-1. The connectors and Aperture Fills shown are for illustration purposes only.

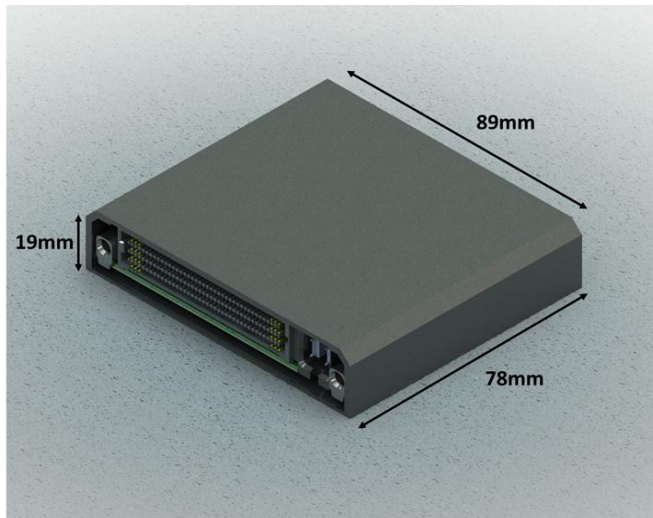


Figure 13.4.2-1: 19mm VNX PIC with No Aperture

13.4.3 VNX+ Connector and Aperture Fills

Reference VITA 90.0 (VNX+ Base Standard) and VITA 90.2 (Optical and Coaxial Interconnects for VNX+ Systems).

Rule 13.4.3-1: The PIC sizes (above) shall utilize predefined combinations of a VNX+ connector along with an optional Aperture module, whose size is described as either a Small Aperture or a Large Aperture, with the Aperture module consisting of a single Aperture Block with predefined numbers of RF and/or optical contacts. Conformance Methodology (I)

Rule 13.4.3-2: Any VNX+ PIC utilizing a Small Aperture shall adhere to the predefined aperture dimensions shown in Figure 13.4.3-1. Conformance Methodology (I)

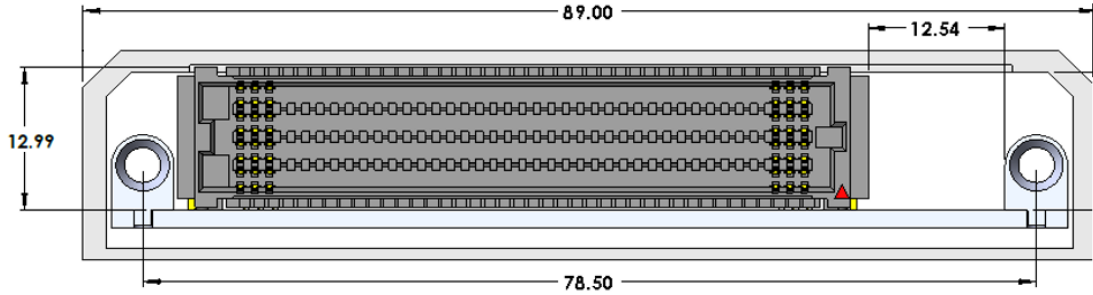


Figure 13.4.3-1: VNX+ PIC Small Aperture Dimensions

Rule 13.4.3-3: Any VNX+ PIC utilizing a Large Aperture shall adhere to the predefined aperture dimensions shown in Figure 13.4.3-2. Conformance Methodology (I)

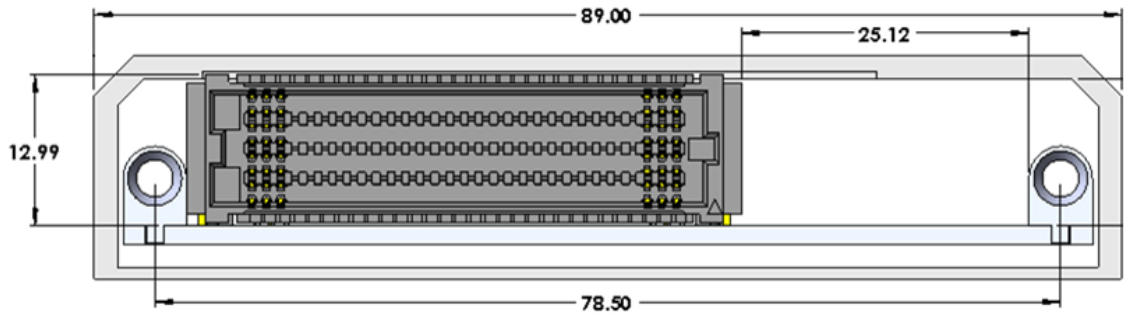


Figure 13.4.3-2: VNX+ PIC Large Aperture Dimensions

The VNX+ connector is unitized for Utility Plane, Data Plane, Control Plane, Expansion Plane, Low Latency Plane, predefined overlays, and other signals as could be deemed necessary and defined in a Slot Profile adopted in this document.

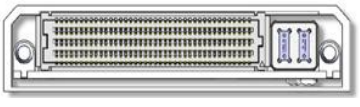
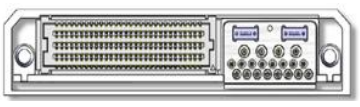
The Aperture module consists of a mechanical Aperture Block which serves to properly align and position coaxial contacts and optical connectors commonly utilized for RF, video, and/or high-speed data.

13.4.3.1 19mm PIC Connector and Aperture Fill

Rule 13.4.3.1-1: The 19mm VNX+ PIC shall utilize predefined combinations of VNX+ connectors and Aperture Fill as shown in Table 13.4.3.1-1. Conformance Methodology (I)

Table 13.4.3.1-1: 19mm VNX Connector and Aperture Fills

Connector/Aperture Combination	Config Class	Connector Type	Aperture Fill Config	Image
VNX+ Connector Only	1	400-pin	None	

Connector/Aperture Combination	Config Class	Connector Type	Aperture Fill Config	Image
VNX+ w/Small Aperture	2	320-pin	2x MT	
VNX+ w/Large Aperture	3	240-pin	2x MT 20x RF	

13.4.3.2 39mm PIC Connector and Aperture Configuration

Note: This material is not yet approved by ANSI/VITA 90.x and is subject to change at any reference to 32.5mm and 39mm module heights.

The 39mm VNX+ PIC will utilize a variety of predefined combinations of VNX+ connectors used for S0, S1, and S2 signals as well as an Aperture module consisting of an Aperture Block specifically machined to accommodate various optical MT ferrule and coaxial connectors as shown in Table 13.4.3.2-2.

Table 13.4.3.2-2: 39mm VNX+ Connector and Aperture Configurations

Connector/Aperture Combination	Config Class	Connector Type	Aperture Fill Config	Image
VNX+ Connector Only	TBD	400-pin	TBD	TBD
VNX+ w/Small Aperture	TBD	320-pin	TBD	TBD
VNX+ w/Large Aperture	TBD	240-pin	TBD	TBD

13.4.3.3 Connector Family

The SOSA SFFSC is developing content that is 19mm SOSA VNX+ PIC to a current version of VITA 90.0 and its fully compliant backplane interface connectors as shown in VITA 90.0 §TBD (400-pin) or VITA 90.2 §7.1.2 (240-pin and 320-pin).

Rule 13.4.3.3-1: SOSA VNX+ PICs shall use backplane interface connectors that are designed to VITA 90.0 and VITA 90.2. Conformance Methodology (I, T)

13.4.3.4 Backplane Apertures for RF/Optical Fiber

One aperture interface standard is utilized in ANSI/VITA 90.1-2022x Slot Profiles: the VITA 90.2 standard for the coaxial contacts and fiber optics, collectively. The Slot Profiles in the previous subsections only define the physical interface of the aperture, whereas this section will further define the recommend signal to be placed on each interface; e.g., the RF channels for a tuner.

This information is intended to minimize the amount of re-cabling required when replacing capabilities within a slot but allowing customization when absolutely required. This balance is accomplished by focusing on the I/O channels while allowing the other connections to be used as required by the user. A future version of this document will include further definition of all SOSA Slot Profiles using VITA 90.2 interfaces in this section.

Analog I/O in this section refers to both RF and IF signals.

13.4.4 VNX+ System Clock

TBD

13.4.5 Utility Plane Requirements

TBD

13.4.5.1 Power Distribution

TBD

13.4.5.2 Geographical Addressing

TBD

13.4.5.3 Console Port

TBD

13.4.5.4 Non-Volatile Memory Read Only (NVMRO)

TBD

13.4.6 General Mechanical

TBD

13.4.6.1 Front Panel Connections

TBD

13.4.6.2 PIC Module Size

Observation 13.4.6.2-1: Because VNX+ is classified as SFF, it is recognized that applications could require that modules be placed adjacent to or in other orientations, making the idea of “slot pitch” irrelevant. VNX+ defines PIC “module size” instead of “slot pitch”.

The SOSA SFFSC is developing content that aligns its 19mm SOSA VNX+ PIC with the current VITA 90.0 standard family of documents.

13.4.6.3 PIC Module Exterior Dimensions

Rule 13.4.6.3-1: 19mm VNX+ modules shall conform to the exterior dimensions in VITA 90.0 §6.1. Conformance Methodology (I)

13.4.6.4 Keying

TBD

13.4.7 Thermal Design

VITA 90.0 describes a thermal interface utilizing compressible Thermal Interface Material (TIM) between the two side-faces, the one handle-face, and the heat-transfer mechanism (fins, cold-plate, heat-exchanger, etc.).

Observation 13.4.7-1: Additional heat-transfer mechanisms, such as wedge locks and mounting plates used for single module deployments, are to be defined in ANSI/VITA 90.4-202x §TBD.

Table 13.4.7-1: Heat Transfer Mechanisms

Heat Transfer Mechanism	Figure
Compressible TIM to Heat Exchanger	TBD
Wedge Locks	TBD
Single-Module Deployment	TBD

13.4.8 VNX+ Payload Slot Profiles

A SOSA VNX+ Slot Profile describes an application-specific pin map to provide specific functions to a SOSA VNX+ PIC. A Slot Profile is used to define the connector type and how each pin is allocated.

All VNX+ Slot Profiles were described within ANSI/VITA 90.1-202x and its three use-case connector types: 240-pin, 320-pin, and 400-pin. All Slot Profiles are grouped into sets of pins called segments. The segments are as follows:

- S0 Utility Segment: common for all VNX+ PICs and Profiles; pins are allocated to the Utility Plane for power, grounds, system discrete signals, and system management
- S1 Communications Segment: region containing primary Data Plane, Control Plane, and/or Expansion Plane links
- S2 Overlay & Aperture Segment: region on some profiles that is used for application-specific Slot Profile implementations

A VNX+ PICP defines ports assigned to specific pins, while the AMPS String defines the mapping of protocols to those ports.

PICs have at least an S0 Utility Segment and an S1 Communications Segment. Regarding the S2 Overlay & Aperture Segment, the connectors vary:

- The 240-pin Payload Slot Profiles offer an S2 Aperture region
- The 320-pin Payload Slot Profiles offer an S2A Overlay and an S2B Aperture region, while the other 320-pin Payload Slot Profiles simply have an S2B Aperture region
- The 400-pin Payload Slot Profiles offer an S2 Overlay region

- Non-Payload Slot Profiles like the Switch Profiles could offer variable S1 Communications Segments and do not offer an S2 Overlay region

To fully specify the SOSA VNX+ PICPs, AMPS Strings are used. AMPS Strings specify both the Slot Profile, including the Slot Profile dash option, and the protocols assigned to each port. See Section 13.3 for a description of how AMPS is applied to SFF.

13.4.8.1 VNX+ Payload Slot Profiles

As a starting point to define basic functionality for VNX+ PICPs, this document uses the concept of Payload Slot Profiles in ANSI/VITA 90.1-202x. The Payload Slot Profiles are used to define baseline profile templates for one of each of the three connector types described within ANSI/VITA 90.1-202x (240-pin, 320-pin, 400-pin).

Payload Slot Profiles are based on a set of three pin map templates, one for each of the three connectors defined by ANSI/VITA 90.1-202x (240-, 320-, and 400-pin). All three templates contain a common S0 Utility Segment, S1 Communication Segment, and an S2 Overlay Segment. In the case of the 240 and 320 pin templates, the S2 Overlay Segment is further divided into S1A Overlay and S1B Aperture regions. VNX+ Payload Slot Profiles are built on these templates, with different Payload Slot Profiles defining different S2 Overlay & Aperture Segment definitions (although different Aperture Fill options are captured in a table under the base profile).

The 240-pin Payload Slot Profile is both a template and a fully defined Payload Slot Profile (described in Section 13.4.8.1.3). The 320- and 400-pin (described in Section 13.4.8.1.2 and Section 13.4.8.1.3) contain all the same regions and pin functions as the 240-pin Payload Slot Profile but expand the Data Plane and Control Plane pipes. The remaining pins in the 320- and 400-pin Payload Slot Profiles form a generic “overlay” region. It is this overlay region, along with the Aperture Fill region, that is used to form the different Slot Profiles based on the templates.

Rule 13.4.8.1-1: All rules described in ANSI/VITA 90.1-202x §TBD and §TBD apply to the SOSA VNX+ cards utilizing these Payload Slot Profiles.

13.4.8.1.1 VNX+ 240-Pin Payload Slot Profiles

The 240-pin VNX+ Payload PIC Slot Profile Template is defined by Figure 13.4.8.1.1-1. The ANSI/VITA 90.1-202x Slot Profile Template from ANSI/VITA 90.1-202x §TBD shown in Figure 13.4.8.1.1-1 is for a 240-pin Payload PIC with a full aperture for RF and/or optical blind-mate connections.

VNX+ Pin Map for 240-Pin High-Speed Connector with Full Aperture																													
Col	Row A			Row B			Row C			Row D			Row E			Row F			Row G			Row H			Col				
	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name		Plane	Pin	Signal Name	
1	A1	EP_RX0_P		B1	GND		C1	EP_RX3_P		D1	GND		E1	EP_RX6_P		F1	GND		G1	VSS1_12V		H1	VSS1_12V		1				
2	A2	EP_RX0_N	Expansion	B2	GND	Expansion	C2	EP_RX3_N	Expansion	D2	GND	Expansion	E2	EP_RX6_N	Expansion	F2	GND	Expansion	G2	VSS1_12V	Expansion	H2	VSS1_12V	Expansion	2				
3	A3	GND		B3	EP_RX2_P		C3	GND		D3	EP_RX5_P		E3	GND		F3	SCM1_RX+		G3	VSS1_12V		H3	VSS1_12V		3				
4	A4	GND		B4	EP_RX2_N		C4	GND		D4	EP_RX5_N		E4	GND		F4	SCM1_RX-		G4	VSS1_12V		H4	VSS1_12V		4				
5	A5	EP_RX1_P		B5	GND		C5	EP_RX4_P		D5	GND		E5	EP_RX7_P		F5	GND		G5	GND		H5	GND		5				
6	A6	EP_RX1_N	Expansion	B6	GND	Expansion	C6	EP_RX4_N	Expansion	D6	GND	Expansion	E6	EP_RX7_N	Expansion	F6	GND	Expansion	G6	VSS2_5V	Expansion	H6	VSS2_5V	Expansion	6				
7	A7	GND		B7	DP1_RX1_P		C7	GND		D7	DP2_RX0_P		E7	GND		F7	IO0_DATA		G7	VSS2_5V		H7	VSS2_5V		7				
8	A8	GND		B8	DP1_RX1_N		C8	GND		D8	DP2_RX0_N		E8	GND		F8	I2C_CLK		G8	VSS2_5V		H8	VSS2_5V		8				
9	A9	DP1_RX0_P	Data	B9	GND	Data	C9	DP1_RX3_P	Data	D9	GND	Data	E9	DP2_RX2_P	Data	F9	GND	Data	G9	VSS2_5V	Data	H9	VSS2_5V	Data	9				
10	A10	DP1_RX0_N	Expansion	B10	GND	Expansion	C10	DP1_RX3_N	Expansion	D10	GND	Expansion	E10	DP2_RX2_N	Expansion	F10	GND	Expansion	G10	GND	Expansion	H10	GND	Expansion	10				
11	A11	GND		B11	DP1_RX2_P		C11	GND		D11	DP2_RX1_P		E11	GND		F11	GP_VDD01_P		G11	VSS3_3V3		H11	VSS3_3V3		11				
12	A12	GND		B12	DP1_RX2_N		C12	GND		D12	DP2_RX1_N		E12	GND		F12	GP_VDD01_N		G12	VSS3_3V3		H12	VSS3_3V3		12				
13	A13	CP1_RX0_F	Control	B13	GND	Control	C13	IPMBS_SCL	Control	D13	GND	Control	E13	DP2_RX3_P	Control	F13	GND	Control	G13	VSS4_Next2V	Control	H13	VBAT_12V	Control	13				
14	A14	CP1_RX0_N	Expansion	B14	GND	Expansion	C14	IPMBS_SDA	Expansion	D14	GND	Expansion	E14	DP2_RX3_N	Expansion	F14	GND	Expansion	G14	3V3_AUX	Expansion	H14	VBAT_3V	Expansion	14				
15	A15	GND		B15	IPMBS_SCL		C15	GND		D15	IPMBS_RD		E15	GND		F15	GP_VDD02_P		G15	GND		H15	GND		15				
16	A16	GND		B16	IPMBS_SDA		C16	GND		D16	IPMBS_IO		E16	GND		F16	GP_VDD02_N		G16	GND		H16	NMI#		16				
17	A17	CP1_TX0_P	Control	B17	GND	Control	C17	EP_TX3_P	Control	D17	EP_TX3_N	Control	E17	REF_CLK_P	Control	F17	GND	Control	G17	UEIO_00	Control	H17	SYSRESET*	Control	17				
18	A18	CP1_TX0_N	Expansion	B18	GND	Expansion	C18	EP_TX3_N	Expansion	D18	GND	Expansion	E18	REF_CLK_N	Expansion	F18	GND	Expansion	G18	UEIO_00	Expansion	H18	GND	Expansion	18				
19	A19	GND		B19	EP_TX1_P		C19	GND		D19	EP_TX5_P		E19	GND		F19	AUX_CLK_P		G19	GND		H19	SER0+RX+		19				
20	A20	GND		B20	EP_TX1_N		C20	GND		D20	EP_TX5_N		E20	GND		F20	AUX_CLK_N		G20	UEIO_03		H20	SER0+RX-		20				
21	A21	EP_TX0_P	Expansion	B21	GND	Expansion	C21	EP_TX4_P	Expansion	D21	GND	Expansion	E21	EP_TX7_P	Expansion	F21	GND	Expansion	G21	UEIO_04	Expansion	H21	SER0+TX+	Expansion	21				
22	A22	EP_TX0_N	Expansion	B22	GND	Expansion	C22	EP_TX4_N	Expansion	D22	GND	Expansion	E22	EP_TX7_N	Expansion	F22	GND	Expansion	G22	UEIO_05	Expansion	H22	SER0+TX-	Expansion	22				
23	A23	GND		B23	EP_TX2_P		C23	GND		D23	EP_TX6_P		E23	GND		F23	USB01_D+		G23	GND		H23	GND		23				
24	A24	GND		B24	EP_TX2_N		C24	GND		D24	EP_TX6_N		E24	GND		F24	USB01_D-		G24	UEIO_06		H24	GA#		24				
25	A25	DP1_TX0_P	Data	B25	GND	Data	C25	DP1_TX3_P	Data	D25	GND	Data	E25	DP2_TX2_P	Data	F25	GND	Data	G25	UEIO_07	Data	H25	GA#	Data	25				
26	A26	DP1_TX0_N	Expansion	B26	GND	Expansion	C26	DP1_TX3_N	Expansion	D26	GND	Expansion	E26	DP2_TX2_N	Expansion	F26	GND	Expansion	G26	USB01_VBUS	Expansion	H26	GA#	Expansion	26				
27	A27	GND		B27	DP1_TX2_P		C27	GND		D27	DP2_TX1_P		E27	GND		F27	SCM1_TX+		G27	GND		H27	GA#		27				
28	A28	GND		B28	DP1_TX2_N		C28	GND		D28	DP2_TX1_N		E28	GND		F28	SCM1_TX-		G28	GDiscrete1		H28	GA#		28				
29	A29	DP1_TX1_P	Data	B29	GND	Data	C29	DP2_TX0_P	Data	D29	GND	Data	E29	DP2_TX3_P	Data	F29	GND	Data	G29	GPIO_0	Data	H29	GA#	Data	29				
30	A30	DP1_TX1_N	Expansion	B30	GND	Expansion	C30	DP2_TX0_N	Expansion	D30	GND	Expansion	E30	DP2_TX3_N	Expansion	F30	GND	Expansion	G30	GPIO_1	Expansion	H30	GND	Expansion	30				

S2 Full Aperture
RF & Optical

Figure 13.4.8.1.1-1: VNX+ 240-Pin Payload Slot Profiles

13.4.8.1.2 VNX+ 320-Pin Payload Slot Profile

The 320-pin VNX+ Payload PIC Slot Profile Template is defined by Figure 13.4.8.1.2-1. The ANSI/VITA 90.1-202x Slot Profile Template from ANSI/VITA 90.1-202x §TBD shown in Figure 13.4.8.1.2-1 is for a 320-pin Payload PICP with a Half Aperture for RF and/or optical blind-mate connections. It is intended to act as a general-purpose Payload Slot Profile with a Half Aperture for RF or optical connectivity.

VNX+ Pin Map for 320-Pin High-Speed Connector with Half Aperture																								
Col	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Col		
1	Expansion	A1	EP_RX0_P	Expansion	B1	GND	Expansion	C1	EP_RX0_P	Expansion	D1	EP_RX0_P	Expansion	E1	EP_RX0_P	Expansion	F1	VSS_12V	Expansion	G1	VSS_12V	Expansion	H1	VSS_12V
2	Expansion	A2	EP_RX0_N	Expansion	B2	GND	Expansion	C2	EP_RX0_N	Expansion	D2	GND	Expansion	E2	EP_RX0_N	Expansion	F2	GND	Expansion	G2	VSS_12V	Expansion	H2	VSS_12V
3	Expansion	A3	GND	Expansion	B3	EP_RX2_P	Expansion	C3	GND	Expansion	D3	EP_RX2_P	Expansion	E3	EP_RX2_P	Expansion	F3	SMUL_RX+	Expansion	G3	VSS_12V	Expansion	H3	VSS_12V
4	Expansion	A4	GND	Expansion	B4	EP_RX2_N	Expansion	C4	GND	Expansion	D4	EP_RX2_N	Expansion	E4	EP_RX2_N	Expansion	F4	SMUL_RX-	Expansion	G4	VSS_12V	Expansion	H4	VSS_12V
5	Expansion	A5	EP_RX1_P	Expansion	B5	GND	Expansion	C5	EP_RX4_P	Expansion	D5	GND	Expansion	E5	EP_RX1_P	Expansion	F5	GND	Expansion	G5	GND	Expansion	H5	GND
6	Expansion	A6	EP_RX1_N	Expansion	B6	GND	Expansion	C6	EP_RX4_N	Expansion	D6	GND	Expansion	E6	EP_RX1_N	Expansion	F6	GND	Expansion	G6	VSS_5V	Expansion	H6	VSS_5V
7	Expansion	A7	GND	Expansion	B7	DP1_RX1_P	Expansion	C7	GND	Expansion	D7	DP2_RX0_P	Expansion	E7	GND	Expansion	F7	DP0_DATA	Expansion	G7	VSS_5V	Expansion	H7	VSS_5V
8	Expansion	A8	GND	Expansion	B8	DP1_RX1_N	Expansion	C8	GND	Expansion	D8	DP2_RX0_N	Expansion	E8	GND	Expansion	F8	DP0_CLK	Expansion	G8	VSS_5V	Expansion	H8	VSS_5V
9	Expansion	A9	DP1_RX0_P	Expansion	B9	GND	Expansion	C9	DP1_RX3_P	Expansion	D9	GND	Expansion	E9	DP2_RX2_P	Expansion	F9	GND	Expansion	G9	VSS_5V	Expansion	H9	VSS_5V
10	Expansion	A10	DP1_RX0_N	Expansion	B10	GND	Expansion	C10	DP1_RX3_N	Expansion	D10	GND	Expansion	E10	DP2_RX2_N	Expansion	F10	GND	Expansion	G10	GND	Expansion	H10	GND
11	Expansion	A11	GND	Expansion	B11	DP1_RX2_P	Expansion	C11	GND	Expansion	D11	DP2_RX1_P	Expansion	E11	GND	Expansion	F11	GP_VB00_P	Expansion	G11	VSS_3V3	Expansion	H11	VSS_3V3
12	Expansion	A12	GND	Expansion	B12	DP1_RX2_N	Expansion	C12	GND	Expansion	D12	DP2_RX1_N	Expansion	E12	GND	Expansion	F12	GP_VB00_N	Expansion	G12	VSS_3V3	Expansion	H12	VSS_3V3
13	Expansion	A13	CP1_RX0_P	Expansion	B13	GND	Expansion	C13	PMBB_SCL	Expansion	D13	GND	Expansion	E13	DP2_RX3_P	Expansion	F13	GND	Expansion	G13	VSS4_Meg1V	Expansion	H13	VBAT_12V
14	Expansion	A14	CP1_RX0_N	Expansion	B14	GND	Expansion	C14	PMBB_SDA	Expansion	D14	GND	Expansion	E14	DP2_RX3_N	Expansion	F14	GND	Expansion	G14	3V3_AUX	Expansion	H14	VBAT_3V
15	Expansion	A15	GND	Expansion	B15	IPMBA_RX0	Expansion	C15	GND	Expansion	D15	MPWR_RD	Expansion	E15	GND	Expansion	F15	GP_VB00_P	Expansion	G15	GND	Expansion	H15	GND
16	Expansion	A16	GND	Expansion	B16	IPMBA_SDA	Expansion	C16	GND	Expansion	D16	MPWR_RD	Expansion	E16	GND	Expansion	F16	GP_VB00_N	Expansion	G16	UEIO_01	Expansion	H16	NVMIRO
17	Expansion	A17	CP1_TX0_P	Expansion	B17	GND	Expansion	C17	EP_TX3_P	Expansion	D17	GND	Expansion	E17	REF_CLK_P	Expansion	F17	GND	Expansion	G17	UEIO_00	Expansion	H17	SYRSBSET*
18	Expansion	A18	CP1_TX0_N	Expansion	B18	GND	Expansion	C18	EP_TX3_N	Expansion	D18	GND	Expansion	E18	REF_CLK_N	Expansion	F18	GND	Expansion	G18	GND	Expansion	H18	GND
19	Expansion	A19	GND	Expansion	B19	EP_TX1_P	Expansion	C19	GND	Expansion	D19	EP_TX5_P	Expansion	E19	GND	Expansion	F19	AUX_CLK_P	Expansion	G19	GND	Expansion	H19	SER01_RX+
20	Expansion	A20	GND	Expansion	B20	EP_TX1_N	Expansion	C20	GND	Expansion	D20	EP_TX5_N	Expansion	E20	GND	Expansion	F20	AUX_CLK_N	Expansion	G20	UEIO_03	Expansion	H20	SER01_RX-
21	Expansion	A21	EP_TX0_P	Expansion	B21	GND	Expansion	C21	EP_TX4_P	Expansion	D21	GND	Expansion	E21	EP_TX7_P	Expansion	F21	GND	Expansion	G21	UEIO_04	Expansion	H21	SER01_TX+
22	Expansion	A22	EP_TX0_N	Expansion	B22	GND	Expansion	C22	EP_TX4_N	Expansion	D22	GND	Expansion	E22	EP_TX7_N	Expansion	F22	GND	Expansion	G22	UEIO_05	Expansion	H22	SER01_TX-
23	Expansion	A23	GND	Expansion	B23	EP_TX2_P	Expansion	C23	GND	Expansion	D23	EP_TX6_P	Expansion	E23	GND	Expansion	F23	USB01_D+	Expansion	G23	GND	Expansion	H23	GND
24	Expansion	A24	GND	Expansion	B24	EP_TX2_N	Expansion	C24	GND	Expansion	D24	EP_TX6_N	Expansion	E24	GND	Expansion	F24	USB01_D-	Expansion	G24	UEIO_06	Expansion	H24	GA0*
25	Expansion	A25	DP1_TX0_P	Expansion	B25	GND	Expansion	C25	DP1_TX3_P	Expansion	D25	GND	Expansion	E25	DP2_TX2_P	Expansion	F25	GND	Expansion	G25	UEIO_07	Expansion	H25	GA1*
26	Expansion	A26	DP1_TX0_N	Expansion	B26	GND	Expansion	C26	DP1_TX3_N	Expansion	D26	GND	Expansion	E26	DP2_TX2_N	Expansion	F26	GND	Expansion	G26	USB01_VBUS	Expansion	H26	GA2*
27	Expansion	A27	GND	Expansion	B27	DP1_TX2_P	Expansion	C27	GND	Expansion	D27	DP2_TX1_P	Expansion	E27	GND	Expansion	F27	SMUL_TX+	Expansion	G27	GND	Expansion	H27	GA3*
28	Expansion	A28	GND	Expansion	B28	DP1_TX2_N	Expansion	C28	GND	Expansion	D28	DP2_TX1_N	Expansion	E28	GND	Expansion	F28	SMUL_TX-	Expansion	G28	GDpower1	Expansion	H28	GA4*
29	Expansion	A29	DP1_TX1_P	Expansion	B29	GND	Expansion	C29	DP2_TX0_P	Expansion	D29	GND	Expansion	E29	DP2_TX3_P	Expansion	F29	GND	Expansion	G29	GP10_0	Expansion	H29	GA5*
30	Expansion	A30	DP1_TX1_N	Expansion	B30	GND	Expansion	C30	DP2_TX0_N	Expansion	D30	GND	Expansion	E30	DP2_TX3_N	Expansion	F30	GP10_1	Expansion	G30	GND	Expansion	H30	GND
31	Expansion	A31	GND	Expansion	B31	OVERLAY	Expansion	C31	GND	Expansion	D31	OVERLAY	Expansion	E31	GND	Expansion	F31	GP_VB00_P	Expansion	G31	GND	Expansion	H31	OVERLAY
32	Expansion	A32	GND	Expansion	B32	OVERLAY	Expansion	C32	GND	Expansion	D32	OVERLAY	Expansion	E32	GND	Expansion	F32	GP_VB00_N	Expansion	G32	GND	Expansion	H32	OVERLAY
33	Expansion	A33	CP2_TX0_P	Expansion	B33	GND	Expansion	C33	OVERLAY	Expansion	D33	GND	Expansion	E33	OVERLAY	Expansion	F33	GND	Expansion	G33	OVERLAY	Expansion	H33	GND
34	Expansion	A34	CP2_TX0_N	Expansion	B34	GND	Expansion	C34	OVERLAY	Expansion	D34	GND	Expansion	E34	OVERLAY	Expansion	F34	GND	Expansion	G34	OVERLAY	Expansion	H34	GND
35	Expansion	A35	GND	Expansion	B35	OVERLAY	Expansion	C35	GND	Expansion	D35	OVERLAY	Expansion	E35	GND	Expansion	F35	OVERLAY	Expansion	G35	GND	Expansion	H35	OVERLAY
36	Expansion	A36	GND	Expansion	B36	OVERLAY	Expansion	C36	GND	Expansion	D36	OVERLAY	Expansion	E36	GND	Expansion	F36	OVERLAY	Expansion	G36	GND	Expansion	H36	OVERLAY
37	Expansion	A37	CP2_RX0_P	Expansion	B37	GND	Expansion	C37	OVERLAY	Expansion	D37	GND	Expansion	E37	OVERLAY	Expansion	F37	GND	Expansion	G37	OVERLAY	Expansion	H37	OVERLAY
38	Expansion	A38	CP2_RX0_N	Expansion	B38	GND	Expansion	C38	OVERLAY	Expansion	D38	GND	Expansion	E38	OVERLAY	Expansion	F38	GND	Expansion	G38	OVERLAY	Expansion	H38	GND
39	Expansion	A39	GND	Expansion	B39	OVERLAY	Expansion	C39	GND	Expansion	D39	OVERLAY	Expansion	E39	GND	Expansion	F39	GND	Expansion	G39	GND	Expansion	H39	OVERLAY
40	Expansion	A40	GND	Expansion	B40	OVERLAY	Expansion	C40	GND	Expansion	D40	OVERLAY	Expansion	E40	GND	Expansion	F40	GP_VB00_P	Expansion	G40	GP_VB00_N	Expansion	H40	OVERLAY

Figure 13.4.8.1.2-1: VNX+ 320-Pin Payload Slot Profiles

13.4.8.1.3 VNX+ 400-Pin Payload Slot Profiles

The 400-pin VNX+ Payload PIC Slot Profile Template is defined by Figure 13.4.8.1.3-1. The ANSI/VITA 90.1-202x Slot Profile shown in Figure 13.4.8.1.3-1 is for a 400-pin Payload Slot Profile intended to act as a general-purpose Payload Slot Profile.

VNX+ Pin Map for 400-Pin High-Speed Connector with Zero Aperture																								
Col	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Col		
1	Expansion	A1	EP_RX0_P	Expansion	B1	GND	Expansion	C1	EP_RX0_P	Expansion	D1	EP_RX0_P	Expansion	E1	EP_RX0_P	Expansion	F1	VSS_12V	Expansion	G1	VSS_12V	Expansion	H1	VSS_12V
2	Expansion	A2	EP_RX0_N	Expansion	B2	GND	Expansion	C2	EP_RX0_N	Expansion	D2	GND	Expansion	E2	EP_RX0_N	Expansion	F2	GND	Expansion	G2	VSS_12V	Expansion	H2	VSS_12V
3	Expansion	A3	GND	Expansion	B3	EP_RX2_P	Expansion	C3	GND	Expansion	D3	EP_RX2_P	Expansion	E3	EP_RX2_P	Expansion	F3	SMUL_RX+	Expansion	G3	VSS_12V	Expansion	H3	VSS_12V
4	Expansion	A4	GND	Expansion	B4	EP_RX2_N	Expansion	C4	GND	Expansion	D4	EP_RX2_N	Expansion	E4	EP_RX2_N	Expansion	F4	SMUL_RX-	Expansion	G4	VSS_12V	Expansion	H4	VSS_12V
5	Expansion	A5	EP_RX1_P	Expansion	B5	GND	Expansion	C5	EP_RX4_P	Expansion	D5	GND	Expansion	E5	EP_RX1_P	Expansion	F5	GND	Expansion	G5	GND	Expansion	H5	GND
6	Expansion	A6	EP_RX1_N	Expansion	B6	GND	Expansion	C6	EP_RX4_N	Expansion	D6	GND	Expansion	E6	EP_RX1_N	Expansion	F6	GND	Expansion	G6	VSS_5V	Expansion	H6	VSS_5V
7	Expansion	A7	GND	Expansion	B7	DP1_RX1_P	Expansion	C7	GND	Expansion	D7	DP2_RX0_P	Expansion	E7	GND	Expansion	F7	DP0_DATA	Expansion	G7	VSS_5V	Expansion	H7	VSS_5V
8	Expansion	A8	GND	Expansion	B8	DP1_RX1_N	Expansion	C8	GND	Expansion	D8	DP2_RX0_N	Expansion	E8	GND	Expansion	F8	DP0_CLK	Expansion	G8	VSS_5V	Expansion	H8	VSS_5V
9	Expansion	A9	DP1_RX0_P	Expansion	B9	GND	Expansion	C9	DP1_RX3_P	Expansion	D9	GND	Expansion	E9	DP2_RX2_P	Expansion	F9	GND	Expansion	G9	VSS_5V	Expansion	H9	VSS_5V
10	Expansion	A10	DP1_RX0_N	Expansion	B10	GND	Expansion	C10	DP1_RX3_N	Expansion	D10	GND	Expansion	E10	DP2_RX2_N	Expansion	F10	GND	Expansion	G10	GND	Expansion	H10	GND
11	Expansion	A11	GND	Expansion	B11	DP1_RX2_P	Expansion	C11	GND	Expansion	D11	DP2_RX1_P	Expansion	E11	GND	Expansion	F11	GP_VB00_P	Expansion	G11	VSS_3V3	Expansion	H11	VSS_3V3
12	Expansion	A12	GND	Expansion	B12	DP1_RX2_N	Expansion	C12	GND	Expansion	D12	DP2_RX1_N	Expansion	E12	GND	Expansion	F12	GP_VB00_N	Expansion	G12	VSS_3V3	Expansion	H12	VSS_3V3
13	Expansion	A13	CP1_RX0_P	Expansion	B13	GND	Expansion	C13	PMBB_SCL	Expansion	D13	GND	Expansion	E13	DP2_RX3_P	Expansion	F13	GND	Expansion	G13	VSS4_Meg1V	Expansion	H13	VBAT_12V
14	Expansion	A14	CP1_RX0_N	Expansion	B14	GND	Expansion	C14	PMBB_SDA	Expansion	D14	GND	Expansion	E14	DP2_RX3_N	Expansion	F14	GND	Expansion	G14	3V3_AUX	Expansion	H14	VBAT_3V
15	Expansion	A15	GND	Expansion	B15	IPMBA_SCL	Expansion	C15	GND	Expansion	D15	MPWR_RD	Expansion	E15	GND	Expansion	F15	GP_VB00_P	Expansion	G15	GND	Expansion	H15	GND
16	Expansion	A16	GND	Expansion	B16	IPMBA_SDA	Expansion	C16	GND	Expansion	D16	MPWR_RD	Expansion	E16	GND	Expansion	F16	GP_VB00_N	Expansion	G16	UEIO_00	Expansion	H16	NVMIRO
17	Expansion	A17	CP1_TX0_P	Expansion	B17	GND	Expansion	C17	EP_TX3_P	Expansion	D17	GND	Expansion	E17	REF_CLK_P	Expansion	F17	GND	Expansion	G17	UEIO_01	Expansion	H17	SYRSBSET*
18	Expansion	A18	CP1_TX0_N	Expansion	B18	GND	Expansion</																	

13.4.8.2 VNX+ Switch Slot Profiles

Two Switch Slot Profiles are defined by this document:

- One with an aperture for blind-mate connectors using the 320-pin connector
- One using the 400-pin connector without an aperture

For applications requiring the use of a network Switch Slot Profile, SOSA VNX+ PICs will reference one of the two network Switch Slot Profiles described within ANSI/VITA 90.1-202x §TBD and §TBD.

Rule 13.4.8.2-1: All rules described in ANSI/VITA 90.1-202x §TBD and §TBD apply to the SOSA VNX+ cards utilizing these Switch Slot Profiles.

13.4.8.2.1 320-Pin VNX+ DP/CP Switch Slot Profile, with Optical

The 320-pin VNX+ Switch Slot Profile is defined by Figure 13.4.8.2.1-1. The ANSI/VITA 90.1-202x Slot Profile shown in Figure 13.4.8.2.1-1 is a 320-pin Payload PICP with an empty aperture. This payload is defined as a Data Plane and Control Plane switch.

Permission 13.4.8.2.1-1: If the Data Plane and the Control Plane for a PIC use the same or compatible protocols, the switch may be implemented with either a single switch matrix or with two switch matrices.

Figure 13.4.8.2.1-1: VNX+ 320-Pin DP/CP Switch Slot Profile, with Optical

13.4.8.2.2 400-Pin VNX+ DP/CP Switch Slot Profile, no Optical

The 400-pin VNX+ Switch Slot Profile is defined by Figure 13.4.8.2.2-1. The ANSI/VITA 90.1-202x Slot Profile from ANSI/VITA 90.1-202x §TBD utilizes the pin mapping shown in Figure 13.4.8.2.2-1. This is defined as a Data Plane and Control Plane switch.

Permission 13.4.8.2.2-1: If the Data Plane and the Control Plane for a PIC use the same or compatible protocols, the switch may be implemented with either a single switch matrix or with two switch matrices.

VNX+ Pin Map for 400-Pin Data Plane / Control Plane Switch

Col	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Col		
1	b	B1	GND	b	B1	GND	b	B1	GND	b	B1	GND	b	B1	GND	b	B1	GND	b	B1	GND	b	B1	GND
2	b	B2	GND	b	B2	GND	b	B2	GND	b	B2	GND	b	B2	GND	b	B2	GND	b	B2	GND	b	B2	GND
3	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N	b	B3	CP1_RX0_N
4	b	B4	GND	b	B4	GND	b	B4	GND	b	B4	GND	b	B4	GND	b	B4	GND	b	B4	GND	b	B4	GND
5	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P	b	B5	CP2_RX0_P
6	b	B6	GND	b	B6	GND	b	B6	GND	b	B6	GND	b	B6	GND	b	B6	GND	b	B6	GND	b	B6	GND
7	b	B7	GND	b	B7	GND	b	B7	GND	b	B7	GND	b	B7	GND	b	B7	GND	b	B7	GND	b	B7	GND
8	b	B8	GND	b	B8	GND	b	B8	GND	b	B8	GND	b	B8	GND	b	B8	GND	b	B8	GND	b	B8	GND
9	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N	b	B9	DP1_RX0_N
10	b	B10	GND	b	B10	GND	b	B10	GND	b	B10	GND	b	B10	GND	b	B10	GND	b	B10	GND	b	B10	GND
11	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P	b	B11	DP2_RX0_P
12	b	B12	GND	b	B12	GND	b	B12	GND	b	B12	GND	b	B12	GND	b	B12	GND	b	B12	GND	b	B12	GND
13	b	B13	GND	b	B13	GND	b	B13	GND	b	B13	GND	b	B13	GND	b	B13	GND	b	B13	GND	b	B13	GND
14	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N	b	B14	DP1_RX1_N
15	b	B15	GND	b	B15	GND	b	B15	GND	b	B15	GND	b	B15	GND	b	B15	GND	b	B15	GND	b	B15	GND
16	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P	b	B16	DP2_RX2_P
17	b	B17	GND	b	B17	GND	b	B17	GND	b	B17	GND	b	B17	GND	b	B17	GND	b	B17	GND	b	B17	GND
18	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N	b	B18	DP1_RX2_N
19	b	B19	GND	b	B19	GND	b	B19	GND	b	B19	GND	b	B19	GND	b	B19	GND	b	B19	GND	b	B19	GND
20	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P	b	B20	DP2_RX3_P
21	b	B21	GND	b	B21	GND	b	B21	GND	b	B21	GND	b	B21	GND	b	B21	GND	b	B21	GND	b	B21	GND
22	b	B22	GND	b	B22	GND	b	B22	GND	b	B22	GND	b	B22	GND	b	B22	GND	b	B22	GND	b	B22	GND
23	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P	b	B23	DP1_RX1_P
24	b	B24	GND	b	B24	GND	b	B24	GND	b	B24	GND	b	B24	GND	b	B24	GND	b	B24	GND	b	B24	GND
25	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P	b	B25	DP2_RX1_P
26	b	B26	GND	b	B26	GND	b	B26	GND	b	B26	GND	b	B26	GND	b	B26	GND	b	B26	GND	b	B26	GND
27	b	B27	GND	b	B27	GND	b	B27	GND	b	B27	GND	b	B27	GND	b	B27	GND	b	B27	GND	b	B27	GND
28	b	B28	GND	b	B28	GND	b	B28	GND	b	B28	GND	b	B28	GND	b	B28	GND	b	B28	GND	b	B28	GND
29	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P	b	B29	DP1_TX1_P
30	b	B30	GND	b	B30	GND	b	B30	GND	b	B30	GND	b	B30	GND	b	B30	GND	b	B30	GND	b	B30	GND
31	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P	b	B31	DP2_TX0_P
32	b	B32	GND	b	B32	GND	b	B32	GND	b	B32	GND	b	B32	GND	b	B32	GND	b	B32	GND	b	B32	GND
33	b	B33	GND	b	B33	GND	b	B33	GND	b	B33	GND	b	B33	GND	b	B33	GND	b	B33	GND	b	B33	GND
34	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N	b	B34	CP1_TX0_N
35	b	B35	GND	b	B35	GND	b	B35	GND	b	B35	GND	b	B35	GND	b	B35	GND	b	B35	GND	b	B35	GND
36	b	B36	GND	b	B36	GND	b	B36	GND	b	B36	GND	b	B36	GND	b	B36	GND	b	B36	GND	b	B36	GND
37	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P	b	B37	DP1_TX0_P
38	b	B38	GND	b	B38	GND	b	B38	GND	b	B38	GND	b	B38	GND	b	B38	GND	b	B38	GND	b	B38	GND
39	b	B39	GND	b	B39	GND	b	B39	GND	b	B39	GND	b	B39	GND	b	B39	GND	b	B39	GND	b	B39	GND
40	b	B40	GND	b	B40	GND	b	B40	GND	b	B40	GND	b	B40	GND	b	B40	GND	b	B40	GND	b	B40	GND
41	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P	b	B41	DP1_TX1_P
42	b	B42	GND	b	B42	GND	b	B42	GND	b	B42	GND	b	B42	GND	b	B42	GND	b	B42	GND	b	B42	GND
43	b	B43	GND	b	B43	GND	b	B43	GND	b	B43	GND	b	B43	GND	b	B43	GND	b	B43	GND	b	B43	GND
44	b	B44	GND	b	B44	GND	b	B44	GND	b	B44	GND	b	B44	GND	b	B44	GND	b	B44	GND	b	B44	GND
45	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P	b	B45	DP1_TX2_P
46	b	B46	GND	b	B46	GND	b	B46	GND	b	B46	GND	b	B46	GND	b	B46	GND	b	B46	GND	b	B46	GND
47	b	B47	GND	b	B47	GND	b	B47	GND	b	B47	GND	b	B47	GND	b	B47	GND	b	B47	GND	b	B47	GND
48	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P	b	B48	DP1_TX3_P
49	b	B49	GND	b	B49	GND	b	B49	GND	b	B49	GND	b	B49	GND	b	B49	GND	b	B49	GND	b	B49	GND
50	b	B50	GND	b	B50	GND	b	B50	GND	b	B50	GND	b	B50	GND	b	B50	GND	b	B50	GND	b	B50	GND

Figure 13.4.8.2.2-1: VNX+ 400-Pin DP/CP Switch Slot Profile, no Optical

13.4.8.3 VNX+ Radial Clock Profiles

13.4.8.3.1 VNX+ 320-Pin Payload with Radial Clock Slot Profile

The 320-pin VNX+ Radial Clock Payload PIC Slot Profile is defined by Figure 13.4.8.3.1-1. The ANSI/VITA 90.1-202x Slot Profile shown in Figure 13.4.8.3.1-1 is a 320-pin Payload PICP with a to-be-defined aperture. This payload profile is defined as a general-purpose radial clock driver profile.

Rule 13.4.8.3.1-1: The VNX+ 320-pin Payload Radial Clock Slot Profile shall implement the rules for radial clocks as detailed in ANSI/VITA65.0 §3.5.4 and conform to the selected rules within Table 13.2.11.5-1 of this document.

320-Pin SEARAY+ Half-Aperture Connector Pin Assignments																					
Col	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name
1	Expansion	A1	EPI_R001_P	Expansion	B1	GND	Expansion	C1	EPI_R01_P	Expansion	D1	GND	Expansion	E1	EPI_R01_P	Expansion	F1	GND	Expansion	G1	V31_12V
2	Expansion	A2	EPI_R001_N	Expansion	B2	GND	Expansion	C2	EPI_R02_P	Expansion	D2	GND	Expansion	E2	EPI_R02_P	Expansion	F2	GND	Expansion	G2	V31_12V
3	Expansion	A3	GND	Expansion	B3	EPI_R02_P	Expansion	C3	GND	Expansion	D3	EPI_R03_P	Expansion	E3	GND	Expansion	F3	SGMI_RX+	Expansion	G3	V31_12V
4	Expansion	A4	GND	Expansion	B4	EPI_R02_N	Expansion	C4	GND	Expansion	D4	EPI_R03_N	Expansion	E4	GND	Expansion	F4	SGMI_RX-	Expansion	G4	V31_12V
5	Expansion	A5	EPI_R03_P	Expansion	B5	GND	Expansion	C5	EPI_R04_P	Expansion	D5	GND	Expansion	E5	EPI_R04_P	Expansion	F5	GND	Expansion	G5	GND
6	Expansion	A6	EPI_R03_N	Expansion	B6	GND	Expansion	C6	EPI_R04_N	Expansion	D6	GND	Expansion	E6	EPI_R04_N	Expansion	F6	GND	Expansion	G6	V32_5V
7	Expansion	A7	GND	Expansion	B7	DP1_R01_P	Expansion	C7	GND	Expansion	D7	DP2_R01_P	Expansion	E7	GND	Expansion	F7	I2C_PDATA	Expansion	G7	V32_5V
8	Expansion	A8	GND	Expansion	B8	DP1_R01_N	Expansion	C8	GND	Expansion	D8	DP2_R01_N	Expansion	E8	GND	Expansion	F8	I2C_CLK	Expansion	G8	V32_5V
9	Expansion	A9	DP1_R02_P	Expansion	B9	GND	Expansion	C9	DP1_R02_P	Expansion	D9	GND	Expansion	E9	DP2_R02_P	Expansion	F9	GND	Expansion	G9	V32_5V
10	Expansion	A10	GND	Expansion	B10	GND	Expansion	C10	DP1_R02_N	Expansion	D10	GND	Expansion	E10	DP2_R02_N	Expansion	F10	GND	Expansion	G10	GND
11	Expansion	A11	GND	Expansion	B11	DP1_R02_P	Expansion	C11	GND	Expansion	D11	DP2_R02_P	Expansion	E11	GND	Expansion	F11	GP_Iv3D01_P	Expansion	G11	V33_3V3
12	Expansion	A12	GND	Expansion	B12	DP1_R02_N	Expansion	C12	GND	Expansion	D12	DP2_R02_N	Expansion	E12	GND	Expansion	F12	GP_Iv3D02_P	Expansion	G12	V33_3V3
13	Expansion	A13	CP1_RX_P	Expansion	B13	GND	Expansion	C13	IPMMA_SCL	Expansion	D13	GND	Expansion	E13	DP2_R03_P	Expansion	F13	GND	Expansion	G13	V34_1V812V
14	Expansion	A14	CP1_RX_N	Expansion	B14	GND	Expansion	C14	IPMMA_SDA	Expansion	D14	GND	Expansion	E14	DP2_R03_N	Expansion	F14	GND	Expansion	G14	V34_1V812V
15	Expansion	A15	GND	Expansion	B15	IPMMA_SCL	Expansion	C15	GND	Expansion	D15	MP01_RD	Expansion	E15	GND	Expansion	F15	GP_Iv3D02_P	Expansion	G15	GND
16	Expansion	A16	GND	Expansion	B16	IPMMA_SDA	Expansion	C16	GND	Expansion	D16	MP01_TD	Expansion	E16	GND	Expansion	F16	GP_Iv3D02_P	Expansion	G16	UEIO_00
17	Expansion	A17	EPI_TX0_P	Expansion	B17	GND	Expansion	C17	EPI_TX0_P	Expansion	D17	GND	Expansion	E17	REF_CLK_P	Expansion	F17	GND	Expansion	G17	UEIO_01
18	Expansion	A18	EPI_TX0_N	Expansion	B18	GND	Expansion	C18	EPI_TX0_N	Expansion	D18	GND	Expansion	E18	REF_CLK_N	Expansion	F18	GND	Expansion	G18	UEIO_02
19	Expansion	A19	GND	Expansion	B19	EPI_TX1_P	Expansion	C19	GND	Expansion	D19	EPI_TX1_P	Expansion	E19	GND	Expansion	F19	AUX_CLK_P	Expansion	G19	GND
20	Expansion	A20	GND	Expansion	B20	EPI_TX1_N	Expansion	C20	GND	Expansion	D20	EPI_TX1_N	Expansion	E20	GND	Expansion	F20	AUX_CLK_N	Expansion	G20	UEIO_03
21	Expansion	A21	EPI_TX0_P	Expansion	B21	GND	Expansion	C21	EPI_TX0_P	Expansion	D21	GND	Expansion	E21	EPI_TX1_P	Expansion	F21	GND	Expansion	G21	UEIO_04
22	Expansion	A22	EPI_TX0_N	Expansion	B22	GND	Expansion	C22	EPI_TX0_N	Expansion	D22	GND	Expansion	E22	EPI_TX1_N	Expansion	F22	GND	Expansion	G22	UEIO_05
23	Expansion	A23	GND	Expansion	B23	EPI_TX1_P	Expansion	C23	GND	Expansion	D23	EPI_TX1_P	Expansion	E23	GND	Expansion	F23	USBD0_D+	Expansion	G23	GND
24	Expansion	A24	GND	Expansion	B24	EPI_TX1_N	Expansion	C24	GND	Expansion	D24	EPI_TX1_N	Expansion	E24	GND	Expansion	F24	USBD0_D-	Expansion	G24	UEIO_06
25	Expansion	A25	DP1_TX_P	Expansion	B25	GND	Expansion	C25	DP1_TX_P	Expansion	D25	GND	Expansion	E25	DP2_TX_P	Expansion	F25	GND	Expansion	G25	UEIO_07
26	Expansion	A26	DP1_TX_N	Expansion	B26	GND	Expansion	C26	DP1_TX_N	Expansion	D26	GND	Expansion	E26	DP2_TX_N	Expansion	F26	GND	Expansion	G26	USBD0_VBUS
27	Expansion	A27	GND	Expansion	B27	DP1_TX_P	Expansion	C27	GND	Expansion	D27	DP2_TX_P	Expansion	E27	GND	Expansion	F27	SBM1_TX+	Expansion	G27	GND
28	Expansion	A28	GND	Expansion	B28	DP1_TX_N	Expansion	C28	GND	Expansion	D28	DP2_TX_N	Expansion	E28	GND	Expansion	F28	SBM1_TX-	Expansion	G28	GBSnet1
29	Expansion	A29	DP1_TX_P	Expansion	B29	GND	Expansion	C29	DP2_TX_P	Expansion	D29	GND	Expansion	E29	DP2_TX_P	Expansion	F29	GND	Expansion	G29	GPS_0
30	Expansion	A30	DP1_TX_N	Expansion	B30	GND	Expansion	C30	DP2_TX_N	Expansion	D30	GND	Expansion	E30	DP2_TX_N	Expansion	F30	GND	Expansion	G30	GPS_0
31	Expansion	A31	GND	Expansion	B31	REFCLK01_LO	Expansion	C31	GND	Expansion	D31	REFCLK01_LO	Expansion	E31	GND	Expansion	F31	GP_Iv3D03_P	Expansion	G31	GND
32	Expansion	A32	GND	Expansion	B32	REFCLK01_L1	Expansion	C32	GND	Expansion	D32	REFCLK01_L1	Expansion	E32	GND	Expansion	F32	GP_Iv3D03_N	Expansion	G32	GND
33	Expansion	A33	CP2_TX_P	Expansion	B33	GND	Expansion	C33	REFCLK04_LO	Expansion	D33	GND	Expansion	E33	ALUCLKIN_LO	Expansion	F33	GND	Expansion	G33	ALUCLK03_LO
34	Expansion	A34	CP2_TX_N	Expansion	B34	GND	Expansion	C34	REFCLK04_L1	Expansion	D34	GND	Expansion	E34	ALUCLKIN_L1	Expansion	F34	GND	Expansion	G34	ALUCLK03_L1
35	Expansion	A35	GND	Expansion	B35	REFCLK02_LO	Expansion	C35	GND	Expansion	D35	REFCLK06_LO	Expansion	E35	GND	Expansion	F35	ALUCLK02_LO	Expansion	G35	GND
36	Expansion	A36	GND	Expansion	B36	REFCLK02_L1	Expansion	C36	GND	Expansion	D36	REFCLK06_L1	Expansion	E36	GND	Expansion	F36	ALUCLK02_L1	Expansion	G36	GND
37	Expansion	A37	CP2_RX_P	Expansion	B37	GND	Expansion	C37	REFCLKUN_LO	Expansion	D37	GND	Expansion	E37	ALUCLK01_LO	Expansion	F37	GND	Expansion	G37	ALUCLK04_LO
38	Expansion	A38	CP2_RX_N	Expansion	B38	GND	Expansion	C38	REFCLKUN_L1	Expansion	D38	GND	Expansion	E38	ALUCLK01_L1	Expansion	F38	GND	Expansion	G38	ALUCLK04_L1
39	Expansion	A39	GND	Expansion	B39	REFCLK03_LO	Expansion	C39	GND	Expansion	D39	REFCLK07_LO	Expansion	E39	GND	Expansion	F39	GP_Iv3D04_P	Expansion	G39	GND
40	Expansion	A40	GND	Expansion	B40	REFCLK03_L1	Expansion	C40	GND	Expansion	D40	REFCLK07_L1	Expansion	E40	GND	Expansion	F40	GP_Iv3D04_N	Expansion	G40	GND

S2B
Half Aperture
RF & Optical

Figure 13.4.8.3.1-1: VNX+ 320-Pin Payload with Radial Clock Slot Profile

13.4.8.3.2 VNX+ 320-Pin Radial Clock Driver Profile

The 320-pin VNX+ Radial Clock PIC Slot Profile is defined by Figure 13.4.8.3.2-1. The ANSI/VITA 90.1-202x Slot Profile shown in Figure 13.4.8.3.2-1 is a 320-pin Radial Clock PICP with a to-be-defined Half Aperture. This is a dedicated Slot Profile for driving radial clocks throughout a system.

Rule 13.4.8.3.2-1: The VNX+ 320-pin Radial Clock Slot Profile shall implement the rules for radial clocks as defined in ANSI/VITA 65.0 §3.5.4 and conform to the selected rules within Table 13.2.11.5-1 of this document.

320-Pin SEARAY + Half-Aperture Connector Pin Assignments																																								
Col	J1 ROW A 50 Pin					J1 ROW B 50 Pin					J1 ROW C 50 Pin					J1 ROW D 50 Pin					J1 ROW E 50 Pin					J1 ROW F 50 Pin					J1 ROW G 50 Pin					J1 ROW H 50 Pin				
Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name	Plane	Pin	Signal Name								
1	A1	SPARE GND 0	B1	GND	C1	REFCLK15 L0	D1	GND	E1	AUXCLK09 L0	F1	GND	G1	VSI_12V	H1	VSI_12V																								
2	A2	SPARE GND 1	B2	GND	C2	REFCLK15 L1	D2	GND	E2	AUXCLK09 L1	F2	GND	G2	VSI_12V	H2	VSI_12V																								
3	A3	GND	B3	REFCLK06 L0	C3	GND	D3	AUXCLK09 L0	E3	GND	F3	SGMR1 RX+	G3	VSI_12V	H3	VSI_12V																								
4	A4	GND	B4	REFCLK06 L1	C4	GND	D4	AUXCLK09 L1	E4	GND	F4	SGMR1 RX-	G4	VSI_12V	H4	VSI_12V																								
5	A5	REFCLK01 L0	B5	GND	C5	REFCLK16 L0	D5	GND	E5	AUXCLK10 L0	F5	GND	G5	GND	H5	GND																								
6	A6	REFCLK01 L1	B6	GND	C6	REFCLK16 L1	D6	GND	E6	AUXCLK10 L1	F6	GND	G6	VSI_3V	H6	VSI_3V																								
7	A7	GND	B7	REFCLK07 L0	C7	GND	D7	AUXCLK01 L0	E7	GND	F7	IC2001 TA	G7	VSI_3V	H7	VSI_3V																								
8	A8	GND	B8	REFCLK07 L1	C8	GND	D8	AUXCLK01 L1	E8	GND	F8	IC20 CLK	G8	VSI_3V	H8	VSI_3V																								
9	A9	REFCLK02 L0	B9	GND	C9	REFCLK17 L0	D9	GND	E9	AUXCLK11 L0	F9	GND	G9	VSI_3V	H9	VSI_3V																								
10	A10	REFCLK02 L1	B10	GND	C10	REFCLK17 L1	D10	GND	E10	AUXCLK11 L1	F10	GND	G10	GND	H10	GND																								
11	A11	GND	B11	REFCLK08 L0	C11	GND	D11	AUXCLK02 L0	E11	GND	F11	GP_VSD01 P	G11	VSI_3V3	H11	VSI_3V3																								
12	A12	GND	B12	REFCLK08 L1	C12	GND	D12	AUXCLK02 L1	E12	GND	F12	GP_VSD01 N	G12	VSI_3V3	H12	VSI_3V3																								
13	A13	CP1_RND_P	B13	GND	C13	IFMIB_SCL	D13	GND	E13	AUXCLK12 L0	F13	GND	G13	V54_Neg12V	H13	VBAT_12V																								
14	A14	CP1_RND_N	B14	GND	C14	IFMIB_SDA	D14	GND	E14	AUXCLK12 L1	F14	GND	G14	V54_ADR	H14	VBAT_3V																								
15	A15	GND	B15	IFMIB_SCL	C15	GND	D15	MIND_RD	E15	GND	F15	GP_VSD02 P	G15	GND	H15	GND																								
16	A16	GND	B16	IFMIB_SDA	C16	GND	D16	MIND_TD	E16	GND	F16	GP_VSD02 N	G16	UEIO_00	H16	RVBRIO																								
17	A17	CP1_TMD_P	B17	GND	C17	REFCLK18 L0	D17	GND	E17	REF_CLK_P	F17	GND	G17	UEIO_01	H17	SWRSET*																								
18	A18	CP1_TMD_N	B18	GND	C18	REFCLK18 L1	D18	GND	E18	REF_CLK_N	F18	GND	G18	UEIO_02	H18	OK*																								
19	A19	GND	B19	REFCLK09 L0	C19	GND	D19	AUXCLK03 L0	E19	GND	F19	AUX_CLK_P	G19	GND	H19	SRIO1_RX+																								
20	A20	GND	B20	REFCLK09 L1	C20	GND	D20	AUXCLK03 L1	E20	GND	F20	AUX_CLK_N	G20	UEIO_03	H20	SRIO1_RX-																								
21	A21	REFCLK03 L0	B21	GND	C21	REFCLK19 L0	D21	GND	E21	AUXCLK13 L0	F21	GND	G21	UEIO_04	H21	SRIO1_TPA																								
22	A22	REFCLK03 L1	B22	GND	C22	REFCLK19 L1	D22	GND	E22	AUXCLK13 L1	F22	GND	G22	UEIO_05	H22	SRIO1_TPA																								
23	A23	GND	B23	REFCLK10 L0	C23	GND	D23	AUXCLK04 L0	E23	GND	F23	USB01 D+	G23	GND	H23	GND																								
24	A24	GND	B24	REFCLK10 L1	C24	GND	D24	AUXCLK04 L1	E24	GND	F24	USB01 D-	G24	UEIO_06	H24	GND*																								
25	A25	REFCLK04 L0	B25	GND	C25	REFCLK20 L0	D25	GND	E25	AUXCLK14 L0	F25	GND	G25	UEIO_07	H25	GND*																								
26	A26	REFCLK04 L1	B26	GND	C26	REFCLK20 L1	D26	GND	E26	AUXCLK14 L1	F26	GND	G26	USB01_VBUS	H26	GND*																								
27	A27	GND	B27	REFCLK11 L0	C27	GND	D27	AUXCLK05 L0	E27	GND	F27	SGMR1_TX+	G27	GND	H27	GND*																								
28	A28	GND	B28	REFCLK11 L1	C28	GND	D28	AUXCLK05 L1	E28	GND	F28	SGMR1_TX-	G28	GDSCore1	H28	GND*																								
29	A29	REFCLK05 L0	B29	GND	C29	REFCLK21 L0	D29	GND	E29	AUXCLK15 L0	F29	GND	G29	GP_VSI_3	H29	GND*																								
30	A30	REFCLK05 L1	B30	GND	C30	REFCLK21 L1	D30	GND	E30	AUXCLK15 L1	F30	GND	G30	GP_VSI_1	H30	GND																								
31	A31	GND	B31	REFCLK12 L0	C31	GND	D31	AUXCLK06 L0	E31	GND	F31	GP_VSD03 P	G31	GND	H31	AUXCLK20 L0																								
32	A32	GND	B32	REFCLK12 L1	C32	GND	D32	AUXCLK06 L1	E32	GND	F32	GP_VSD03 N	G32	GND	H32	AUXCLK20 L1																								
33	A33	CP2_TMD_P	B33	GND	C33	REFCLK22 L0	D33	GND	E33	AUXCLK16 L0	F33	GND	G33	AUXCLK18 L1	H33	GND																								
34	A34	CP2_TMD_N	B34	GND	C34	REFCLK22 L1	D34	GND	E34	AUXCLK16 L1	F34	GND	G34	AUXCLK18 L1	H34	GND																								
35	A35	GND	B35	REFCLK13 L0	C35	GND	D35	AUXCLK07 L0	E35	GND	F35	AUXCLK17 L0	G35	GND	H35	AUXCLK21 L0																								
36	A36	GND	B36	REFCLK13 L1	C36	GND	D36	AUXCLK07 L1	E36	GND	F36	AUXCLK17 L1	G36	GND	H36	AUXCLK21 L1																								
37	A37	CP2_RND_P	B37	GND	C37	REFCLK14 L0	D37	GND	E37	AUXCLK16 L0	F37	GND	G37	AUXCLK19 L0	H37	GND																								
38	A38	CP2_RND_N	B38	GND	C38	REFCLK14 L1	D38	GND	E38	AUXCLK16 L1	F38	GND	G38	AUXCLK19 L1	H38	GND																								
39	A39	GND	B39	REFCLK14 L0	C39	GND	D39	AUXCLK08 L0	E39	GND	F39	GP_VSD04 P	G39	GND	H39	AUXCLK22 L0																								
40	A40	GND	B40	REFCLK14 L1	C40	GND	D40	AUXCLK08 L1	E40	GND	F40	GP_VSD04 N	G40	GND	H40	AUXCLK22 L1																								

S2B
Half Aperture
RF & Optical

Figure 13.4.8.3.2-1: VNX+ 320-Pin Radial Clock Slot Profile

13.4.9 Power Supply Cards (PSC) and Energy Storage Cards (ESC)

TBD

13.4.9.1 PSC Input Rules

TBD

13.4.9.2 PSC Power Outputs

TBD

13.4.9.3 PSC Output Support

TBD

13.4.9.4 PSC Utility Plane Signals

TBD

13.4.9.5 PSC SYNC Signals

TBD

13.4.10 Security Keying

TBD

13.5 SOSA Aperture and Chassis Electrical and Mechanical Interface Standard

13.5.1 Electrical Classes

The interface standard defined in this section provides testable rules and conformance testing approaches for the physical interface between the SOSA sensor and its host platform, as defined by the SV-1 in Section 4.1 (see Figure 4.1-1 and Figure 4.1-2). The SOSA sensor's physical electrical interfaces and sensor mechanical interfaces (Section 13.5.5) define the physical interface.

The standard defines several electrical classes, each class representing a suite of physical electrical connector types and signal assignments. A SOSA sensor is assigned an electrical class based on the sensor's electrical connection requirements.

The electrical connector class (Electrical Class) of a SOSA sensor defines the allowable suite of electrical interfaces (connector types and their associated signal interfaces) that can be used on SOSA sensor electrical interfaces. Currently, there are Electrical Classes 1 & 2, Class 3, and Class 5. Electrical Classes 1 & 2 are coupled, because they are coupled in SAE AS6129A.

Rule 13.5.1-1: Turreted physical package SOSA sensors shall conform to the Turret Classes requirements of SAE AS6129A (§4.1, Table 3), which are equivalent to the Turreted SOSA Electrical Classes outlined in Table 13.5.1-1. Conformance Methodology (I)

Table 13.5.1-1: Turreted SOSA Sensor Electrical Classes

Turreted SOSA Sensor Electrical Class	SAE AS6129A Turret Class
Electrical Class 1 & 2	Class I or Class II
Electrical Class 3	Class III

The scope of this document includes more than turreted physical packages, so additional connectors are included in SOSA Electrical Classes, which are not included in SAE AS6129A. Rule 13.5.1-1 prohibits the use of non-SAE AS6129A connectors for SOSA turreted physical packages. Thus, a conformant SOSA turreted physical package would also be compliant with SAE AS6129A.

It is expected that a future version of the interface standard could include additional connectors. Additional Electrical Classes could be proposed for inclusion in a future version of this document.

Observation 13.5.1-1: Some connectors could have identical definitions (shell size, pin configuration, and keying) in more than one electrical class. Only connectors defined within a particular electrical class are intended to be utilized in an individual sensor.

13.5.1.1 SOSA Input Power

Rule 13.5.1.1-1: All SOSA Class 1, 2, and 3 sensors shall use at least one of the following input power choices per Table 13.5.1.1-1. Input power for Class 5 sensors is discussed in Section 13.5.4.2.1.

Table 13.5.1.1-1: Acceptable Input Power Specifications

Nominal Input Voltage Description	Applicable Power Specification	Compliance Guidance	Typical Usage
+28Vdc	MIL-STD-704	MIL-HDBK-704-8	Aircraft
	MIL-STD-1275		Ground Vehicles
	DO-160 (§16)	DO-357	Airborne Equipment
115Vac/400Hz (3φ or 1φ) (wye)	MIL-STD-704 ("wye" only)	MIL-HDBK-704-2, -3	Aircraft
	DO-160 (§16)	DO-357	Airborne Equipment
	MIL-STD-1399/300-1		Shipboard
115Vac/400Hz (3φ or 1φ) (delta)	MIL-STD-1399/300-1		Shipboard
115Vac/60Hz (3φ or 1φ) (wye or delta)	MIL-STD-704 (1φ only)	MIL-HDBK-704-6	Aircraft
	MIL-STD-1399/300-1		Shipboard
+270Vdc	MIL-STD-704	MIL-HDBK-704-7	Aircraft
	DO-160 (§16)	DO-357	Airborne Equipment

13.5.2 SOSA Electrical Class 1 & 2 Sensor Electrical Interfaces

13.5.2.1 Class 1 & 2 Electrical Connector Characteristics

There are multiple connectors defined by this electrical standard. Table 13.5.2.1-1 describes the Class 1 & 2 connectors including sensor modalities, type, shell size, gender, keying, and inserts. Detailed requirements for each connector, defined separately for each modality of sensor, are defined in later sections.

Rule 13.5.2.1-1: The Class 1 & 2 SOSA sensor connectors shall meet the type, size, gender, and insert attributes in Table 13.5.2.1-1. Conformance Methodology (I)

Rule 13.5.2.1-2: For SOSA sensors assigned an Electrical Class 1 & 2, a J2, J14, or J15 connector shall be required. Conformance Methodology (I)

Permission 13.5.2.1-1: J2-defined signal pins may not be fully allocated to the connector depending on the mission of the SOSA sensor.

Rule 13.5.2.1-3: If the J2 connector does not fully allocate all the signal pins, then the claimant of conformance shall provide a written pin allocation of used and unused pins. Conformance Methodology (A)

Mission requirements could necessitate multiples of the same connector. For example, a mission or application of one SOSA sensor could use two J4 connectors, one J2 connector, and one J1 connector. However, there is only one J1 connector for DC power for each external sensing element. If additional power is required, then the J6 auxiliary power connector, or possibly multiple J6 connectors, in addition to the J1 connector, could be used.

Permission 13.5.2.1-2: Multiple instantiations of each J connector may be used on a SOSA sensor, except for J1 for DC power for each external sensing element.

Rule 13.5.2.1-4: No more than one J1 connector shall be used for a single external sensing element. Conformance Methodology (I)

Rule 13.5.2.1-5: Only if a J1 connector is used shall additional J6 connectors be used. Conformance Methodology (I)

Rule 13.5.2.1-6: The first instantiation of J1, J2, J3, J4, J8, J9, J10, J11, J14, or J15 shall use the keying position listed in Table 13.5.2.1-1 conforming to the key/keyway rotation position in MIL-DTL-38999M, Figure 6. Conformance Methodology (I)

Rule 13.5.2.1-7: The first instantiation of J7 shall use the keying position listed in Table 13.5.2.1-1 conforming to the key/keyway rotation position in ANSI/VITA 76.0, Rule 2.3-1 and Rule 2.3-2. Conformance Methodology (I)

Rule 13.5.2.1-8: Any additional instantiations of J6 beyond its first instantiation shall use any key/keyway rotation positions conforming to MIL-DTL-38999M, Figure 6, with the exception of position A and position N. Conformance Methodology (I)

Rule 13.5.2.1-9: Any additional instantiations of J2, J3, J4, J8, J9, J10, J11, J14, or J15 beyond their first instantiation shall use any key/keyway rotation positions conforming to MIL-DTL-38999M, Figure 6, except for position N. Conformance Methodology (I)

Rule 13.5.2.1-10: Any additional instantiations of J7 beyond its first instantiation shall use any other key/keyway rotation position conforming to ANSI/VITA 76.0, Rule 2.3-1 and Rule 2.3-2, except for position N. Conformance Methodology (I)

There are finite key positions available, as specified by the standards referenced in the rules above. When there are multiple instantiations of the same J connector, it is best practice to name them as “J#”-“key position”. For example, if there are two J3 connectors, then one could be J3-A and another J3-B. Furthermore, best practices include a description that differentiates the multiple connectors. For example, J3-A could be described as “Video cable for SWIR”, and J3-B as “Video cable for MWIR”.

Permission 13.5.2.1-3: It is not required that all of the connectors listed in Table 13.5.2.1-1 are needed depending on the mission of the SOSA sensor.

Rule 13.5.2.1-11: The claimant for conformance shall list all used SOSA connectors. If multiple instantiations of the same J connector are used, then the list shall differentiate each of the multiple connectors by key position using the nomenclature “J#”- “key position”. Conformance Methodology (A)

Rule 13.5.2.1-12: If multiple instantiations of the same J connector are used, each connector on the list shall include a brief description of the connector, indicating its difference from the others. Conformance Methodology (A)

While SOSA defined connectors are preferred, they are not required. However, interoperability can only be achieved through an open electrical interface. It is expected that non-defined SOSA cables include enough description to recreate a functional interface. Non-defined SOSA connectors cannot be considered SOSA conformant.

Rule 13.5.2.1-13: If non-defined SOSA connectors are used, the claimant for conformance shall list all connectors that are not defined in this document, as well as provide for each an associated pin assignment including the modality, connection description, pin number, wire type, signal name, and signal type, as well as the pin arrangement. Conformance Methodology (A)

Table 13.5.2.1-1: Class 1 & 2 Sensor Connectors

Designator	Purpose	Modality Support	Type	Shell Size	Sensor LRU Gender	Platform Umbilical Gender	Keying	Insert
J1	DC Power	All	MIL-DTL-38999/Series III	21	Receptacle with pin inserts	Plug with socket inserts	N	21-11
J2	Signal	All	MIL-DTL-38999/Series III	25	Receptacle with socket inserts	Plug with pin inserts	N	25-7
J3	Video (Copper)	EO-IR, Communications	MIL-DTL-38999/Series III	21	Receptacle with socket inserts	Plug with pin inserts	C	21-11
J4	Fiber Optic	All	MIL-DTL-38999/Series III	19	Receptacle with socket inserts for fiber optics	Plug with pin inserts for fiber optics	N	19-11
J5	GPS Antenna	All	MIL-PRF-39012	TNC	Receptacle	Plug	—	—
J6	Aux DC Power	All	MIL-DTL-38999/Series III	21	Receptacle with pin inserts	Plug with socket inserts	A	21-11
J7	High Speed (Copper)	All	ANSI/VITA 76.0	17	Receptacle with pin inserts	Plug with socket inserts	N	
J8	High Density RF	Comms., EW, Radar/SAR, SIGINT	MIL-DTL-38999/Series III	25	Receptacle with socket inserts	Plug with pin inserts	N	25-19
J9	Low Loss RF	Comms., EW, Radar/SAR, SIGINT	MIL-DTL-38999/Series III	25	Receptacle with socket inserts	Plug with pin inserts	N	25-8
J10	AC Power	Comms., EW, Radar/SAR, SIGINT	MIL-DTL-38999/Series III	17	Receptacle with pin inserts	Plug with socket inserts	N	17-6
J11	High Voltage DC	All	MIL-DTL-38999/Series III	15	Receptacle with pin inserts	Plug with socket inserts	N	15-5
J12	Key Fill – Non-GPS	All	MIL-DTL-55116	N/A	NSA P/N 0N241775	NSA P/N 0N241774	N/A	N/A
J13	Key Fill – GPS	All	MIL-DTL-55116	N/A	NSA P/N 0N241775	NSA P/N 0N241774	N/A	N/A

Designator	Purpose	Modality Support	Type	Shell Size	Sensor LRU Gender	Platform Umbilical Gender	Keying	Insert
J14	High Density Fiber	All		15	Receptacle with 4 optical MT with physical contacts for 96 optic fibers	Plug with socket inserts	N	N/A
J15	High Density Fiber	All	VITA 87.0	11	Receptacle with 1 optical MT with physical contacts for 24 optic fibers	Plug with socket inserts	N	—
J16	External Battery	All	MIL-DTL-38999/Series III	9	Receptacle with pin inserts	Plug with socket inserts	N	9-35
J17X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	TNC	Receptacle	Plug		
J18X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	SMA	Receptacle	Plug		
J19X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	2.4mm	Receptacle	Plug		
J20X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	1.0mm	Receptacle	Plug		

13.5.2.2 Class 1 & 2 Sensor J1-DC Power Connector

Rule 13.5.2.2-1: The sensor system’s J1-DCPower Connector shall have a 21-11 insert pattern as shown in Figure 13.5.2.2-1. Conformance Methodology (I)

Rule 13.5.2.2-2: When the J1 Power Connector is used, the pins shall be assigned in accordance with Table 13.5.2.2-1. Conformance Methodology (I)

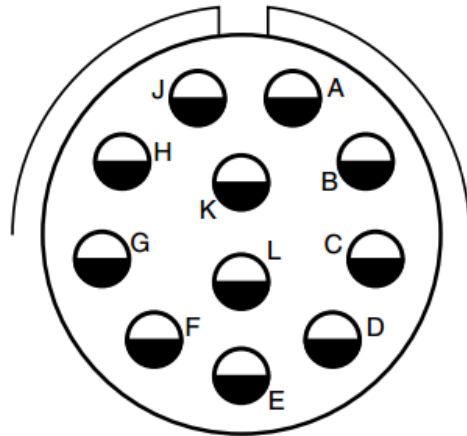


Figure 13.5.2.2-1: J1-DCPower Connector Pin Arrangement

Table 13.5.2.2-1: J1-DC Power Connector Pin Allocation

J1-DC Power (21-11 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**G11PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*G11SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
+28VDC	D	SC-AWG12	DC-1	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	E	SC-AWG12	DC-1 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
+28VDC	F	SC-AWG12	DC-2	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	L	SC-AWG12	DC-2 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
+28VDC	C	SC-AWG12	DC-3	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	G	SC-AWG12	DC-3 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
Safety Ground	K	SC-AWG12	Chassis	Platform	Ground	✓	✓	✓	✓	✓
+28VDC	A	SC-AWG12	DC-4	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	J	SC-AWG12	DC-4 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
+28VDC	B	SC-AWG12	DC-5	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	H	SC-AWG12	DC-5 RTN	Platform	DC RTN	✓	✓	✓	✓	✓

13.5.2.2.1 Power

Rule 13.5.2.2.1-1: Where +28 Voltage Direct Current (VDC) input power is used, the vendor shall select one or more of the applicable standards per Table 13.5.1.1-1, to define input power characteristics for the sensor system’s J1-DC Power Connector (Table 13.5.2.2-1). Conformance Methodology (I)

Rule 13.5.2.2.1-2: The sensor system’s J1-DC Power connector shall accept +28 VDC power on any combination of the ‘+28VDC/RTN’ pin pairs listed in Table 13.5.2.2-1. Conformance Methodology (I)

Rule 13.5.2.2.1-3: Where a J1 Power Connector pair is used, the allowable inrush limit shall be specified by the procuring activity. Conformance Methodology (I)

Observation 13.5.2.2.1-1: The ‘+28VDC/RTN’ pair inrush limit could be accomplished by the platform.

Observation 13.5.2.2.1-2: Where more than 15A (nominal) current of +28VDC power is required to the sensor, the J1-DC Power connector’s +28 VDC and RTN pairs (as identified in Table 13.5.2.2-1) could be connected in parallel, up to a maximum of 5 pairs.

Rule 13.5.2.2.1-4: Where more than 15A (nominal) current of +28VDC power is required to the sensor, the J1-DC Power connector's +28 VDC and RTN pairs (as identified in Table 13.5.2.2-1) shall be connected in parallel, up to a maximum of 5 pairs. Conformance Methodology (I)

Rule 13.5.2.2.1-5: The nominal current input to any '+28VDC/RTN' pair shall not exceed 15A per Table 13.5.2.2-1. Conformance Methodology (A)

Observation 13.5.2.2.1-3: Where more than 500W of input power is needed, utilization of a higher input voltage is recommended.

Rule 13.5.2.2.1-6: The sensor chassis shall exhibit $\geq 1M\Omega$ isolation to any J1 connector power returns. Conformance Methodology (I)

13.5.2.2.2 Safety Ground

Rule 13.5.2.2.2-1: The J1-DC Power connector Safety Ground shall connect between the SOSA sensor safety ground contact and the chassis with a resistance of $\leq 0.1 \Omega$, in accordance with MIL-STD-1310H §3.20. Conformance Methodology (I)

13.5.2.3 Class 1 & 2 Sensor J2-Signal Connector

Rule 13.5.2.3-1: The sensor system J2-Signal Connector shall have a 25-7 insert pattern as shown in Figure 13.5.2.3-1. Conformance Methodology (I)

Rule 13.5.2.3-2: When the J2 Signal Connector is used, the sensor system shall assign signals to the connector's pins as in Table 13.5.2.3-1. Conformance Methodology (I)

Observation 13.5.2.3-1: When commercial protocols are routed through connector J2, pin out and nomenclature in this document are based upon the commercial standard but could vary slightly as required to maintain signal and ground paths and preserve signal integrity.

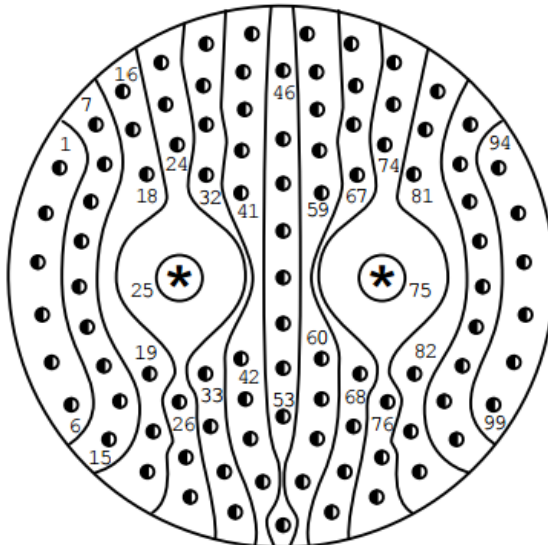


Figure 13.5.2.3-1: J2-Signal Connector Pin Arrangement

Table 13.5.2.3-1: J2-Signal Connector Pin Allocation

SOSA Electrical Interface J2-Signal (25-7 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**J7SN (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J7PN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Power Enable Discrete	46	STP 2419	PWR_EN	Platform	Open/Closed Circuit	✓	✓	✓	✓	✓
	47	STP 2419	PWR_EN_RTN	Platform	Open/Closed Circuit					
Ethernet	28	100Ω STP – AWG 24, CAT 6A SAE AS6070/6 Recommended ¹	DA+	Platform/ Sensor	1000BaseT	✓	✓	✓	✓	✓
	35		DA-							
	36		DA Shield							
	44		DB+							
	53		DB-							
	62		DB Shield							
	45		DC+							
	54		DC-							
	63		DC Shield							
	70		DD+							
	71		DD-							
78	DD Shield									
Serial Comms 1	7	100 Ohm STP 2419	TX1+	Sensor	TIA 422	✓	✓	✓	✓	✓
	8	100 Ohm STP 2419	TX1-	Sensor						
	17	SC-AWG24	422_1_RTN							
	16	100 Ohm STP 2419	RX1+	Platform						
	23	100 Ohm STP 2419	RX1-	Platform						
Serial Comms 2	22	100 Ohm STP 2419	TX2+	Sensor	TIA 422	✓	✓	✓	✓	✓

SOSA Electrical Interface J2-Signal (25-7 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**J7SN (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J7PN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	30	100 Ohm STP 2419	TX2-	Sensor						
	29	SC-AWG24	422_2_RTN							
	37	100 Ohm STP 2419	RX2+	Platform						
	38	100 Ohm STP 2419	RX2-	Platform						
Serial Comms 3	55	100 Ohm STP 2419	TX3+	Sensor	TIA 422	✓	✓	✓	✓	✓
	56	100 Ohm STP 2419	TX3-	Sensor						
	64	SC-AWG24	422_3_RTN							
	65	100 Ohm STP 2419	RX3+	Platform						
	72	100 Ohm STP 2419	RX3-	Platform						
Serial Comms 4	73	100 Ohm STP 2419	TX4+	Sensor	TIA 422	✓	✓	✓	✓	✓
	79	100 Ohm STP 2419	TX4-	Sensor						
	80	SC-AWG24	422_4_RTN							
	85	100 Ohm STP 2419	RX4+	Platform						
	86	100 Ohm STP 2419	RX4-	Platform						
Emi- ssions Arming	2	AWG22	MASTER_AR M	Platform	open/closed circuit	✓	✓			
	95	AWG22	MASTER_AR M_RET	Platform	open/closed circuit return					
NEZ Cutout	4	AWG24	NEZ_SELECT _BIT 0	Platform	open/closed circuit	✓	✓			
	5	AWG24	NEZ_SELECT _BIT 1	Platform	open/closed circuit					

SOSA Electrical Interface J2-Signal (25-7 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**J7SN (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J7PN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	11	AWG24	NEZ_SELECT _PARITY	Platform	open/closed circuit					
	12	AWG24	NEZ_SELECT _RTN	Platform	open/closed circuit return					
Emissions Mode Select	89	AWG24	MODE_SELEC T_BIT 0	Platform	open/closed circuit	✓	✓			
	90	AWG24	MODE_SELEC T_BIT 1	Platform	open/closed circuit					
	97	AWG24	MODE_SELEC T_PARITY	Platform	open/closed circuit					
	98	AWG24	MODE_SELEC T_RTN	Platform	open/closed circuit return					
Emission Annun- ciation	20	100 Ohm STP 2419	LF+	Sensor	Isolated 28V Logic	✓	✓			
	21		LF-	Sensor	Isolated 28V Logic					
Safety Status (Dis- cretes)	15	100 Ohm STP 2419	SS1+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	19		SS1-	Sensor	Isolated 28V Logic					
	42	100 Ohm STP 2419	SS2+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	60		SS2-	Sensor	Isolated 28V Logic					
	82	100 Ohm STP 2419	SS3+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	93		SS3-	Sensor	Isolated 28V Logic					
Enable Gimbal Move- ment	51	AWG22	ENBL_GIMB	Platform	open/closed circuit	✓	✓			
	52	AWG22	ENBL_GIMB_ RTN	Platform	open/closed circuit					
Time Sync 1	48	100 Ohm STP 2419	1 PPS	Platform	10 V logic	✓	✓	✓	✓	✓

SOSA Electrical Interface J2-Signal (25-7 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**J7SN (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J7PN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
PPS	49	100 Ohm STP 2419	1 PPS RTN	Platform	10 V logic					
Reserved	81									
	91									
HC Power	68	AWG22	HAND_CONT_PWR	Sensor	28VDC@500ma	✓				
	69	AWG22	H_C_PWR_RT N	Sensor	DC Return					
Memory Purge	76	AWG24	PURG_MEM	Platform	Differential 5 V logic	✓	✓	✓	✓	✓
	77	AWG24	PURG_MEM_RT N	Platform	Differential 5 V logic					
	61	Shield	PURG_MEM_SHD	Platform	Shield					
MIL-STD-1553B Twinax inserts M39029 /90-529 (pin) M39029 /91-530 (socket)	25-1	77 Ohm Twin-Ax	TX/RX A+	Platform/Sensor/Backshell	MIL-STD-1553B	✓	✓	✓	✓	✓
	25-2		TX/RX A-							
	25-S		A-Shield							
	75-1	77 Ohm Twin-Ax	TX/RX B+	Platform/Sensor/Backshell	MIL-STD-1553B	✓	✓	✓	✓	✓
	75-2		TX/RX B-							
	75-S		B-Shield							
USB 2.0 Data	6	STP 2419	USB_DATA+	Platform/Sensor	USB Data	✓	✓	✓	✓	✓
	13	STP 2419	USB_DATA-	Platform/Sensor	USB Data					
	14	Shield	GND	Platform/Sensor	USB Data Shield					
USB 2.0 Power	33	STP 2419	USB_PWR_+5 V	Sensor	USB Power	✓	✓	✓	✓	✓
	34	STP 2419	USB_PWR_RT N	Sensor	USB Power					

SOSA Electrical Interface J2-Signal (25-7 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**J7SN (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J7PN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	43	Shield	GND	Sensor	USB Power Shield					
LVDS1	26	100 Ohm STP 2419	LVDS1+				✓	✓	✓	✓
	27		LVDS1-							
LVDS2	18	100 Ohm STP 2419	LVDS2+				✓	✓	✓	✓
	41		LVDS2-							
LVDS3	50	100 Ohm STP 2419	LVDS3+				✓	✓	✓	✓
	59		LVDS3-							
LVDS4	83	100 Ohm STP 2419	LVDS4+				✓	✓	✓	✓
	84		LVDS4-							
LVDS5	92	100 Ohm STP 2419	LVDS5+				✓	✓	✓	✓
	99		LVDS5-							
Sensor Manu- facturer	24,31, 32,39, 40,57, 58,66, 67,74	AWG24	SENMAN_1 to SENMAN_10	Sensor		✓	✓	✓	✓	✓
Res- erved	1,3,9, 10,87, 88,94, 96		For arming isolation							

Observation 13.5.2.3-2: Each J2-Signal connector signal group in Table 13.5.2.3-1 can be described in more detail below. By convention of this document, individual signal sets can have their own return line. This is done for Electromagnetic Compatibility/Electromagnetic Interference (EMC/EMI) performance, as well as ease of platform integration.

Rule 13.5.2.3-3: When an isolated +28Vdc discrete signal of amplitude $\geq 18.0\text{VDC}$ is received by the J2-Signal connector, the signal shall be interpreted as a logic level '1'. Conformance Methodology (T)

Rule 13.5.2.3-4: When an isolated +28Vdc discrete signal of amplitude $\leq 1.5\text{VDC}$ is received by the J2-Signal connector, the signal shall be interpreted as a logic level '0'. Conformance Methodology (T)

Observation 13.5.2.3-3: Some acquisition programs could allow higher voltage levels to also be interpreted as logic '0'. A typical impetus for this would be the result of a system safety analysis.

Observation 13.5.2.3-4: The J2-Signal connector wire type 2419 in Table 13.5.2.3-1 refers to a wire with an AWG 24 silver-plated conductor with 19 strands.

13.5.2.3.1 Power Enable

The Power Enable signal is used for a controlled power up and shutdown of the sensor system. This control is necessary if the sensor system is required to execute a sequence of steps upon shutdown, steps that the sensor system would be precluded from executing if power were simply removed from the system. The Power Enable signal is controlled by the platform and, when disabled, instructs the sensor to power down.

Power Enable is a switch, relay, or Solid-State Relay (SSR) controlled by the platform (or human on the platform side of the interface). The switch goes across PWR_EN and PWR_EN_RTN. The sensor provides the voltage for this. Power Enable is disabled if an open circuit exists externally between the contacts (i.e., the switch is open). Power Enable is enabled if a closed circuit is externally applied between the contacts.

Rule 13.5.2.3.1-1: When the J2-Signal connector Power Enable circuit has a resistance value $\geq 100\text{k } \Omega$, the sensor system shall enter the power OFF condition. Conformance Methodology (I)

Rule 13.5.2.3.1-2: When the J2-Signal connector Power Enable circuit has a resistance value $\leq 5\Omega$, the sensor system shall enter the power ON condition. Conformance Methodology (I)

Rule 13.5.2.3.1-3: The J2-Signal connector Power Enable signal shall source a maximum current of 100mA. Conformance Methodology (I)

Rule 13.5.2.3.1-4: The J2-Signal connector Power Enable signal shall drive a maximum voltage of 30 VDC. Conformance Methodology (I)

13.5.2.3.2 Ethernet (Copper)

Rule 13.5.2.3.2-1: The J2 connector's Ethernet signals shall implement Gigabit Ethernet. Conformance Methodology (I)

Gigabit Ethernet is an 8-wire (4 twisted-pair), 100 Ω connection.

Rule 13.5.2.3.2-2: The J2-Signal connector Gigabit Ethernet shall comply with IEEE 802.3-2008 (a 1000BaseT channel) using CAT 6A AS6070/6 cable or equivalent. Conformance Methodology (I)

13.5.2.3.3 Serial Communications

Up to four application-configurable serial communication ports are defined.

Rule 13.5.2.3.3-1: The J2-Signal connector serial ports shall conform to TIA/EIA-422-B. Conformance Methodology (I)

Observation 13.5.2.3.3-1: Each serial communications port includes a return connection for ease of platform integration. The sensor system supplier can determine the need for this return line and implement it taking into consideration best practices regarding EMC/EMI.

13.5.2.3.4 Arming, Cutouts, and Mode Selects

A set of ten pins is dedicated to control of energy emitting sensors such as the arming of laser devices, or RF transmission devices. This includes the selection of predefined emission suppression zone maps for turreted sensors.

Rule 13.5.2.3.4-1: The J2-Signal connector shall source a maximum current of 100 mA on the Arming signals. Conformance Methodology (A)

Rule 13.5.2.3.4-2: The J2-Signal connector shall source a maximum current of 100 mA on the Cutout signals. Conformance Methodology (A)

Rule 13.5.2.3.4-3: The J2-Signal connector shall source a maximum current of 100 mA on Emission Mode signals. Conformance Methodology (A)

Rule 13.5.2.3.4-4: The J2-Signal connector shall drive a maximum voltage of 30VDC on the Arming signals. Conformance Methodology (A)

Rule 13.5.2.3.4-5: The J2-Signal connector shall drive a maximum voltage of 30 VDC on the Cutout signals. Conformance Methodology (A)

Rule 13.5.2.3.4-6: The J2-Signal connector shall drive a maximum voltage of 30 VDC on Emission Mode signals. Conformance Methodology (A)

13.5.2.3.4.1 MASTER_ARM

To arm an emission device, the platform closes the switch which completes the circuit. The current which goes through it, and the voltage across it, come from the sensor system. These pins form part of the power circuit for an emission device in the sensor. When the pins are open, power to the device is disabled; when close-circuited, power is enabled. The pins allow the integrator to connect a simple arming switch to these contacts.

Rule 13.5.2.3.4.1-1: The J2-Signal connector shall use pins 2 and 95 for Emissions Arming. Conformance Methodology (I)

13.5.2.3.4.2 No Emit Zone (NEZ) Cutout

The sensor systems can have a No Emit Zone NEZ or Cutout Map. The NEZ is a two-dimensional map, in azimuth and elevation that defines where the device can and cannot emit. It is designed to inhibit emissions when the system Line-of-Sight (LOS) is over any part of the platform. This prevents energy from reflecting, posing a hazard. The map is stored in the sensor memory. A sensor could have several maps stored, enabling it to be mounted at several points on the platform, or on several platform models, without modification. The NEZ is a high-reliability mechanism to select which map to be used.

There are three (NEZ) circuits. Each is a switch, relay, or SSR provided by, and independently controlled by, the platform. The three circuits have a common return, NEZ_SELECT_RTN.

Rule 13.5.2.3.4.2-1: The J2-Signal connector shall use pins 4, 5, 11, and 12 for NEZ map selection. Conformance Methodology (I)

If three of the four pins allocated to this function are used to select a map, up to four maps can be defined in the turret. The fourth pin would be used as a parity check for safety.

13.5.2.3.5 Emissions Mode Select

Rule 13.5.2.3.5-1: The J2-Signal connector shall use pins 89, 90, 97, and 98 for Emissions Mode Select. Conformance Methodology (I)

Note: If three of the four pins allocated to this function are used to select a mode, up to four modes can be defined in the sensor. The fourth pin would be used as a parity check for safety.

13.5.2.3.6 Emissions Annunciation

Rule 13.5.2.3.6-1: The J2-Signal connector shall use emissions signals to annunciate firing of an emission device. Conformance Methodology (I)

Rule 13.5.2.3.6-2: The J2-Signal connector Emission signal shall be an isolated 28 VDC signal. Conformance Methodology (I)

Rule 13.5.2.3.6-3: The J2-Signal connector Emission signal shall provide 30 VDC max voltage and 100mA max current. Conformance Methodology (I)

13.5.2.3.7 Safety Status

A set of three signal pairs are available to indicate the status of safety-relevant functions in the sensor system.

Rule 13.5.2.3.7-1: The J2-Signal connector Safety Status signal shall be an isolated 28 VDC signal. Conformance Methodology (I)

Rule 13.5.2.3.7-2: The J2-Signal connector Safety Status signal shall provide 30 VDC max voltage and 100mA max current. Conformance Methodology (I)

13.5.2.3.8 Enable Gimbal Movement

This control is necessary to ensure that the sensor does not move in azimuth and/or elevation at high speeds endangering individuals that could be working near the sensor. The Enable Gimbal Movement signal originates from the sensor with the platform opening and closing the circuit.

13.5.2.3.9 Time Synchronization – 1 PPS

Rule 13.5.2.3.9-1: When provided by the platform, the J2 connector shall accept the input time roll-over pulse (1 PPS) signal which is in accordance with ICD-GPS-060B. See also Figure 13.5.2.3.9-1. Conformance Methodology (I)

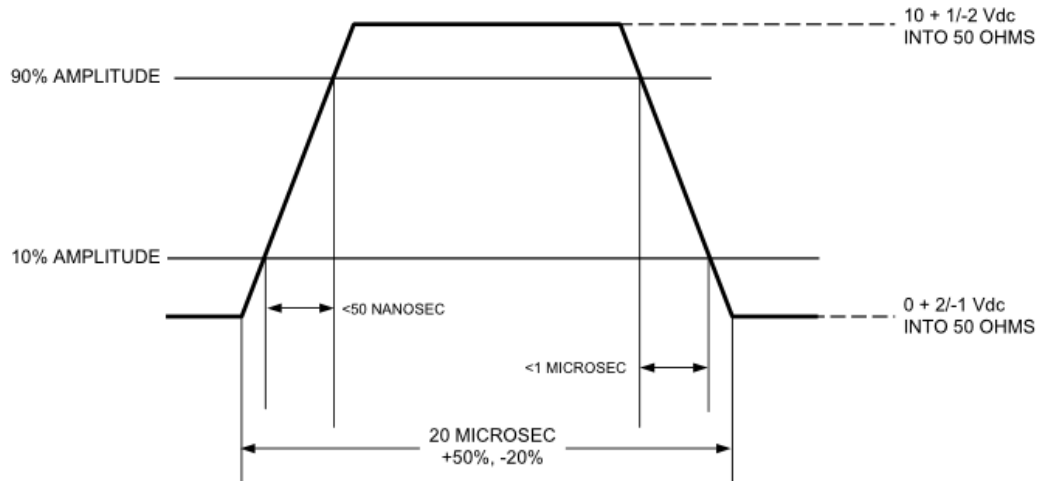


Figure 13.5.2.3.9-1: Input Time Rollover Pulse (1 PPS) Signal Characteristics

13.5.2.3.10 Unused

13.5.2.3.11 Hand Controller Power

Rule 13.5.2.3.11-1: Where a hand controller is required, the J2 Signal connector shall provide power with a maximum of 30 VDC and 500mA. Conformance Methodology (I)

13.5.2.3.12 Memory Purge

This signal is to be used for the erasure of system data. Usage of this interface is implementation-specific and could be used to clear any memory that could be sensitive.

Rule 13.5.2.3.12-1: The J2 Signal connector shall provide PURG_MEM and PURG_MEM_RTN pins, for connectivity to an external switch closure in the platform, to command erasure of memory in the sensor. Note that a switch closure refers to any means to connect the PURG_MEM and PURG_MEM_RTN pins. Conformance Methodology (I)

Rule 13.5.2.3.12-2: The temporal length of the J2-Signal connector switch closure for memory erase shall be 30ms. Conformance Methodology (I)

13.5.2.3.13 MIL-STD 1553B Twinax Inserts

Observation 13.5.2.3.13-1: A set of two Size 8 Twin axial contacts could be available for MIL-STD-1553B. Pin 25 is intended for Bus A and pin 75 for Bus B.

13.5.2.3.14 USB Data

Permission 13.5.2.3.14-1: The sensor system may optionally provide a USB 2.0 Host interface.

13.5.2.3.15 USB Power

Rule 13.5.2.3.15-1: When a USB 2.0 Host interface is required, the J2 Signal connector shall supply power at 5V @+/-5% and up to 500mA. Conformance Methodology (I, T)

13.5.2.3.16 Low Voltage Differential Signal (LVDS)

Observation 13.5.2.3.16-1: The LVDS discrete signals are available to the sensor manufacturers for use between sensor elements.

13.5.2.3.17 Sensor Manufacturer Pins

A set of 10 pins are reserved for use by individual sensor system suppliers, primarily for maintenance purposes when the sensor is not connected to the platform.

13.5.2.4 Class 1 & 2 Sensor J3-Video (Copper) Connector

Rule 13.5.2.4-1: The J3 Video connector shall have a 21-11 pin arrangement shown in Figure 13.5.2.4-1. Conformance Methodology (I)

Rule 13.5.2.4-2: The J3 Video connector shall be in accordance with Table 13.5.2.4-1. Conformance Methodology (I)

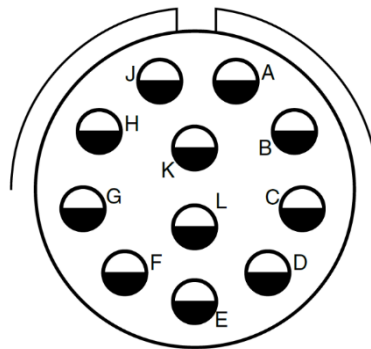


Figure 13.5.2.4-1: J3-Video Connector Pin Arrangement

Table 13.5.2.4-1: J3-Video Connector Pin Allocation

J3-Video (21-11 insert, C-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted. Sensor: MIL-DTL-38999/**G11PC-LC/M39029/75-416 (receptacle with coax socket inserts) Platform Umbilical: MIL-DTL-38999/26*G11PC-LC/M39029/28-211 (plug with coax pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Communications	
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used	Notes
A	Coax-75Ω	Digital Video Ch1	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor
B	Coax-75Ω	Digital Video Ch2	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor

J3-Video (21-11 insert, C-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted. Sensor: MIL-DTL-38999/**G11PC-LC/M39029/75-416 (receptacle with coax socket inserts) Platform Umbilical: MIL-DTL-38999/26*G11PC-LC/M39029/28-211 (plug with coax pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Communications	
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used	Notes
C	Coax-75Ω	Digital Video Ch3	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor
D	Coax-75Ω	Digital Video Ch4	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor
E	Coax-75Ω	Digital Video Ch5	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor
F	Coax-75Ω	Digital Video Ch6	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For input from EO/IR sensor
G	Coax-75Ω	Composite Video Ch 1	Sensor	RS-170a Composite Video	✓				✓	For input from EO/IR sensor
H	Coax-75Ω	Composite Video Ch 2	Sensor	RS-170a Composite Video	✓				✓	For input from EO/IR sensor
J	Coax-75Ω	Analog video Ch3 Y	Sensor	RS-170a Video Luminance	✓				✓	For input from EO/IR sensor
K	Coax-75Ω	Analog video Ch3 C	Sensor	RS-170a Video Chrominance	✓				✓	For input from EO/IR sensor
L	Unused									

Rule 13.5.2.4-3: The sensor system digital channels shall comply with the SMPTE ST 292, SMPTE ST 424, SMPTE ST 2081, or SMPTE ST 2082 standard, driving into 75 Ω #12 coax contacts. Conformance Methodology (T)

Rule 13.5.2.4-4: The J3 Video connector digital signal pins shall drive 75 Ω size 12 contacts. Conformance Methodology (T)

Rule 13.5.2.4-5: The J3 Video connector’s analog channels shall comply with the RS-170a standard. Conformance Methodology (A)

Rule 13.5.2.4-6: The J3 Video connector analog signals shall drive 75 Ω size 12 contacts. Conformance Methodology (A)

13.5.2.5 *Class 1 & 2 Sensor J4-Fiber Optics Connector*

Rule 13.5.2.5-1: The J4 Fiber Optic connector shall have a 19-11 pin arrangement in Figure 13.5.2.5-1. Conformance Methodology (I)

Rule 13.5.2.5-2: The J4 Fiber Optic connector shall be in accordance with Table 13.5.2.5-1. Conformance Methodology (I)

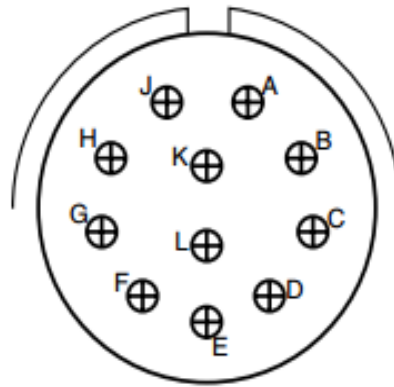


Figure 13.5.2.5-1: J4-Fiber Optics Connector Pin Arrangement

Table 13.5.2.5-1: J4-Fiber Optics Connector Pin Allocation

SOSA Electrical Interface J4-Fiber (19-11 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and fiber contacts inserted Sensor MIL-DTL-38999/**F11SN-LC/29504/5 (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F11PN-LC/29504/4 (plug with pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
A	MM Fiber	Sensor Transmit 1	Sensor	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
B	MM Fiber	Sensor Receive 1	Platform	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓

SOSA Electrical Interface J4-Fiber (19-11 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and fiber contacts inserted Sensor MIL-DTL-38999/**F11SN-LC/29504/5 (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F11PN-LC/29504/4 (plug with pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
C	MM Fiber	Sensor Transmit 2	Sensor	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
D	MM Fiber	Sensor Receive 2	Platform	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
E	MM Fiber	Sensor Transmit 3	Sensor	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
F	MM Fiber	Sensor Receive 3	Platform	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
G	MM Fiber	Sensor Transmit 4	Sensor	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
H	MM Fiber	Sensor Receive 4	Platform	10GBase-SR/ 25GBASE-SR 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
J	MM Fiber	Video Ch 1	Sensor	SMPTE ST 297	✓				
K	MM Fiber	Video Ch 2	Sensor	SMPTE ST 297	✓				
L	MM Fiber	Video Ch 3	Sensor	SMPTE ST 297	✓				

Rule 13.5.2.5-3: The J4 Fiber Optic connector shall transmit and receive at 850nm per IEEE 802.3-2008. This is for applications at 10GBASE-SR, 25GBASE-SR, 40GBASE-SR, and 100GBASE-SR. Conformance Methodology (I)

Rule 13.5.2.5-4: The sensor system SMPTE ST 297 Channels shall transmit low power SMPTE ST 292, SMPTE ST 424, SMPTE ST 2081, or SMPTE ST 2082 signals at 1310nm specifically according to call out L-PC-CD-1310. Conformance Methodology (I)

Rule 13.5.2.5-5: Fiber optic shall be multi-mode fiber. The core diameter shall be $50\mu\text{m} \pm 3\mu\text{m}$ and the cladding diameter shall be $125\mu\text{m} \pm 2\mu\text{m}$. Conformance Methodology (I)

Rule 13.5.2.5-6: The sensor system MM Fiber termini shall be MIL-PRF-29504/4 (Pin) or MIL-PRF-29504/5 (Socket) which fit into size 16 entry holes. Conformance Methodology (I)

Rule 13.5.2.5-7: The sensor system MM Fiber shall be per ARINC 802-3 aramid reinforced 1.8 mm fiber optic cable. Conformance Methodology (I)

Rule 13.5.2.5-8: The J4 Fiber Optic connector shall baseline OM3 optical fiber as defined in ISO/IEC 11801. Conformance Methodology (I)

Rule 13.5.2.5-9: Fiber Optic 1.8 mm simplex cabling reinforced with aramid strength member shall be per ARINC 802-3. Fiber core size and bandwidth shall be matched for optimum performance. Conformance Methodology (I, A)

13.5.2.6 *Class 1 & 2 Sensor J5-GPS Antenna Connector*

Rule 13.5.2.6-1: Where a GPS receiver internal to the sensor system is used and requires an external antenna, the J5 GPS Antenna connector shall be used. Conformance Methodology (I)

Rule 13.5.2.6-2: The J5 GPS Antenna connector shall use GPS signals that conform to SAE AS6129 §A.6 (Sensor Requirements). Conformance Methodology (I)

Rule 13.5.2.6-3: The J5 GPS Antenna connector shall use MIL-STD-188-148B TNC connectors. Conformance Methodology (I)

Table 13.5.2.6-1: J5-GPS Connector Pin Allocation

SOSA Electrical Interface Recommendations					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
J5-GPS Ant (TNC)									
Sensor – Receptacle					Used	Used	Used	Used	Used
Platform Umbilical – Plug									
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Coaxial	Coax-50Ω	GPS Antenna	Platform	RF	✓	✓	✓	✓	✓

13.5.2.7 *Class 1 & 2 Sensor J6-DC Auxiliary Power Connector*

Rule 13.5.2.7-1: When additional 28VDC power is required, the J6 DC Auxiliary Power connector shall accept it (in accordance with MIL-STD-704F) to at pins listed in Table 13.5.2.7-1. Conformance Methodology (I)

Rule 13.5.2.7-2: The J6 DC Auxiliary Power connector shall have a 21-11 insert pattern shown in Figure 13.5.2.7-1. Conformance Methodology (I)

Rule 13.5.2.7-3: The J6 DC Auxiliary Power connector signals shall be assigned to pins in accordance with Table 13.5.2.7-1. Conformance Methodology (I)

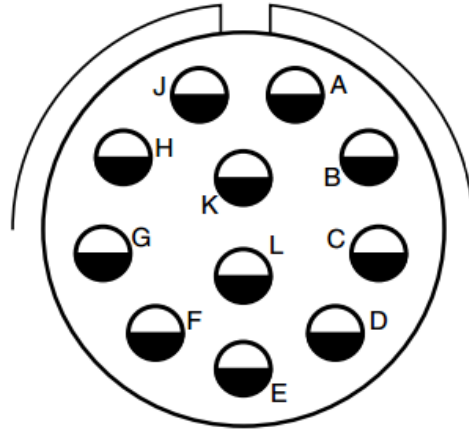


Figure 13.5.2.7-1. J6-DC Auxiliary Power Connector Pin Arrangement

Table 13.5.2.7-1: J6-DC Auxiliary Power Connector

SOSA Electrical Interface						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
J6 Aux Power (21-11 insert, A-Keying)										
For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish										
Sensor MIL-DTL-38999/**G11PA (receptacle with pin inserts)										
Platform Umbilical MIL-DTL-38999/26*G11SA (plug with sockets inserts)										
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
28VDC	D	SC-AWG12	DC-6	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	E	SC-AWG12	DC-6 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
28VDC	F	SC-AWG12	DC-7	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	L	SC-AWG12	DC-7 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
28VDC	C	SC-AWG12	DC-8	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	G	SC-AWG12	DC-8 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
Safety Ground	K	SC-AWG12	Chassis	Platform	Ground	✓	✓	✓	✓	✓
28VDC	A	SC-AWG12	DC-9	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	J	SC-AWG12	DC-9 RTN	Platform	DC RTN	✓	✓	✓	✓	✓
28VDC	B	SC-AWG12	DC-10	Platform	28V DC@15A	✓	✓	✓	✓	✓
Return	H	SC-AWG12	DC-10 RTN	Platform	DC RTN	✓	✓	✓	✓	✓

13.5.2.7.1 Power

Rule 13.5.2.7.1-1: Where +28 VDC input power is required from J6, the vendor shall select the same standard as for J1, to define input power characteristics for the sensor system's J6-DC Power Connector (+28Vdc Power Selections). Conformance Methodology (I)

Rule 13.5.2.7.1-2: The sensor system's J6-DC Power connector shall accept +28 VDC power on any combination of the '+28VDC/RTN' pin pairs listed in Table 13.5.2.7-1. Conformance Methodology (I)

Recommendation 13.5.2.7.1-1: The '+28VDC/RTN' pin pairs included in the J1 connector should be utilized prior to those in J6. When J6 is used, the '+28VDC/RTN' pin pairs should start with the lowest numbered pair, continuing in increasing order. Conformance Methodology (I)

Rule 13.5.2.7.1-3: Where a J6 Power Connector pair is used, the allowable inrush current at each '+28VDC/RTN' pair shall be specified by the procuring activity. Conformance Methodology (I)

Rule 13.5.2.7.1-4: The nominal current input to any '+28VDC/RTN' pair shall not exceed 15A per Table 13.5.2.7-1. Conformance Methodology (A, T)

Observation 13.5.2.7.1-1: The '+28VDC/RTN' pair inrush limit could be accomplished by the platform.

Observation 13.5.2.7.1-2: Where more than 15A (nominal) current of +28VDC power is required to the sensor, the J6-DC Power connector's +28 VDC and RTN pairs (as identified in Table 13.5.2.7-1) could be connected in parallel, up to a maximum of 5 pairs.

Observation 13.5.2.7.1-3: The '+28VDC/RTN' pair inrush limit could be accomplished by the platform.

Rule 13.5.2.7.1-5: Reserved.

Rule 13.5.2.7.1-6: The sensor chassis shall exhibit $\geq 1M\Omega$ isolation to any J6 connector power returns. Conformance Methodology (I)

13.5.2.7.2 Safety Ground

Rule 13.5.2.7.2-1: The J6-DC Power connector Safety Ground shall connect between the SOSA sensor safety ground contact and the chassis with a resistance of $\leq 0.1 \Omega$ in accordance with MIL-STD-1310 §3.20. Conformance Methodology (I)

13.5.2.8 Class 1 & 2 Sensor J7-High Speed Connector

The J7-High Speed Connector supports electrical interfaces such as 10Gig Ethernet, USB 3.0 G1, USB 3.0 G2, SATA Gen 3.0, and DisplayPort 1.3.

Observation 13.5.2.8-1: When commercial protocols are routed through connector J7, pin out and nomenclature in this document are based upon the commercial standard, but could vary slightly as required to maintain signal and ground paths and preserve signal integrity.

Rule 13.5.2.8-1: The J7 High Speed Electrical connector shall have the pin arrangement in Figure 13.5.2.8-1. Conformance Methodology (I)

Rule 13.5.2.8-2: The J7 High Speed Electrical connector shall assign pins in accordance with Table 13.5.2.8-1. Conformance Methodology (I)

**Size17 Mapping:
Pigtail Plug common grounds**

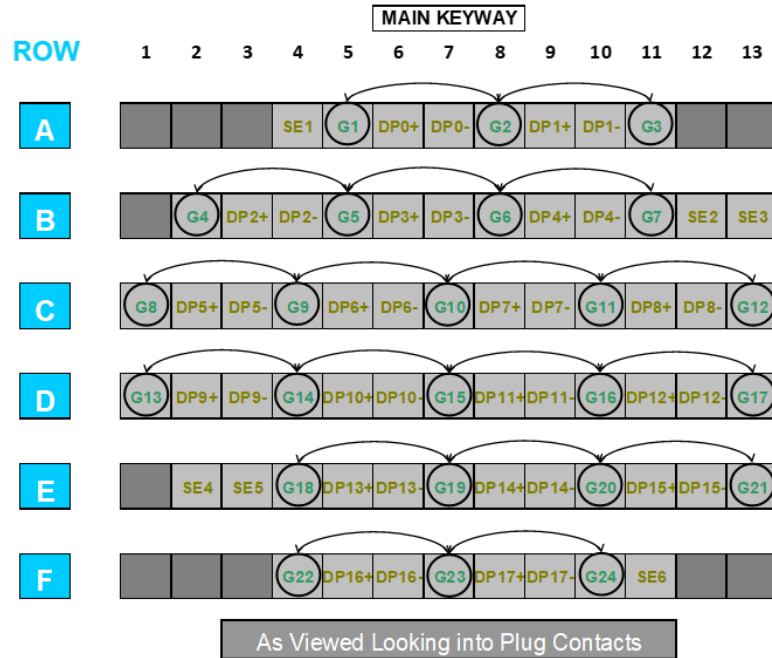


Figure 13.5.2.8-1: J7-High Speed Electrical Connector Pin Arrangement

Table 13.5.2.8-1: J7-High Speed Electrical Pin Allocations

SOSA Electrical Interface J7-High Speed Electrical (ANSI/VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
10Gig Ethernet	B3	100Ω STP – AWG 24, CAT 6A SAE AS6070/6	DA+	Platform/Sensor	10GBaseT	✓	✓	✓	✓	✓
	B4		DA-							
	B5		DA Shield							
	C2		DB+							

SOSA Electrical Interface										
J7-High Speed Electrical (ANSI/VITA 76.0 #17 shell, N-keying)										
Sensor: 985217*N**** Receptacle, Size 17, N keying										
Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length										
Platform Umbilical: 985017*N**** Plug, Size 17, N keying										
Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length or contact for specific options										
Fields noted (*) are implementer's discretion										
The Shell Plating on the Receptacle and the Plug shall be the same plating						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
The requirements of v76.0 are met by a Meritec part number or equivalent										
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	C3		DB-							
	C4		DB Shield							
	C5		DC+							
	C6		DC-							
	C7		DC Shield							
	C8		DD+							
	C9		DD-							
	C10		DD Shield							
USB 3.0/2.0	E8	100 Ohm STP 2419	USB_SS TX+	Sensor	USB 3.X Tx DATA	✓	✓	✓	✓	✓
	E9		USB_SS TX-							
	E7	SC-AWG24	USB GND DRAIN							
	E5	100 Ohm STP 2419	USBSS_RX+	Platform	USB 3.X Rx DATA					
	E6		USB_SS_RX-							
	F9	100 Ohm STP 2419	USB_D-	Sensor/ Platform	USB 2.X Data	✓	✓	✓	✓	✓
	F8		USB_D+							
	F11	AWG24	USB_PWR	Sensor	USB Power	✓	✓	✓	✓	✓
	F10	AWG24	USB_GND							
E10	AWG24	USB_SHLD		Shield	✓	✓	✓	✓	✓	
Display Port	E2	AWG24	+3.3V	Sensor	Display Port	✓	✓	✓	✓	✓
	E4	AWG24	+3.3V_RTN							
	E11	100 Ohm	AUX+							

SOSA Electrical Interface										
J7-High Speed Electrical (ANSI/VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms	
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	E12	STP 2419	AUX-							
	C11	AWG24	CONFIG1							
	C12	AWG24	CONFIG2							
	E13	SHIELD	GND							
	E3	AWG24	HOTPLUG							
	D3	100 Ohm STP 2419	LANE0-							
	D4		LANE0_SHIELD							
	D2		LANE0+							
	D6	100 Ohm STP 2419	LANE1-							
	D7		LANE1_SHIELD							
	D5		LANE1+							
	D9	100 Ohm STP 2419	LANE2-							
	D10		LANE2_SHIELD							
	D8		LANE2+							
	D12	100 Ohm STP 2419	LANE3-							
	D13		LANE3_SHIELD							
	D11		LANE3+							
SATA	A5	100Ω STP 2419	DA Shield		SATA	✓	✓	✓	✓	✓
	A6		A+	Sensor						
	A7		A-							
	A8	Shield	Shield							
	A9	100Ω STP	B+	Platform						

SOSA Electrical Interface J7-High Speed Electrical (ANSI/VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms	
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used	
	A10	2419	B-								
	A11		DB Shield								
Serial	F5	100Ω STP 2419	Serial_TX	Sensor	TIA 232	✓	✓	✓	✓	✓	
	F7		Serial_RTN								
	F6		Serial_RX	Platform							
Write Enable	B12	AWG24	WR_EN	Sensor	Switch Closure	✓	✓	✓	✓	✓	
	B13	AWG24	WR_EN_RTN								
Digital Ground	B2 B8 B11 C1 C13 D1 F4					✓	✓	✓	✓	✓	
Spare SE	A4										
Spare DP	B6 B7										
Spare DP	B9 B10										

13.5.2.8.1 10G Ethernet (Copper)

Rule 13.5.2.8.1-1: The J7 High Speed Electrical connector shall implement an Ethernet interface per IEEE 802.3an-2006 for 10GBase-T. Conformance Methodology (I)

13.5.2.8.2 USB 3.1/2.0

Rule 13.5.2.8.2-1: The J7 High Speed Electrical connector shall implement a USB interface per USB 3.1 G2. Conformance Methodology (I)

Rule 13.5.2.8.2-2: The J7 High Speed Electrical Interface shall be backwards-compatible with USB 2.0. Conformance Methodology (I)

13.5.2.8.3 Display Port

Rule 13.5.2.8.3-1: The J7 High Speed Electrical connector shall implement DisplayPort 1.3. Conformance Methodology (I)

13.5.2.8.4 SATA

Rule 13.5.2.8.4-1: The J7 High Speed Electrical connector shall implement a SATA interface per SATA Gen 3.0. Conformance Methodology (I)

13.5.2.8.5 Serial Communications

Rule 13.5.2.8.5-1: The J7 High Speed Electrical connector serial port shall conform to TIA 232. Conformance Methodology (I)

13.5.2.8.6 Write Enable

Observation 13.5.2.8.6-1: Write Enable is available for use as a maintenance function where it is desired to limit writing to non-volatile memory only during system maintenance periods.

Rule 13.5.2.8.6-1: When writing to non-volatile memory, the J7 High Speed Electrical connector shall implement an external switch to close WR_EN and WR_EN_RTN together. Conformance Methodology (I)

Rule 13.5.2.8.6-2: The J7 High Speed Electrical connector shall enable write when the WR_EN and WR-EN_RTN circuit is closed. Conformance Methodology (I)

13.5.2.9 Class 1 & 2 Sensor J8-High Density RF Connector

Rule 13.5.2.9-1: Where required, the sensor system shall utilize a high-density RF connection between sensor elements as defined in Table 13.5.2.9-1. Conformance Methodology (I)

Rule 13.5.2.9-2: The J8 RF connector shall have a 25-19 insert pattern shown in Figure 13.5.2.9-1. Conformance Methodology (I)

Rule 13.5.2.9-3: The J8 RF connector shall assign pins in accordance with Table 13.5.2.9-1. Conformance Methodology (A)

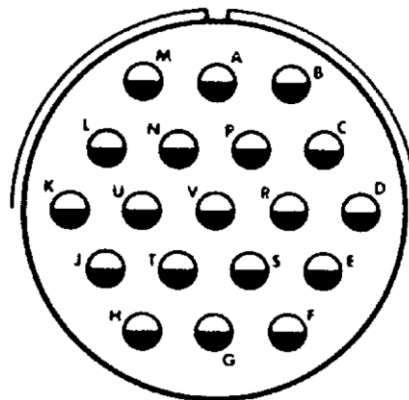


Figure 13.5.2.9-1: J8 RF Connector Pin Arrangement

Table 13.5.2.9-1: J8 RF Pin Allocations

SOSA Electrical Interface J8-RF (25-19 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted per description below Sensor MIL-DTL-38999/20*J19SN-LC (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*J19PN-LC (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
RF	A	Coax-50Ω	Ch1	Antenna	RF up to 50GHz		✓	✓	✓	✓
	B	Coax-50Ω	Ch2	Antenna	RF up to 50GHz		✓	✓	✓	✓
	C	Coax-50Ω	Ch3	Antenna	RF up to 50GHz		✓	✓	✓	✓
	D	Coax-50Ω	Ch4	Antenna	RF up to 50GHz		✓	✓	✓	✓
	E	Coax-50Ω	Ch5	Antenna	RF up to 50GHz		✓	✓	✓	✓
	F	Coax-50Ω	Ch6	Antenna	RF up to 50GHz		✓	✓	✓	✓
	G	Coax-50Ω	Ch7	Antenna	RF up to 50GHz		✓	✓	✓	✓
	H	Coax-50Ω	Ch8	Antenna	RF up to 50GHz		✓	✓	✓	✓
	J	Coax-50Ω	Ch9	Antenna	RF up to 50GHz		✓	✓	✓	✓
	K	Coax-50Ω	Ch10	Antenna	RF up to 50GHz		✓	✓	✓	✓
	L	Coax-50Ω	Ch11	Antenna	RF up to 50GHz		✓	✓	✓	✓
	M	Coax-50Ω	Ch12	Antenna	RF up to 50GHz		✓	✓	✓	✓
	N	Coax-50Ω	Ch13	Antenna	RF up to 50GHz		✓	✓	✓	✓
	P	Coax-50Ω	Ch14	Antenna	RF up to 50GHz		✓	✓	✓	✓
	R	Coax-50Ω	Ch15	Antenna	RF up to 50GHz		✓	✓	✓	✓
	S	Coax-50Ω	Ch16	Antenna	RF up to 50GHz		✓	✓	✓	✓
	T	Coax-50Ω	Ch17	Antenna	RF up to 50GHz		✓	✓	✓	✓
	U	Coax-50Ω	Ch18	Antenna	RF up to 50GHz		✓	✓	✓	✓
	V	Coax-50Ω	Ch19	Antenna	RF up to 50GHz		✓	✓	✓	✓

Rule 13.5.2.9-4: The J8 RF connector shall use a MIL-DTL-38999 size 12 socket per SAE AS39029/56 with a SMPM pin interface. Conformance Methodology (I)

Rule 13.5.2.9-5: The J8 RF connector SMPM pin interface dimensions shall conform to MIL-STD-348B (w/Change 3), in Figure 13.5.2.9-2. Conformance Methodology (I)

Rule 13.5.2.9-6: When the J8 RF connector's SMPM socket interface is present, the socket's interface shall conform to MIL-STD-348B, Figure 313-2 (w/Change 3), in Figure 13.5.2.9-2. Conformance Methodology (I)

Rule 13.5.2.9-7: The J8 RF connector receptacle SMPM pin and socket interface shall conform to MIL-STD-348B, Figure 313-2 (w/Change 3), in Figure 13.5.2.9-2. Conformance Methodology (I)

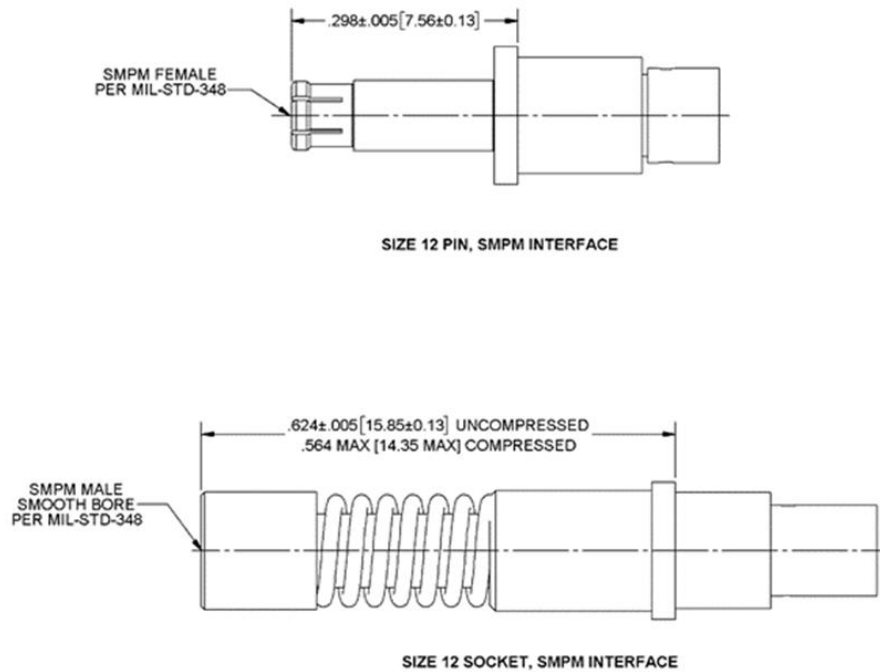


Figure 13.5.2.9-2: Size 12 Pin and Socket

13.5.2.10 *High Density RF Performance Testing*

Rule 13.5.2.10-1: The J8 RF connector size 12 contact mated pairs shall meet or exceed the Voltage Standing Wave Ratio (VSWR) requirements per Table 13.5.2.10-1. Conformance Methodology (I)

Table 13.5.2.10-1: VSWR and Frequency Range

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
DC-18 GHz	1.25:1
18-26.5 GHz	1.30:1
26.5-40 GHz	1.40:1

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
40-50 GHz	1.60:1

13.5.2.11 Class 1 & 2 Sensor J9-Low Loss RF Connector

Rule 13.5.2.11-1: When a low loss RF connection is required, the J9 Low Loss RF Connector shall use values defined in Table 13.5.2.11-1. Conformance Methodology (I)

Rule 13.5.2.11-2: The J9 Low Loss RF Connector shall use a 25-8 insert pattern shown in Figure 13.5.2.11-1. Conformance Methodology (I)

Rule 13.5.2.11-3: The J9 Low Loss RF Connector shall assign pins in accordance with Table 13.5.2.11-1. Conformance Methodology (I)

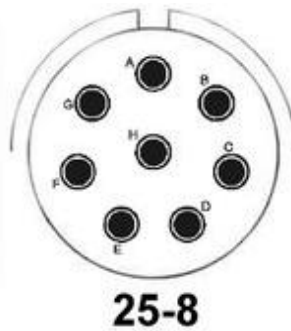


Figure 13.5.2.11-1: J9 RF Connector Pin Arrangement

Table 13.5.2.11-1: J9 RF Pin Allocation

SOSA Electrical Interface Recommendations										
J9-RF (25-8 insert, N-Keying)										
For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish										
Connectors are ordered without contacts and coax contacts inserted per description below										
Antenna MIL-DTL-38999/**J19SN-LC (receptacle with socket inserts)										
Platform Umbilical MIL-DTL-38999/26*J19PN-LC (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
RF	A	Coax-50Ω	Ch1	Antenna	RF up to 22GHz		✓	✓	✓	✓
	B	Coax-50Ω	Ch2	Antenna	RF up to 22GHz		✓	✓	✓	✓
	C	Coax-50Ω	Ch3	Antenna	RF up to 22GHz		✓	✓	✓	✓
	D	Coax-50Ω	Ch4	Antenna	RF up to 22GHz		✓	✓	✓	✓
	E	Coax-50Ω	Ch5	Antenna	RF up to 22GHz		✓	✓	✓	✓

SOSA Electrical Interface Recommendations										
J9-RF (25-8 insert, N-Keying)										
For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish										
Connectors are ordered without contacts and coax contacts inserted per description below										
Antenna MIL-DTL-38999/**J19SN-LC (receptacle with socket inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Platform Umbilical MIL-DTL-38999/26*J19PN-LC (plug with pin inserts)										
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	F	Coax-50Ω	Ch6	Antenna	RF up to 22GHz		✓	✓	✓	✓
	G	Coax-50Ω	Ch7	Antenna	RF up to 22GHz		✓	✓	✓	✓
	H	Coax-50Ω	Ch8	Antenna	RF up to 22GHz		✓	✓	✓	✓

Rule 13.5.2.11-4: The J9 Low Loss RF Connector shall utilize a MIL-DTL-38999 size 8 socket per SAE AS39029/59 with a BMB pin interface. Conformance Methodology (I)

Rule 13.5.2.11-5: The J9 Low Loss RF Connector Blind Mate Bullet (BMB) pin dimensions (in Figure 13.5.2.11-2) shall conform to MIL-STD-348B (w/Change 3). Conformance Methodology (I)

Rule 13.5.2.11-6: The J9 Low Loss RF Connector BMB socket pin dimensions (in Figure 13.5.2.11-2) shall conform to MIL-STD-348B (w/Change 3). Conformance Methodology (I)

Rule 13.5.2.11-7: The J9 Low Loss RF Connector BMB pin and socket interface shall conform to Figure 13.5.2.11-2. Conformance Methodology (I)

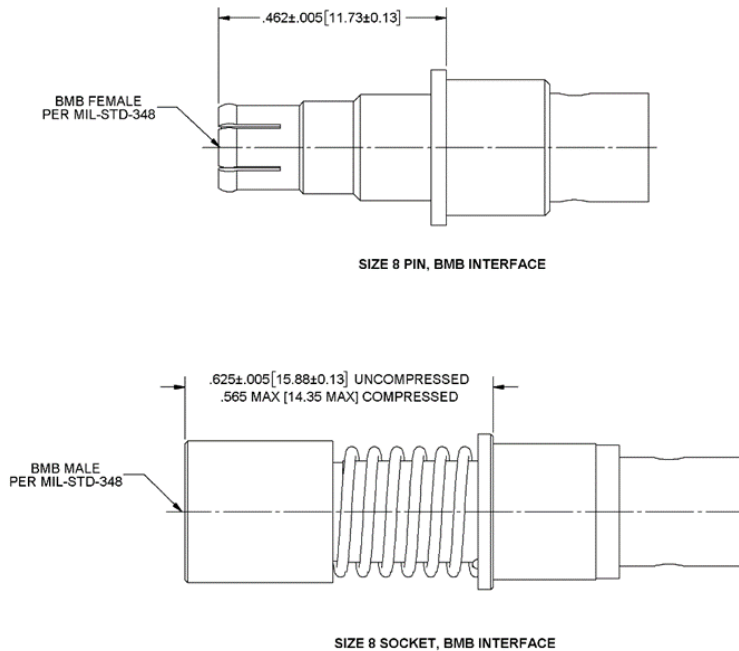


Figure 13.5.2.11-2: Size 8 Pin and Socket

13.5.2.11.1 Low Loss RF Performance Testing

Rule 13.5.2.11.1-1: The J9 Low Loss RF Connector mated pairs shall meet VSWR requirements in Table 13.5.2.11.1-1. Conformance Methodology (I)

Table 13.5.2.11.1-1: Size 8 Connector VSWR Requirements

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
DC-22 GHz	1.40:1

13.5.2.12 Class 1 & 2 Sensor Auxiliary RF Connectors

Rule 13.5.2.12-1: When high-frequency discrete signals are required, the Auxiliary RF Connector shall use pin assignments in Table 13.5.2.12-1. Conformance Methodology (I)

Table 13.5.2.12-1: Auxiliary RF Connections

Auxiliary RF Connectors – Quantity is Application-Specific						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
TNC		RG142 50Ω		Antenna	RF up to 3 GHz	✓	✓	✓	✓	✓
SMA		RG174 50Ω		Antenna	RF up to 27 GHz		✓	✓	✓	✓
2.4 mm		Coax-50Ω		Antenna	RF up to 50 GHz		✓	✓	✓	✓
1.0 mm		Coax-50Ω		Antenna	RF up to 110 GHz		✓	✓	✓	✓

13.5.2.13 Class 1 & 2 Sensor J10-AC Power Connector

Rule 13.5.2.13-1: The J10 AC Power Connector shall use a 17-6 insert pattern shown in Figure 13.5.2.13-1. Conformance Methodology (I)

Rule 13.5.2.13-2: The J10 AC Power Connector shall assign pins in accordance with Table 13.5.2.13-1. Conformance Methodology (I)

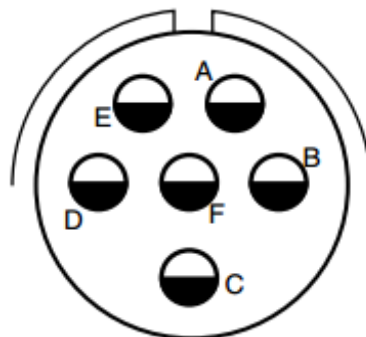


Figure 13.5.2.13-1: J10-AC Power Connector Pin Arrangement

Table 13.5.2.13-1: J10-AC Power Pin Allocations

SOSA Electrical Interface J10-AC Power (17-6 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999 contacts M39029/58-365 (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*E6SN contacts M39029/56-353 (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
3φ 400Hz AC Power (wye)	A	12AWG	115/200VAC Phase A	Platform	AC Power		✓	✓	✓	✓
	B	12AWG	115/200VAC Phase B	Platform	AC Power		✓	✓	✓	✓
	C	12AWG	115/200VAC Phase C	Platform	AC Power		✓	✓	✓	✓
	D	12AWG	115/200VAC Neutral	Platform	AC Power		✓	✓	✓	✓
	E		Unused							
	F	12AWG	Chassis	Platform	Ground		✓	✓	✓	✓

13.5.2.13.1 AC Power Description

Rule 13.5.2.13.1-1: Where utilized, the J10 AC Power Connector shall accept 115/200 V_{RMS} power at the pins listed in Table 13.5.2.13-1. Conformance Methodology (I)

Rule 13.5.2.13.1-2: When the J10-AC Power Connector is used, the vendor procuring activity shall select one or more of the applicable standards per Table 13.5.1.1-1 to define input power characteristics. Conformance Methodology (I)

Rule 13.5.2.13.1-3: The nominal current input to any AC phase shall not exceed 10A. Conformance Methodology (A, T, I)

Rule 13.5.2.13.1-4: Where a J10 Power Connector pair is used, the allowable inrush current shall be specified by the procuring activity. Conformance Methodology (I)

Recommendation 13.5.2.13.1-1: When an over-current condition occurs on any phase of the 3φ, 115/200 V RMS AC power at the J10 AC Power Connector, all three phases should then be interrupted. Conformance Methodology (I)

Recommendation 13.5.2.13.1-2: Where a delta configuration for AC input voltage is required, a unique connector and pin configuration should be used. Conformance Methodology (I)

Recommendation 13.5.2.13.1-3: Where 60 Hz AC input voltage is required, a unique connector and pin configuration should be used. Conformance Methodology (I)

13.5.2.14 Class 1 & 2 Sensor J11 – High Voltage DC Power Connector

Rule 13.5.2.14-1: Where required, the sensor system J11 High Voltage DC Power Connector shall have a 15-5 insert pattern as shown in Figure 13.5.2.14-1. Conformance Methodology (I)

Rule 13.5.2.14-2: Signals for the J11 High Voltage DC Connector shall be assigned to pins in accordance with Table 13.5.2.14-1. Conformance Methodology (I)

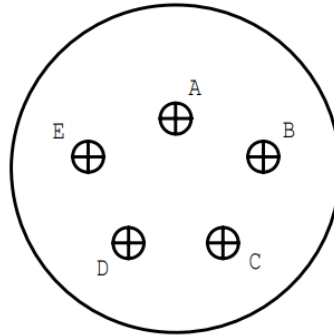


Figure 13.5.2.14-1: J11 High Voltage DC Connector Pin Arrangement

Table 13.5.2.14-1: J11 High Voltage DC Power Pin Allocations

SOSA Electrical Interface J11 High Voltage DC Power (15-5 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**D5PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*D5SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
270VDC	A	SC-AWG16	HVDC-1	Platform	270VDC@10A	✓	✓	✓	✓	✓
	B	SC-AWG16	HVDC-1_RTN	Platform	270VDC RTN	✓	✓	✓	✓	✓
Safety Ground	C	SC-AWG16	Chassis Ground	Common	Ground	✓	✓	✓	✓	✓
Reserved	D,E		Reserved		Safety Interlock	✓	✓	✓	✓	✓

13.5.2.14.1 Power

Rule 13.5.2.14.1-1: Where utilized, the sensor system shall accept 270 VDC power in accordance with one or more of the applicable standards per Table 13.5.1.1-1, at the pins listed in Table 13.5.2.14-1. Conformance Methodology (I)

Rule 13.5.2.14.1-2: Where a J11 High Voltage DC connector is used, the allowable inrush current shall be specified by the procuring activity. Conformance Methodology (T)

Rule 13.5.2.14.1-3: The sensor shall isolate power returns from the chassis. Conformance Methodology (I)

13.5.2.14.2 Safety Ground

Rule 13.5.2.14.2-1: The sensor system ground contact shall be used to provide electrical continuity to the sensor system chassis in accordance with MIL-STD-1310H §3.20. Conformance Methodology (I)

13.5.2.14.3 Connectivity Materials and Wire Type

Recommendation 13.5.2.14.3-1: When enabling 270 VDC, power systems should incorporate polyimide-free SAE AS22759/70/75 wire types to prevent arc track events and potential fires caused by dielectric breakdown or damage. Conformance Methodology (I)

Recommendation 13.5.2.14.3-2: When considering connector contacts and wire compatibility, the design authority should evaluate wire size and environmental conditions to suppress corona. Conformance Methodology (A)

13.5.2.15 Class 1 & 2 Sensor J12 – Key Fill Connector, Non-GPS Devices

Rule 13.5.2.15-1: Where a DS-101 Interface is used to distribute security keys or similar data to non-GPS elements in the sensor, using a bussed key fill service, the sensor component shall employ a J12 chassis-mounted Key Fill Connector (NSA P/N 0N241775 or equivalent) in accordance with EKMS 308 as shown in Figure 13.5.2.15-1. Conformance Methodology (I)

Rule 13.5.2.15-2: When the J12 Key Fill Connector is used, the shell of the J12 connector shall make electrical contact with the sensor system chassis for grounding in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

Rule 13.5.2.15-3: The J12 Key Fill Connector signals shall be assigned to pins in accordance with Table 13.5.2.15-1. Conformance Methodology (I)

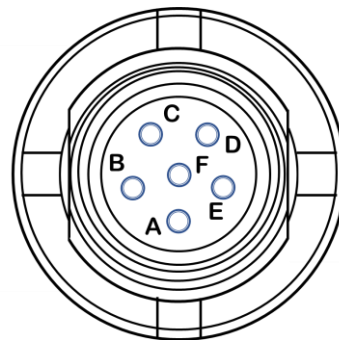


Figure 13.5.2.15-1: J12 Key Fill Connector Pin Arrangement

Table 13.5.2.15-1: J12 Key Fill Connector Pin Out Details

SOSA Electrical Interface J12 DS101 Key Fill Connector NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Reference	A	Logic Reference	Reference	✓	✓	✓	✓	✓

SOSA Electrical Interface J12 DS101 Key Fill Connector NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Signal	B	Balanced Line (+)	TIA 485-A	✓	✓	✓	✓	✓
Signal	C	Wake Up	Logic	✓	✓	✓	✓	✓
Reserved	D	NC	N/A					
Signal	E	Balanced Line (-)	TIA 485-A	✓	✓	✓	✓	✓
Reserved	F							

Rule 13.5.2.15-4: The J12 Key Fill Connector electrical signals for connector positions B and E shall be differential lines in accordance with the EKMS 308 TIA 485-A Interface. Conformance Methodology (I)

Rule 13.5.2.15-5: Where a Wake-Up capability is supported, the J12 Key Fill Connector shall provide a pin to activate the Key Fill Interface upon detection of a Wake-Up signal from a ground in accordance with the EKMS 308 Interface. Conformance Methodology (I)

13.5.2.16 Class 1 & 2 Sensor J13 – Key Fill Connector, GPS Devices

Rule 13.5.2.16-1: Where a DS-101 Interface is used with a sensor component that has provisions for a dedicated key fill port to a single End Cryptographic Unit (ECU) to distribute security keys or similar data to devices within the sensor, the sensor component shall employ a J13 chassis mounted Key Fill Connector (NSA P/N 0N241775 or equivalent) in accordance with EKMS 308 as shown in Figure 13.5.2.16-1. Conformance Methodology (I)

Observation 13.5.2.16-1: When the security policy requires a dedicated key fill port for the ECU, a dedicated connector, J13, will be provided.

Rule 13.5.2.16-2: If present, the J13 connector shall support either balanced mode (TIA 485) or unbalanced mode (TIA 232) or both modes.

Rule 13.5.2.16-3: If J13 supports both modes, the SOSA system shall implement a control mechanism to select which mode of operation is used for any key fill operation.

Rule 13.5.2.16-4: The SOSA system J13 connector and related electrical components shall not be damaged by being connected to a key fill device that is attempting to drive signals using a mismatched mode.

Rule 13.5.2.16-5: When the J13 Key Fill Connector is used, the J13 connector shell shall make electrical contact with the chassis for grounding in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

Rule 13.5.2.16-6: The J13 Key Fill Connector signals shall be assigned to pins in accordance with Table 13.5.2.16-1 if using the TIA 232 Protocol or Table 13.5.2.16-2 if using the TIA 485 Protocol. Conformance Methodology (I)

I/O signal designations are from the perspective of the box; that is, Data Out refers to a signal being driven from inside the box going out through the connector; Data In refers to signals being received inside the box coming in through the connector.

Observation 13.5.2.16-2: A cross-over cable that swaps pin B with E and C with D will be required when the TIA 232 Protocol is used.

Rule 13.5.2.16-7: When a J13 DS-101 Key Fill Connector implements a TIA 232 Interface, J13 connector pins B and D shall be inputs that follow the TIA 232 electrical standard.

Rule 13.5.2.16-8: When a J13 DS-101 Key Fill Connector implements a TIA 232 Interface, J13 connector pins C and E shall be outputs that follow the TIA 232 electrical standard.

Rule 13.5.2.16-9: When the J13 Key Fill Connector is used, the shell of the J13 connector shall make electrical contact with the sensor system chassis for grounding in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

Rule 13.5.2.16-10: The J13 Key Fill Connector signals shall be assigned to pins in accordance with Table 13.5.2.16-1. Conformance Methodology (I)

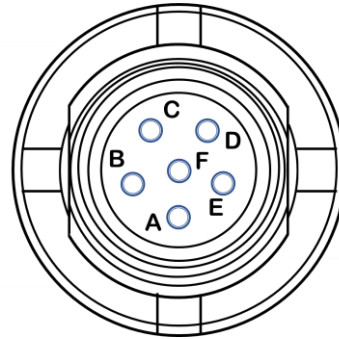


Figure 13.5.2.16-1: J13 Key Fill Connector Pin Arrangement

Table 13.5.2.16-1: J13 Key Fill Connector Pin Out Details when used with the TIA 232 Protocol

SOSA Electrical Interface J13 DS101 Key Fill Connector NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Reference	A	GND	Reference	✓	✓	✓	✓	✓
Signal	B	Flow Control In (FCI)	TIA 232	✓	✓	✓	✓	✓
Signal	C	Data Out	TIA 232	✓	✓	✓	✓	✓
Signal	D	Data In	TIA 232	✓	✓	✓	✓	✓
Signal	E	Flow Control Out (FCO)	TIA 232	✓	✓	✓	✓	✓
Reserved	F	Not Used						

Table 13.5.2.16-2: J13 Key Fill Connector Pin Out Details when used with the TIA 485 Protocol

SOSA Electrical Interface J12 DS101 Key Fill Connector NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Reference	A	Logic Reference	Reference	✓	✓	✓	✓	✓
Signal	B	Balanced Line (+)	TIA 485-A	✓	✓	✓	✓	✓
Signal	C	Wake Up	Logic	✓	✓	✓	✓	✓
Reserved	D	NC	N/A					
Signal	E	Balanced Line (-)	TIA 485-A	✓	✓	✓	✓	✓
Reserved	F							

Rule 13.5.2.16-11: When used with the TIA 232 Protocol, the J13 Key Fill Connector electrical signals for connector positions C and D shall be single-ended signals in accordance with the EKMS 308 TIA 232 Interface. Conformance Methodology (I)

Observation 13.5.2.16-3: When using the TIA 232 Protocol, signal position E is for Flow Control Out (FCO) for the TIA 232 Protocol for the SOSA sensor’s Key Fill Activity. Signal position B is for Flow Control In (FCI) supporting the TIA 232 Interface in accordance with EKMS 308 for the SOSA sensor’s Key Fill Activity.

Rule 13.5.2.16-12: When a DS-101 key fill is implemented with a TIA 232 Interface on the J13 Key Fill Connector, the J13 connector signal position C shall implement Data Out as described in EKMS 308. Conformance Methodology (I)

Rule 13.5.2.16-13: When a DS-101 key fill is implemented with a TIA 232 Interface on the J13 Key Fill Connector, the J13 connector signal position D shall implement Data In as described in EKMS 308. Conformance Methodology (I)

Rule 13.5.2.16-14: When a DS-101 key fill is implemented with a TIA 232 Interface on the J13 Key Fill Connector, the J13 connector signal position E shall implement FCO as described in EKMS 308. Conformance Methodology (I)

Rule 13.5.2.16-15: When a DS-101 key fill is implemented with a TIA 232 Interface on the J13 Key Fill Connector, the J13 connector signal position B shall implement FCI as described in EKMS 308. Conformance Methodology (I)

Rule 13.5.2.16-16: When a DS-101 key fill is implemented with a TIA 485 Interface, electrical signals for connector positions B and E shall be a differential pair (balanced lines) in accordance with the EKMS 308 TIA 485-A Interface. Conformance Methodology (I)

Rule 13.5.2.16-17: When a DS-101 key fill is implemented with a TIA 485 Interface, and where a Wake-Up capability is supported, the J13 Key Fill Connector shall provide a pin to activate the

Key Fill Interface upon detection of a Wake-Up signal from a ground in accordance with the EKMS 308 Interface. Conformance Methodology (I)

13.5.2.17 Class 1 and 2 Sensor J14 – Circular High-Density MT Connectors

13.5.2.17.1 Common Rules for Circular High-Density MT Connectors

Rule 13.5.2.17.1-1: The Circular High-Density MT connectors shall comply with following set of rules:

- Rule 13.5.3.5-3 Conformance Methodology (T)
- Rule 13.5.2.5-7 Conformance Methodology (I)
- Rule 13.5.2.16.1-2 Conformance Methodology (I)
- Rule 13.5.2.16.1-3 Conformance Methodology (T)
- Rule 13.5.2.16.1-4 Conformance Methodology (T)

Rule 13.5.2.17.1-2: The sensor system MM Fiber termini shall use MT ferrules complying with the applicable mechanical characteristics defined in IEC 61754-5. Conformance Methodology (I)

Rule 13.5.2.17.1-3: The F1 fiber shall be in the corner location, the closest to the identification mark of the MT ferrule (see Figure 13.5.2.17.1-1). Conformance Methodology (T)

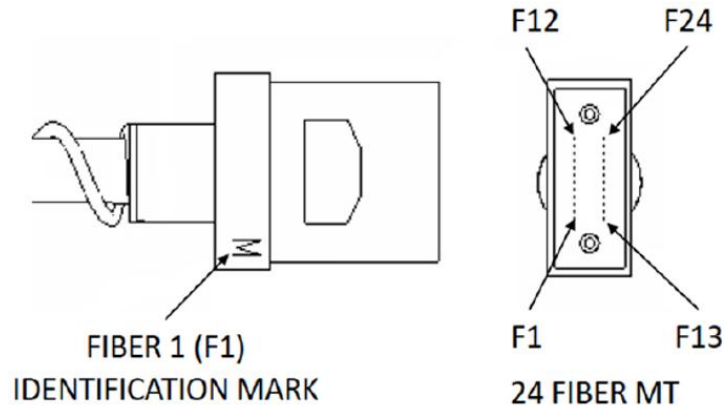


Figure 13.5.2.17.1-1: Mechanical Transfer Ferrule Pin Out

Table 13.5.2.17.1-1: High Density MT Connector MT Pin Allocation

SOSA Electrical Interface					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
High Density MT Connector – MT Pin Allocation on the connector plug side									
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
1	MM Fiber	Sensor Receive 12	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓

SOSA Electrical Interface					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
High Density MT Connector – MT Pin Allocation on the connector plug side					Used	Used	Used	Used	Used
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
13	MM Fiber	Sensor Transmit 12	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
2	MM Fiber	Sensor Receive 11	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
14	MM Fiber	Sensor Transmit 11	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
3	MM Fiber	Sensor Receive 10	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
15	MM Fiber	Sensor Transmit 10	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
4	MM Fiber	Sensor Receive 09	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
16	MM Fiber	Sensor Transmit 09	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
5	MM Fiber	Sensor Receive 08	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
17	MM Fiber	Sensor Transmit 08	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
6	MM Fiber	Sensor Receive 07	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
18	MM Fiber	Sensor Transmit 07	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓

SOSA Electrical Interface					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
High Density MT Connector – MT Pin Allocation on the connector plug side					Used	Used	Used	Used	Used
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
7	MM Fiber	Sensor Receive 06	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
19	MM Fiber	Sensor Transmit 06	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
8	MM Fiber	Sensor Receive 05	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
20	MM Fiber	Sensor Transmit 05	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
9	MM Fiber	Sensor Receive 04	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
21	MM Fiber	Sensor Transmit 04	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
10	MM Fiber	Sensor Receive 03	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
22	MM Fiber	Sensor Transmit 03	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
11	MM Fiber	Sensor Receive 02	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
23	MM Fiber	Sensor Transmit 02	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓
12	MM Fiber	Sensor Receive 01	Sensor	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓

SOSA Electrical Interface					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
High Density MT Connector – MT Pin Allocation on the connector plug side					Used	Used	Used	Used	Used
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
24	MM Fiber	Sensor Transmit 01	Platform	10GBase-SR/ 25GBASE-SR/ 40GBase-SR4/ 100GBase-SR4	✓	✓	✓	✓	✓

Rule 13.5.2.17.1-4: Where a three FPs configuration is used, the FP positions allocation shall be: Conformance Methodology (T)

- Fat Pipe 1: positions 12, 24, 11, 23, 10, 22, 9, 21
- Fat Pipe 2: positions 8, 20, 7, 19, 6, 18, 5, 17
- Fat Pipe 3: positions 4, 16, 3, 15, 2, 14, 1, 13

13.5.2.17.2 Class 1 and 2 Sensor J14 Connector

Recommendation 13.5.2.17.2-1: Where the sensor requires to interconnect more than 24 optical fibers, connector J14 should be used. Conformance Methodology (I)

Rule 13.5.2.17.2-1: The sensor system fiber J14 shall comply with the rules defined in Rule 13.5.2.17.1-1. Conformance Methodology (I)

Rule 13.5.2.17.2-2: J14 High Density Fiber Connector shall have MT arrangement as shown in Figure 13.5.2.17.2-1. Conformance Methodology (I)

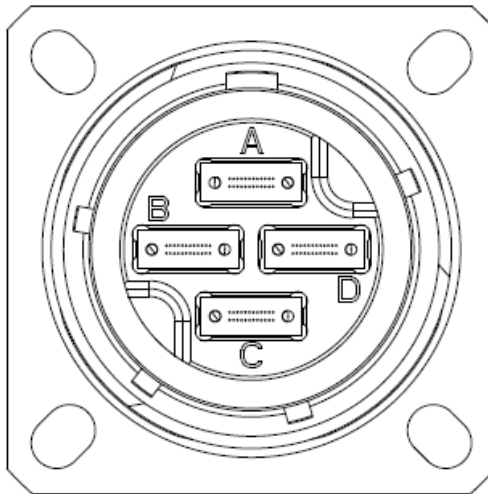


Figure 13.5.2.17.2-1: J14 High Density Fiber Connector (4 MT)

Observation 13.5.2.17.2-1: When fewer than four MT ferrules are needed, J14 High Density Fiber Connector could include dummy ferrule modules.

13.5.2.18 Class 1 and 2 Sensor J15 – Circular High-Density MT Connectors

Observation 13.5.2.18-1: Where the sensor requires to interconnect with 24 optical fibers or less, connector J15 could be used.

Rule 13.5.2.18-1: The sensor system fiber J15 shall comply with the set of common rules defined in Rule 13.5.2.17.1-1. Conformance Methodology (I)

Rule 13.5.2.18-2: J15 High Density Fiber Connector shall have MT arrangement as shown in Figure 13.5.2.18-1. Conformance Methodology (I)

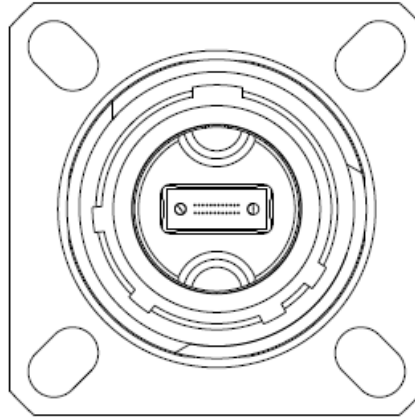


Figure 13.5.2.18-1: J15 High Density Fiber Connector (1 MT)

13.5.2.19 Class 1 and 2 Sensor J16 – External Battery Connectors

Rule 13.5.2.19-1: Where required, the sensor system J16 External Battery Connector shall have a 9-35 insert with 6 contacts pattern as shown in Figure 13.5.2.19-1. Conformance Methodology (I)

Rule 13.5.2.19-2: Signals for the sensor system J16 External Battery Connector shall be assigned to pins in accordance with Table 13.5.2.19-1. Conformance Methodology (I)

Table 13.5.2.19-1: J16 External Battery Connector Pin Allocation

J16-VBAT (9-35 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**A35PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*A35SN (plug with sockets inserts)						EO-IR Sensor	Radar/SA R Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
EXT VBAT	1	AWG22	V_BATT	Platform	3.3VDC	✓	✓	✓	✓	✓
	5	AWG22	V_BATT_RTN	Platform	DC Return					
EXT ALT_V BAT	3	AWG22	ALT_V_BATT	Platform	3.9VDC	✓	✓	✓	✓	✓
	4	AWG22	ALT_V_BATT_RTN	Platform	DC Return					

J16-VBAT (9-35 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**A35PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*A35SN (plug with sockets inserts)						EO-IR Sensor	Radar/SA R Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Reserved	2									
	6									

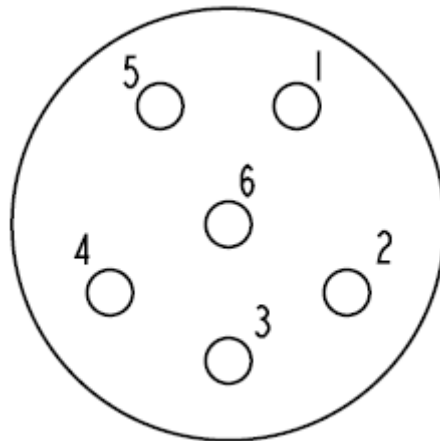


Figure 13.5.2.19-1: J16 External Battery Connector Pin Arrangement

13.5.2.19.1 VBAT Battery Power

Rule 13.5.2.19.1-1: The sensor system J16 shall support a low current battery power input to be provided by the platform to hold up services such as volatile memory and real-time clocks over power cycles. The maximum voltage is 3.5 VDC with a maximum current of 115mA. Conformance Methodology (I)

13.5.2.19.2 ALT_VBAT Battery Power

Rule 13.5.2.19.2-1: The sensor system J16 shall support a low current battery power input to be provided by the platform to hold up services such as key fill devices over power cycles. The maximum voltage is 3.9 VDC with a maximum current of 115mA. Conformance Methodology (I)

13.5.3 SOSA Electrical Class 3 Electrical Interfaces

13.5.3.1 Class 3 Sensor Electrical Connector Characteristics

There are multiple connectors defined by this electrical standard. Table 13.5.3.1-1 describes the Class 3 connectors including sensor modalities, type, shell size, gender, keying, and inserts. Detailed requirements for each connector, defined separately for each modality of sensor, are defined in later sections.

Rule 13.5.3.1-1: The Class 3 SOSA sensor connectors shall meet the type, size, gender, and insert attributes in Table 13.5.3.1-1. Conformance Methodology (I)

Rule 13.5.3.1-2: For SOSA sensors assigned an Electrical Class 3, a J2, J3, J4, J8, J9, J10, J11, J14, or J15 connector shall be required. Conformance Methodology (I)

Permission 13.5.3.1-1: J2-defined signal pins may not be fully allocated to the connector depending on the mission of the SOSA sensor.

Rule 13.5.3.1-3: If the J2 connector does not fully allocate all the signal pins, then the claimant of conformance shall provide a written pin allocation of used and unused pins. Conformance Methodology (A)

Mission requirements could necessitate multiples of the same connector. For example, a mission or application of one SOSA sensor could use two J4 connectors, one J2 connector, and one J1 connector. However, there is only one J1 connector for DC power for each external sensing element. If additional power is required, then the J6 auxiliary power connector, or possibly multiple J6 connectors, in addition to the J1 connector, could be used.

Permission 13.5.3.1-2: Multiple instantiations of each J connector may be used on a SOSA sensor, except for J1 for DC power for each external sensing element.

Rule 13.5.3.1-4: No more than one J1 connector shall be used for a single external sensing element. Conformance Methodology (I)

Rule 13.5.3.1-5: Only if a J1 connector is used, shall additional J6 connectors be used. Conformance Methodology (I)

Rule 13.5.3.1-6: The first instantiation of J1, J2, J3, J4, J8, J9, J11, J14, or J15 shall use the keying position listed in Table 13.5.3.1-1 conforming to the key/keyway rotation position in MIL-DTL-38999M, Figure 6. Conformance Methodology (I)

Rule 13.5.3.1-7: The first instantiation of J7 shall use the keying position listed in Table 13.5.3.1-1 conforming to the key/keyway rotation position in ANSI/VITA 76.0 Rule 2.3-1 and Rule 2.3-2. Conformance Methodology (I)

Rule 13.5.3.1-8: Any additional instantiations of J6 beyond its first instantiation shall use any key/keyway rotation positions conforming to MIL-DTL-38999M, Figure 6, with the exception of position A and position N. Conformance Methodology (I)

Rule 13.5.3.1-9: Any additional instantiations of a J2, J3, J4, J8, J9, J10, J11, J14, or J15 connector beyond their first instantiation shall use any key/keyway rotation positions conforming to MIL-DTL-38999M, Figure 6, except for position N. Conformance Methodology (I)

Rule 13.5.3.1-10: Any additional instantiations of J7 beyond its first instantiation shall use any other key/keyway rotation position conforming to ANSI/VITA 76.0 Rule 2.3-1 and Rule 2.3-2, with the exception of position N. Conformance Methodology (I)

There are finite key positions available, as specified by the standards referenced in the rules above. When there are multiple instantiations of the same J connector, it is best practice to name them as “J#”-“key position”. For example, if there are two J3 connectors, then one could be J3-A and another J3-B. Furthermore, best practices include a description that differentiates the

multiple connectors. For example, J3-A could be described as “Video cable for SWIR”, and J3-B as “Video cable for MWIR”.

Permission 13.5.3.1-3: It is not required that all of the connectors listed in Table 13.5.3.1-1 are needed depending on the mission of the SOSA sensor.

Rule 13.5.3.1-11: The claimant for conformance shall list all used SOSA connectors. If multiple instantiations of the same J connector are used, then the list shall differentiate each of the multiple connectors by key position using the nomenclature, “J#”-“key position”. Conformance Methodology (A)

Rule 13.5.3.1-12: If multiple instantiations of the same J connector are used, each connector on the list shall include a brief description of the connector, indicating its difference from the others. Conformance Methodology (A)

While SOSA defined connectors are preferred, they are not required. However, interoperability can only be achieved through an open electrical interface. It is expected that SOSA non-defined cables include enough description to recreate a functional interface. SOSA non-defined connectors cannot be considered SOSA conformant.

Permission 13.5.3.1-4: It is permissible to use non-SOSA defined connectors.

Rule 13.5.3.1-13: If SOSA non-defined connectors are used, the claimant for conformance shall list all connectors that are not defined in this document, as well as provide for each an associated pin assignment including the modality, connection description, pin number, wire type, signal name, and signal type, as well as the pin arrangement. Conformance Methodology (A)

Table 13.5.3.1-1: Class 3 Sensor Connectors

Designator	Purpose	Modality Support	Type	Shell Size	Sensor LRU Gender	Platform Umbilical Gender	Keying	Insert
J1	DC Power	All	MIL-DTL-38999/Series III	19	Receptacle with pin inserts	Plug with socket inserts	N	19-11
J2	Signal	All	MIL-DTL-38999/Series III	19	Receptacle with socket inserts	Plug with pin inserts	N	19-35
J3	Video (Copper)	EO-IR, Communications	MIL-DTL-38999/Series III	17	Receptacle with socket inserts	Plug with pin inserts	N	17-6
J4	Fiber Optic	All	MIL-DTL-38999/Series III	13	Receptacle with socket inserts for fiber optics	Plug with pin inserts for fiber optics	N	13-4
J5	GPS Antenna	All	MIL-PRF-39012	TNC	Receptacle	Plug	—	—
J6	Aux DC Power	All	MIL-DTL-38999/Series III	19	Receptacle with pin inserts	Plug with socket inserts	A	19-11
J7	High Speed (Copper)	All	ANSI/VITA 76.0	17	Receptacle with pin inserts	Plug with socket inserts	N	

Designator	Purpose	Modality Support	Type	Shell Size	Sensor LRU Gender	Platform Umbilical Gender	Keying	Insert
J8	High Density RF	Comms., EW, Radar/SAR, SIGINT	MIL-DTL-38999/Series III	21	Receptacle with socket inserts	Plug with pin inserts	N	21-11
J9	Low Loss RF	Comms., EW, Radar/SAR, SIGINT	MIL-DTL-38999/Series III	21	Receptacle with socket inserts	Plug with pin inserts	N	21-75
J11	High Voltage DC	All	MIL-DTL-38999/Series III	11	Receptacle with pin inserts	Plug with socket inserts	N	11-5
J14	High Density Fiber	All	VITA 87.0	13	Receptacle with 2 optical MT with physical contacts for 48 optic fibers	Plug with socket inserts	N	-
J15	High Density Fiber	All	VITA 87.0	11	Receptacle with 1 optical MT with physical contacts for 24 optic fibers	Plug with socket inserts	N	-
J16	External Battery	All	MIL-DTL-38999/Series III	9	Receptacle with pin inserts	Plug with socket inserts	N	9-6
J17X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	TNC	Receptacle	Plug		
J18X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	SMA	Receptacle	Plug		
J19X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	2.4mm	Receptacle	Plug		
J20X	Auxiliary RF Connector	EO/IR, Comms., EW, Radar/SAR, SIGINT	MIL-PRF-39012	1.0mm	Receptacle	Plug		

13.5.3.2 Class 3 Sensor J1-DC Power Connector

Rule 13.5.3.2-1: The J1 Power Connector shall use a 19-11 insert pattern shown in Figure 13.5.3.2-1. Conformance Methodology (I)

Rule 13.5.3.2-2: The Class 3 J1 Power Connector shall assign pins in accordance with Table 13.5.3.2-1. Conformance Methodology (I)

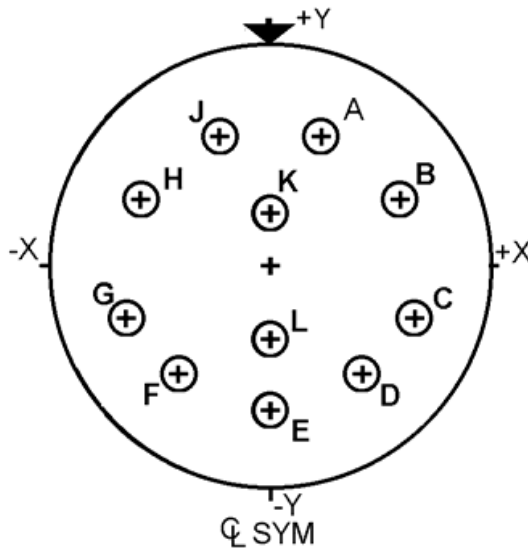


Figure 13.5.3.2-1: J1-DC Power Connector Pin Arrangement

Table 13.5.3.2-1: J1-DC Power Connector Pin Allocation

J1-DC Power (19-11 insert, N-Keying)										
For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish										
Sensor MIL-DTL-38999/**F11PN (receptacle with pin inserts)										
Platform Umbilical MIL-DTL-38999/26*F11SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
28VDC	D	SC-AWG16	DC-1	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	E	SC-AWG16	DC-1 RTN	Platform	DC RTN					
28VDC	F	SC-AWG16	DC-2	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	L	SC-AWG16	DC-2 RTN	Platform	DC RTN					
28VDC	C	SC-AWG16	DC-3	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	G	SC-AWG16	DC-3 RTN	Platform	DC RTN					
Safety Ground	K	SC-AWG16	Chassis	Platform	Ground	✓	✓	✓	✓	✓
28VDC	A	SC-AWG16	DC-4	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	J	SC-AWG16	DC-4 RTN	Platform	DC RTN					
28VDC	B	SC-AWG16	DC-5	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	H	SC-AWG16	DC-5 RTN	Platform	DC RTN					

13.5.3.2.1 Power

Rule 13.5.3.2.1-1: Where +28 VDC input power is used, the vendor shall select one or more of the applicable standards per Table 13.5.1.1-1, to define input power characteristics for the sensor system's J1-DC Power Connector (Table 13.5.3.2-1). Conformance Methodology (I)

Rule 13.5.3.2.1-2: The sensor system's J1-DC Power connector shall accept +28 VDC power on any combination of the '+28VDC/RTN' pin pairs listed in Table 13.5.3.2-1. Conformance Methodology (I)

Rule 13.5.3.2.1-3: Where a J1 Power Connector '+28VDC/RTN' pair is used, the allowable inrush limit shall be specified by the procuring activity. Conformance Methodology (I)

Observation 13.5.3.2.1-1: The '+28VDC/RTN' pair inrush limit could be accomplished by the platform.

Observation 13.5.3.2.1-2: Where more than 10A (nominal) current of +28VDC power is required to the sensor, the J1-DC Power connector's +28 VDC and RTN pairs (as identified in Table 13.5.3.2-1) could be connected in parallel, up to a maximum of 5 pairs.

Rule 13.5.3.2.1-4: The nominal current input to any '+28VDC/RTN' pair shall not exceed 10A per Table 13.5.3.2-1. Conformance Methodology (A)

Observation 13.5.3.2.1-3: Where more than 350W of input power is needed, utilization of a higher input voltage is recommended.

Rule 13.5.3.2.1-5: The sensor chassis shall exhibit $\geq 1M\Omega$ isolation to any J1 connector power returns. Conformance Methodology (I)

13.5.3.2.2 Safety Ground

Rule 13.5.3.2.2-1: The Class 3 J1-DC Power connector Safety Ground shall connect between the sensor system ground contact and the sensor system chassis with a resistance of $\leq 0.1 \Omega$ in accordance with MIL-STD-1310 §3.20. Conformance Methodology (I)

13.5.3.3 Class 3 Sensor J2-Signal Connector

Observation 13.5.3.3-1: When commercial protocols are routed through connector J2, pin out and nomenclature in this document are based upon the commercial standard but could vary slightly as required to maintain signal and ground paths, and preserve signal integrity.

Rule 13.5.3.3-2: The Class 3 J2 Signal Connector shall use a 19-35 insert pattern shown in Figure 13.5.3.3-1. Conformance Methodology (I)

Rule 13.5.3.3-3: The Class 3 J2 Signal Connector shall assign pins in accordance with Table 13.5.3.3-1. Conformance Methodology (I)

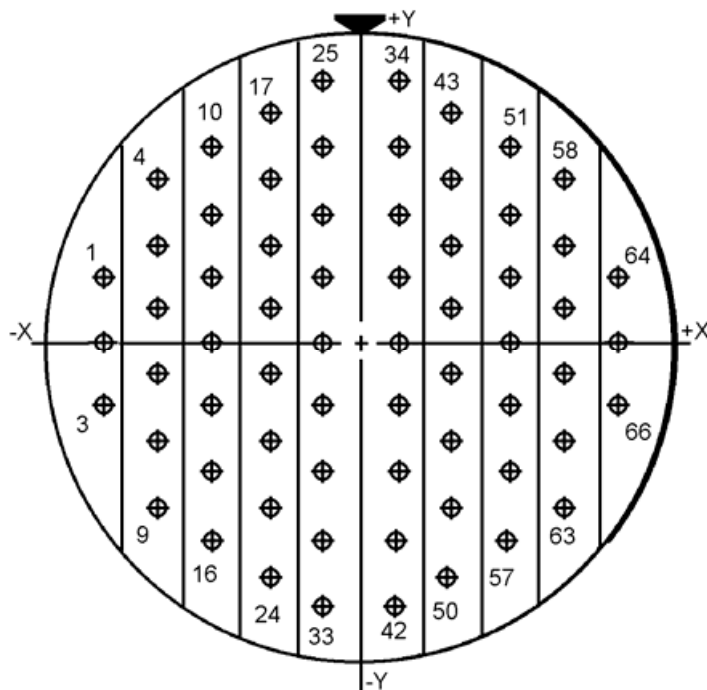


Figure 13.5.3.3-1: J2-Signal Connector Pin Arrangement

Table 13.5.3.3-1: J2-Signal Connector Pin Allocation

SOSA Electrical Interface										
J2-Signal (19-35 insert, A-Keying)										
For Part Numbers insert receptacle choice (20 or24) and relevant plating finish										
Sensor MIL-DTL-38999/**D35SA (receptacle with socket inserts)						EO-IR	Radar/SAR	EW	SIGINT	Comms
Platform Umbilical MIL-DTL-38999/26*F35PA (plug with pin inserts)						Sensor	Sensor	Sensor	Sensor	
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Power Enable Discrete	19	STP 2419	PWR_EN	Platform	Open/Closed Circuit	✓	✓	✓	✓	✓
	27	STP 2419	PWR_EN_RTN	Platform	Open/Closed Circuit					
Ethernet	22	100Ω STP – AWG 24, CAT 6A SAE AS6070/6 Recommendation	DA+	Platform/ Sensor	1000BaseT	✓	✓	✓	✓	✓
	23		DA-	Platform/ Sensor						
	31		DA Shield	Platform/ Sensor						
	32		DB+	Platform/ Sensor						
	33		DB-	Platform/ Sensor						

SOSA Electrical Interface J2-Signal (19-35 insert, A-Keying) For Part Numbers insert receptacle choice (20 or24) and relevant plating finish Sensor MIL-DTL-38999/**D35SA (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F35PA (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	24		DB Shield	Platform/ Sensor						
	48		DC+	Platform/ Sensor						
	49		DC-	Platform/ Sensor						
	40		DC Shield	Platform/ Sensor						
	41		DD+	Platform/ Sensor						
	42		DD-	Platform/ Sensor						
	50		DD Shield	Platform/ Sensor						
Serial Comms 1	8	100 Ohm STP 2419	TX1+	Sensor	TIA 422	✓	✓	✓	✓	✓
	14	100 Ohm STP 2419	TX1-	Sensor						
	15	SC-AWG24	422_1_RTN							
	9	100 Ohm STP 2419	RX1+	Platform						
	16	100 Ohm STP 2419	RX1-	Platform						
Serial Comms 2	20	100 Ohm STP 2419	TX2+	Sensor	TIA 422	✓	✓	✓	✓	✓
	28	100 Ohm STP 2419	TX2-	Sensor						
	29	SC-AWG24	422_2_RTN							
	21	100 Ohm STP 2419	RX2+	Platform						
	30	100 Ohm STP 2419	RX2-	Platform						

SOSA Electrical Interface J2-Signal (19-35 insert, A-Keying) For Part Numbers insert receptacle choice (20 or24) and relevant plating finish Sensor MIL-DTL-38999/**D35SA (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F35PA (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Serial Comms 3	44	100 Ohm STP 2419	TX3+	Sensor	TIA 422	✓	✓	✓	✓	✓
	46	100 Ohm STP 2419	TX3-	Sensor						
	38	SC-AWG24	422_3_RTN							
	47	100 Ohm STP 2419	RX3+	Platform						
	39	100 Ohm STP 2419	RX3-	Platform						
Serial Comms 4	55	100 Ohm STP 2419	TX4+	Sensor	TIA 422	✓	✓	✓	✓	✓
	62	100 Ohm STP 2419	TX4-	Sensor						
	56	SC-AWG24	422_4_RTN							
	57	100 Ohm STP 2419	RX4+	Platform						
	63	100 Ohm STP 2419	RX4-	Platform						
Emi- sion Arming	2	AWG22	MASTER_AR M	Platform	open/closed circuit	✓	✓			
	5	AWG22	MASTER_AR M_RET	Platform	open/closed circuit					
NEZ Cutout (Dis- cretes)	11	AWG24	NEZ_SELECT _BIT 0	Platform	open/closed circuit	✓	✓			
	12	AWG24	NEZ_SELECT _BIT 1	Platform	open/closed circuit					
	13	AWG24	NEZ_SELECT _PARITY	Platform	open/closed circuit					
	52	AWG24	NEZ_SELECT _RTN	Platform	open/closed circuit					
Emi- ssions Mode Select	53	AWG24	MODE_SELEC T_BIT 0	Platform	28 V logic	✓	✓			

SOSA Electrical Interface J2-Signal (19-35 insert, A-Keying) For Part Numbers insert receptacle choice (20 or24) and relevant plating finish Sensor MIL-DTL-38999/**D35SA (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F35PA (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	54	AWG24	MODE_SELEC T_BIT 1	Platform	28 V logic					
	59	AWG24	MODE_SELEC T_PARITY	Platform	28 V logic					
	65	AWG24	MODE_SELEC T_RTN	Platform	28 V logic (rtn)					
Em- ission Annun- ciation	51	100 Ohm STP 2419	LF+	Sensor	Isolated 28V Logic	✓	✓			
	58	100 Ohm STP 2419	LF-	Sensor	Isolated 28V Logic					
Safety Status (Dis- cretes)	4	100 Ohm STP 2419	SS1+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	10	100 Ohm STP 2419	SS1-	Sensor	Isolated 28V Logic					
	17	100 Ohm STP 2419	SS2+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	25	100 Ohm STP 2419	SS2-	Sensor	Isolated 28V Logic					
	34	100 Ohm STP 2419	SS3+	Sensor	Isolated 28V Logic	✓	✓	✓	✓	✓
	43	100 Ohm STP 2419	SS3-	Sensor	Isolated 28V Logic					
Enable Gimbal Move- ment	60	AWG22	ENBL_GIMB	Platform	open/closed circuit	✓	✓			
	61	AWG22	ENBL_GIMB_ RTN	Platform	open/closed circuit					
Time Sync 1 PPS	35	100 Ohm STP 2419	1 PPS	Platform	10 V logic	✓	✓	✓	✓	✓
	45	100 Ohm STP 2419	1 PPS RTN	Platform	10 V logic					
HC Power	36	AWG22	HAND_CONT _PWR	Sensor	28VDC@500ma	✓				

SOSA Electrical Interface J2-Signal (19-35 insert, A-Keying) For Part Numbers insert receptacle choice (20 or24) and relevant plating finish Sensor MIL-DTL-38999/**D35SA (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*F35PA (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	37	AWG22	H_C_PWR_RT N	Sensor	DC Return					
Reserve d										
USB Data	1	90 – 100 Ohm STP 2419	USB_DATA+	Platform/ Sensor	USB Data	✓	✓	✓	✓	✓
	3	90 – 100 Ohm STP 2419	USB_DATA-	Platform/ Sensor	USB Data					
	6	Shield	GND	Platform/ Sensor	USB Data Shield					
USB Power	7	STP 2419	USB_PWR_+5 V	Sensor	USB Power	✓	✓	✓	✓	✓
	64	STP 2419	USB_PWR_RT N	Sensor	USB Power					
	66	Shield	GND	Sensor	USB Power Shield					

Observation 13.5.3.3-1: Each signal group in Table 13.5.3.3-1 is described in more detail below. By convention of this document, individual signal sets will have their own return line. This is done for EMC performance, as well as ease of platform integration.

Rule 13.5.3.3-4: When an isolated +28Vdc discrete signal of amplitude $\geq 18.0\text{VDC}$ is received by the J2-Signal connector, the signal shall be interpreted as a logic level ‘1’. Conformance Methodology (T)

Rule 13.5.3.3-5: The sensor system shall interpret a voltage level of $\leq 1.5\text{VDC}$ as logic ‘0’. Conformance Methodology (T)

13.5.3.3.1 Power Enable

The Power Enable signal is used for a controlled power up and shutdown of the sensor system. This control is necessary if the sensor system is required to execute a sequence of steps upon shutdown, steps that the sensor system would be precluded from executing if power were simply removed from the system. The Power Enable signal is controlled by the platform and, when disabled, instructs the sensor to power down.

Power Enable is a switch, relay, or SSR controlled by the platform (or human on the platform side of the interface). The switch goes across PWR_EN and PWR_EN_RTN. The sensor

provides the voltage for this. Power Enable is disabled if an open circuit exists externally between the contacts (i.e., the switch is open). Power Enable is enabled if a closed circuit is externally applied between the contacts.

Rule 13.5.3.3.1-1: When the Power Enable circuit has a resistance value $\geq 100\text{K}\Omega$, the Class 3 J2 Signal Connector shall enter the Power OFF condition. Conformance Methodology (I)

Rule 13.5.3.3.1-2: When the Power Enable circuit has a resistance value $< 5\text{ Ohms}$, the Class 3 J2 Signal Connector shall enter the Power ON condition. Conformance Methodology (I)

Rule 13.5.3.3.1-3: The Class 3 J2 Signal Connector shall source a 100mA maximum current on the Power Enable signal. Conformance Methodology (I)

Rule 13.5.3.3.1-4: The Class 3 J2 Signal Connector shall drive a maximum of 30 VDC on the Power Enable signal. Conformance Methodology (I)

13.5.3.3.2 Ethernet (Copper)

Gigabit Ethernet is an 8-wire (4 twisted-pair), 100 Ω connection.

Rule 13.5.3.3.2-1: The Class 3 J2 Signal Connector shall implement Gigabit Ethernet. Conformance Methodology (I)

Rule 13.5.3.3.2-2: Where using Gigabit Ethernet, the Class 1&2 J2 Signal Connector shall conform with IEEE 802.3-2008 for a 1000BaseT channel using CAT 6A AS6070/6 cable or equivalent. Conformance Methodology (I)

13.5.3.3.3 Serial Communications

Up to four application-configurable serial communication ports are defined.

Rule 13.5.3.3.3-1: The Class 1&2 J2 Signal Connector ports shall conform to TIA/EIA-422. Conformance Methodology (I)

Observation 13.5.3.3.3-1: Each serial communications port includes a return connection for ease of platform integration. The sensor system supplier can determine the need for this return line and implement it taking into consideration best practices regarding EMC/EMI.

13.5.3.3.4 Arming and Cutouts

A set of ten pins is dedicated to control of energy emitting sensors such as the arming of laser devices, or RF transmission devices. This includes the selection of predefined emission suppression zone maps for turreted sensors.

Rule 13.5.3.3.4-1: The Class 3 J2 Signal Connector shall source 100mA (maximum) for the Arming and Cutout signal channels. Conformance Methodology (I)

Rule 13.5.3.3.4-2: The Class 3 J2 Signal Connector shall drive 30 VDC (maximum) for the Arming and Cutout signal channels. Conformance Methodology (I)

13.5.3.3.4.1 MASTER_ARM

To arm an emission device, the platform closes the switch which completes the circuit. The current which goes through it, and the voltage across it, come from the sensor system. These pins form part of the power circuit for an emission device in the sensor. When the pins are open,

power to the device is disabled; when close-circuited, power is enabled. The pins allow the integrator to connect a simple arming switch to these contacts.

Rule 13.5.3.3.4.1-1: The Class 3 J2 Signal Connector shall use pins 2 and 95 for Emissions Arming. Conformance Methodology (I)

13.5.3.3.4.2 NEZ Cutout

The sensor systems can have a NEZ, or Cutout Map. The NEZ is a two-dimensional map, in azimuth and elevation that defines where the device can and cannot emit. It is designed to inhibit emissions when the turret's LOS is over any part of the platform. This prevents energy from reflecting, posing a hazard. The map is stored in the sensor memory. A sensor could have several maps stored, enabling it to be mounted at several points on the platform, or on several platform models, without modification. The NEZ is a high-reliability mechanism is to select which map to be used.

There are three NEZ circuits. Each is a switch, relay, or SSR provided by, and independently controlled by, the platform. The three circuits have a common return, NEZ_SELECT_RTN.

The sensor system J2 pins 4, 5, 11, and 12 shall be used for NEZ map selection. If three of the four pins allocated to this function are used to select a map, up to four maps can be defined in the turret. The fourth pin would be used as a parity check for safety.

Rule 13.5.3.3.4.2-1: The Class 3 J2 Signal Connector shall use pins 4, 5, 11, and 12 for NEZ map selection. Conformance Methodology (I)

Observation 13.5.3.3.4.2-1: If three of the four pins allocated to this function are used to select a map, up to four maps can be defined in the turret. The fourth pin would be used as a parity check for safety.

13.5.3.3.4.3 Emissions Mode Select

The sensor system could have several modes. These pins determine under what conditions or states the device will be used. For example, if there are multiple lasers in a sensor, these pins could be used to select one or more lasers to fire.

There are three Mode Select circuits. Each is a switch, relay, or SSR provided by, and independently controlled by, the platform. The three circuits have a common return MODE_SELECT_RTN.

Rule 13.5.3.3.4.3-1: The Class 3 J2 Signal Connector shall use pins 89, 90, 97, and 98 for emissions mode select. Conformance Methodology (I)

Observation 13.5.3.3.4.3-1: If three of the four pins allocated to this function are used to select a mode, up to four modes can be defined in the sensor. The fourth pin would be used as a parity check for safety.

13.5.3.3.5 Emissions Annunciation

Rule 13.5.3.3.5-1: The Class 3 J2 Signal Connector shall use Emissions signals to annunciate the firing of an emission device. Conformance Methodology (I)

Rule 13.5.3.3.5-2: The Class 3 J2 Signal Connector Emissions signals shall be an isolated 28 VDC signal. Conformance Methodology (I)

Rule 13.5.3.3.5-3: The Class 3 J2 Signal Connector Emissions signals shall be a maximum of 30 VDC/100mA. Conformance Methodology (I)

13.5.3.3.6 Safety Status

A set of three signal pairs are available to indicate the status of safety-relevant functions in the sensor system.

Rule 13.5.3.3.6-1: The Class 3 J2 Signal Connector's Safety Status signals shall be 28 VDC isolated signals. Conformance Methodology (I)

Observation 13.5.3.3.6-1: These signals are controlled by the sensor.

Rule 13.5.3.3.6-2: The Class 3 J2 Signal Connector Safety Status signals shall be a maximum of 30 VDC/100mA. Conformance Methodology (I)

13.5.3.3.7 Enable Gimbal Movement

This control is necessary to ensure that the sensor does not move in azimuth and/or elevation at high speeds endangering individuals that could be working near the sensor. The Enable Gimbal Movement signal originates from the sensor with the platform opening and closing the circuit.

Rule 13.5.3.3.7-1: When the gimbal motors are required to be disabled, the Enable Gimbal Movement signal on the Class 3 J2 signal connector shall be an open circuit. Conformance Methodology (T)

13.5.3.3.8 Time Synchronization – 1 PPS

Rule 13.5.3.3.8-1: When provided by the platform, the Class 3 J2 connector shall accept the input time roll-over pulse (1 PPS) signal which is in accordance with ICD-GPS-060B. See also Figure 13.5.3.3-1. Conformance Methodology (I)

13.5.3.3.9 Hand Controller Power

Rule 13.5.3.3.9-1: The Class 3 J2 Signal Connector shall provide power for a hand controller. Conformance Methodology (I)

Rule 13.5.3.3.9-2: When hand controller is required, the Class 3 J2 Signal Connector shall provide power with a maximum of 30 VDC and 500mA. Conformance Methodology (I)

13.5.3.3.10 USB Data

Permission 13.5.3.3.10-1: The sensor may optionally provide a USB 2.0 Host interface.

13.5.3.3.11 USB Power

Rule 13.5.3.3.11-1: When a USB 2.0 Host interface is required, the Class 3 J2 Signal Connector shall supply power at 5V @+/-5% and up to 500mA. Conformance Methodology (I)

13.5.3.4 Class 3 Sensor J3-Video (Copper) Connector

Rule 13.5.3.4-1: The sensor system J3-Video Connector shall have a 17-6 pin arrangement as shown in Figure 13.5.3.4-1. Conformance Methodology (I)

Rule 13.5.3.4-2: Signals for the J3-Video Connector shall be assigned to pins in accordance with Table 13.5.3.4-1. Conformance Methodology (I)

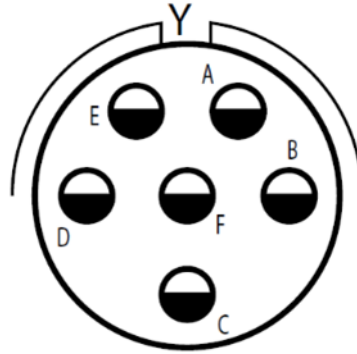


Figure 13.5.3.4-1: J3-Video Connector Pin Arrangement

Table 13.5.3.4-1: J3-Video Connector Pin Allocation

J3-Video (17-6 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted Sensor: MIL-DTL-38999***E06SNLC/M39029/75-416 (receptacle with coax socket inserts) Platform Umbilical: MIL-DTL-38999***26*E06PNLC/M39029/28-211 (plug with coax pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms	
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used	Notes
A	Coax-75Ω	Digital Video Ch1	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For Input from EO/IR Sensor
B	Coax-75Ω	Digital Video Ch2	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For Input from EO/IR Sensor
C	Coax-75Ω	Digital Video Ch3	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For Input from EO/IR Sensor
D	Coax-75Ω	Digital Video Ch4	Sensor	SMPTE ST 292/424/2081/2082	✓				✓	For Input from EO/IR Sensor
E	Coax-75Ω	Composite Video Ch 1	Sensor	RS-170a Composite Video	✓				✓	For Input from EO/IR Sensor

J3-Video (17-6 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted Sensor: MIL-DTL-38999***E06SNLC/M39029/75-416 (receptacle with coax socket inserts) Platform Umbilical: MIL-DTL-38999***26*E06PNLC/M39029/28-211 (plug with coax pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms	
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used	Notes
F	Coax-75Ω	Composite Video Ch 2	Sensor	RS-170a Composite Video	✓				✓	For Input from EO/IR Sensor

Rule 13.5.3.4-3: The sensor system digital channels shall comply with the SMPTE ST 292, SMPTE ST 424, SMPTE ST 2081, or SMPTE ST 2082 standard, driving into 75Ω: #12 coax contacts. Conformance Methodology (I)

Rule 13.5.3.4-4: The sensor system analog channels shall comply with the RS-170a standard, driving into 75 Ω #12 coax contacts. Conformance Methodology (I)

13.5.3.5 Class 3 Sensor J4-Fiber Optics Connector

Rule 13.5.3.5-1: The J4 Fiber Optic connector shall have a 13-4 pin arrangement in Figure 13.5.3.5-1. Conformance Methodology (I)

Rule 13.5.3.5-2: Signals for the J4-Fiber Optics Connector shall be assigned to pins in accordance with Table 13.5.3.5-1. Conformance Methodology (I)

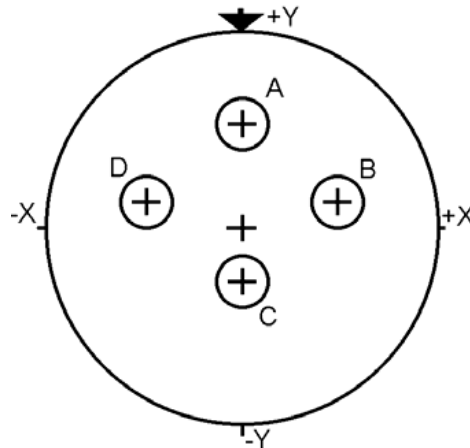


Figure 13.5.3.5-1: J4-Fiber Optics Connector Pin Arrangement

Table 13.5.3.5-1: J4-Fiber Optics Connector Pin Allocation

SOSA Electrical Interface J4-Fiber (13-4 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and fiber contacts inserted Sensor MIL-DTL-38999/**C04SNLCM/29504/5 (receptacle with socket inserts) Platform Umbilical MIL-DTL-3899926*C04PNLCM/29504/4 (plug with pin inserts)					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
A	MM Fiber	Sensor Transmit 1	Sensor	10GBase-SR/ 25GBase-SR	✓	✓	✓	✓	✓
B	MM Fiber	Sensor Receive 1	Platform	10GBase-SR/ 25GBase-SR					
C	MM Fiber	Sensor Transmit 2	Sensor	10GBase-SR/ 25GBase-SR	✓	✓	✓	✓	✓
D	MM Fiber	Sensor Receive 2	Platform	10GBase-SR/ 25GBase-SR					

Rule 13.5.3.5-3: Ethernet Channels shall transmit and receive at 850nm per IEEE 802.3-2008 for 10GBASE-SR applications. Conformance Methodology (I)

Rule 13.5.3.5-4: The sensor system SMPTE ST 297 Channels shall transmit low power SMPTE ST 292, SMPTE ST 424, SMPTE ST 2081, or SMPTE ST 2082 signals at 1310nm specifically according to call out L-PC-CD-1310. Conformance Methodology (I)

Rule 13.5.3.5-5: Fiber optic shall be multi-mode fiber. The core diameter shall be $50\mu\text{m} \pm 3\mu\text{m}$ and the cladding diameter shall be $125\mu\text{m} \pm 2\mu\text{m}$. Conformance Methodology (I)

Rule 13.5.3.5-6: The termini shall be MIL-PRF-29504/4 (Pin) or MIL-PRF-29504/5 (Socket) which fit into size 16 entry holes. Conformance Methodology (I)

Rule 13.5.3.5-7: MM Fiber per ARINC 802-3. Fiber core size and bandwidth shall be matched for optimum performance for aramid reinforced 1.8 mm fiber optic cable. Conformance Methodology (I, A)

Rule 13.5.3.5-8: Fiber used shall be OM2-compliant or better, as defined by ISO/IEC 11801. Conformance Methodology (I)

Rule 13.5.3.5-9: Fiber Optic 1.8 mm simplex cabling reinforced with aramid strength member shall be per ARINC 802-3. Fiber core size and bandwidth shall be matched for optimum performance. Conformance Methodology (I, A)

13.5.3.6 *Class 3 Sensor J5-GPS Antenna Connector*

Rule 13.5.3.6-1: When a GPS receiver internal to the sensor system is used and requires an external antenna, the J5 GPS Antenna connector shall be used. Conformance Methodology (I)

Rule 13.5.3.6-2: The J5 GPS Antenna connector shall use GPS signals that conform to SAE AS6129 §A.6 (Sensor Requirements). Conformance Methodology (I)

Rule 13.5.3.6-3: The J5 GPS Connector shall use MIL-STD-348B (w/Change 3) TNC connectors. Conformance Methodology (I)

Table 13.5.3.6-1: J5-GPS Connector Pin Allocation

SOSA Electrical Interface									
J5-GPS Ant (TNC)									
Sensor – Receptacle					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Platform Umbilical – Plug									
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Coaxial	Coax-50Ω	GPS Antenna	Platform	RF	✓	✓	✓	✓	✓

13.5.3.7 Class 3 Sensor J6-DC Auxiliary Power Connector

Rule 13.5.3.7-1: The J6 DC Auxiliary Power connector shall use a 19-11 insert pattern shown in Figure 13.5.3.7-1. Conformance Methodology (I)

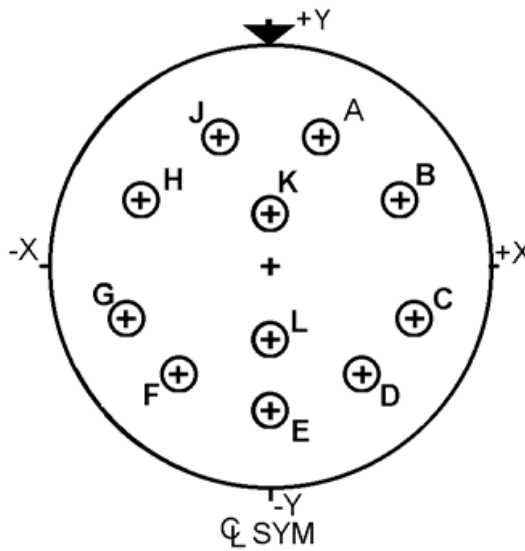


Figure 13.5.3.7-1: J6-DC Auxiliary Power Connector Pin Arrangement

Table 13.5.3.7-1: J6-DC Auxiliary Power Connector Pin Allocation

SOSA Electrical Interface J6-DC Auxiliary Power (19-11 insert, A-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**F11PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*F11SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
28VDC	D	SC-AWG16	DC-1	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	E	SC-AWG16	DC-1 RTN	Platform	DC RTN					
28VDC	F	SC-AWG16	DC-2	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	L	SC-AWG16	DC-2 RTN	Platform	DC RTN					
28VDC	C	SC-AWG16	DC-3	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	G	SC-AWG16	DC-3 RTN	Platform	DC RTN					
Safety Ground	K	SC-AWG16	Chassis	Platform	Ground	✓	✓	✓	✓	✓
28VDC	A	SC-AWG16	DC-4	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	J	SC-AWG16	DC-4 RTN	Platform	DC RTN					
28VDC	B	SC-AWG16	DC-5	Platform	28V DC@10A	✓	✓	✓	✓	✓
Return	H	SC-AWG16	DC-5 RTN	Platform	DC RTN					

13.5.3.7.1 Power

Rule 13.5.3.7.1-1: Where a J6 Power Connector pair is used, the allowable inrush current at each ‘+28VDC/RTN’ pair shall be specified by the procuring activity. Conformance Methodology (I)

Recommendation 13.5.3.7.1-1: The ‘+28VDC/RTN’ pin pairs included in the J1 connector should be utilized prior to those in J6. When J6 is used, the ‘+28VDC/RTN’ pin pairs should start with the lowest numbered pair, continuing in increasing order. Conformance Methodology (I)

Rule 13.5.3.7.1-2: Where a J6 Power Connector pair is used, the allowable inrush current at each ‘+28VDC/RTN’ pair shall be specified by the procuring activity.

Rule 13.5.3.7.1-3: When the inrush timing limitation is exceeded, the nominal current input to any ‘+28VDC/RTN’ pair shall not exceed 10A per Table 13.5.3.7-1. Conformance Methodology (A, T)

Observation 13.5.3.7.1-1: The ‘+28VDC/RTN’ pair inrush limit could be accomplished by the platform.

Rule 13.5.3.7.1-4: The sensor system's J6-DC Power connector shall accept +28 VDC power on any combination of the '+28VDC/RTN' pin pairs listed in Table 13.5.3.7-1. Conformance Methodology (I)

Recommendation 13.5.3.7.1-2: The '+28VDC/RTN' pin pairs included in the J1 connector should be utilized prior to those in J6. When J6 is used, the '+28VDC/RTN' pin pairs should start with the lowest numbered pair, continuing in increasing order.

Observation 13.5.3.7.1-2: Where more than 10A (nominal) current of +28VDC power is required to the sensor, the J6-DC Power connector's +28 VDC and RTN pairs (as identified in Table 13.5.3.7-1) could be connected in parallel, up to a maximum of 5 pairs. Conformance Methodology (I)

Rule 13.5.3.7.1-5: The nominal current input to any '+28VDC/RTN' pair shall not exceed 10A per Table 13.5.3.7-1. Conformance Methodology (A, T)

Rule 13.5.3.7.1-6: The sensor chassis shall exhibit $\geq 1M\Omega$ isolation to any J6 connector power returns. Conformance Methodology (I)

13.5.3.7.2 Safety Ground

Rule 13.5.3.7.2-1: The J6 Auxiliary DC Power connector Safety Ground shall connect between the sensor system ground contact and the sensor system chassis with a resistance of $\leq 0.1 \Omega$ in accordance with MIL-STD-1310 §3.20. Conformance Methodology (I)

13.5.3.8 Class 3 Sensor J7-High Speed Electrical Connector

Observation 13.5.3.8-1: When commercial protocols are routed through connector J7, pin out and nomenclature in this document are based upon the commercial standard but could vary slightly as required to maintain signal and ground paths and preserve signal integrity.

The J7-High Speed Connector supports electrical interfaces such as 10Gig Ethernet, USB 3.0, SATA, and DisplayPort.

Rule 13.5.3.8-1: The J7 High Speed Electrical connector shall have a pin arrangement in Figure 13.5.3.8-1. Conformance Methodology (I)

Rule 13.5.3.8-2: The J7 High Speed Electrical connector shall assign pins in accordance with Table 13.5.3.8-1. Conformance Methodology (I)

Size17 Mapping: Pigtail Plug common grounds



Figure 13.5.3.8-1: J7-High Speed Electrical Connector Pin Arrangement

Table 13.5.3.8-1: J7-High Speed Electrical Pin Allocations

<p>SOSA Electrical Interface J7-High Speed Electrical (VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length, or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritex part number or equivalent</p>						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
10Gig Ethernet	B3	100Ω STP – AWG 24, CAT 6A SAE AS6070/6	DA+	Platform/ Sensor	10GBaseT	✓	✓	✓	✓	✓
	B4		DA-							
	B5		DA Shield							
	C2		DB+							
	C3		DB-							

SOSA Electrical Interface										
J7-High Speed Electrical (VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length, or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	C4		DB Shield							
	C5		DC+							
	C6		DC-							
	C7		DC Shield							
	C8		DD+							
	C9		DD-							
	C10		DD Shield							
USB 3.0/2.0	E8	100 Ohm STP 2419	USB3_SS_TX +	Sensor	USB3.X Tx DATA	✓	✓	✓	✓	✓
	E9		USB3_SS_TX-							
	E7	SC-AWG24	USB3_GND_DRAIN							
	E5	100 Ohm STP 2419	USB3_SS_RX +	Platform	USB3.X Rx DATA					
	E6		USB3_SS_RX-							
	F9	100 Ohm STP 2419	USB2_D-	Sensor/ Platform	USB 2.X Data	✓	✓	✓	✓	✓
	F8		USB2_D+							
	F11	AWG24	USB_PWR	Sensor	USB Power	✓	✓	✓	✓	✓
	F10	AWG24	USB_GND							
	E10	AWG24	USB_SHLD		Shield	✓	✓	✓	✓	✓
Display Port	E2	AWG24	+3.3V	Sensor	Display Port	✓	✓	✓	✓	✓
	E4	AWG24	+3.3V_RTN							
	E11	100 Ohm	AUX+							

SOSA Electrical Interface										
J7-High Speed Electrical (VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length, or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	E12	STP 2419	AUX-							
	C11	AWG24	CONFIG1							
	C12	AWG24	CONFIG2							
	E13	SHIELD	GND							
	E3	AWG24	HOTPLUG							
	D3	100 Ohm STP 2419	LANE0-							
	D4		LANE0_SHIELD							
	D2		LANE0+							
	D6	100 Ohm STP 2419	LANE1-							
	D7		LANE1_SHIELD							
	D5		LANE1+							
	D9	100 Ohm STP 2419	LANE2-							
	D10		LANE2_SHIELD							
	D8		LANE2+							
	D12	100 Ohm STP 2419	LANE3-							
	D13		LANE3_SHIELD							
	D11		LANE3+							
SATA	A5	100Ω STP 2419	DA Shield		SATA	✓	✓	✓	✓	✓
	A6		A+	Sensor						
	A7		A-							

SOSA Electrical Interface J7-High Speed Electrical (VITA 76.0 #17 shell, N-keying) Sensor: 985217*N**** Receptacle, Size 17, N keying Choose Jam Nut/Flange, Press Fit /Solder, Low/High Profile, Plating Finish, Tail Length Platform Umbilical: 985017*N**** Plug, Size 17, N keying Choose Straight/Angle end 1&2, Plating Finish, Cable Gauge, Length, or contact for specific options Fields noted (*) are implementer's discretion The Shell Plating on the Receptacle and the Plug shall be the same plating The requirements of v76.0 are met by a Meritec part number or equivalent						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	A8	Shield	Shield							
	A9	100Ω STP 2419	B+	Platform						
	A10		B-							
	A11		DB Shield							
Serial	F5	100Ω STP 2419	Serial_TX	Sensor	TIA 232	✓	✓	✓	✓	✓
	F7		Serial_RTN							
	F6		Serial_RX	Platform						
Write Enable	B12	AWG24	WR_EN	Sensor	Switch Closure	✓	✓	✓	✓	✓
	B13	AWG24	WR_EN_RTN							
Digital Ground	B2 B8 B11 C1 C13 D1 F4					✓	✓	✓	✓	✓
Spare SE	A4									
Spare DP	B6 B7									
Spare DP	B9 B10									

13.5.3.8.1 10G Ethernet (Copper)

Rule 13.5.3.8.1-1: The J7 High Speed Electrical connector shall implement IEEE 802.3an-2006 for 10GBase-T service. Conformance Methodology (I)

13.5.3.8.2 USB 3.1/2.0

Rule 13.5.3.8.2-1: The J7 High Speed Electrical connector shall implement a USB interface per USB 3.1 G2. Conformance Methodology (I)

Rule 13.5.3.8.2-2: The J7 High Speed Electrical Interface shall be backwards-compatible with USB 2.0. Conformance Methodology (I)

13.5.3.8.3 Display Port

Rule 13.5.3.8.3-1: The J7 High Speed Electrical connector shall implement DisplayPort 1.3. Conformance Methodology (I)

13.5.3.8.4 SATA

Rule 13.5.3.8.4-1: The J7 High Speed Electrical connector shall implement a SATA interface per SATA Gen 3.0. Conformance Methodology (I)

13.5.3.8.5 Serial Communications

Rule 13.5.3.8.5-1: The J7 High Speed Electrical Connector Serial port shall be compliant to TIA 232. Conformance Methodology (I)

13.5.3.8.6 Write Enable

Observation 13.5.3.8.6-1: Write Enable is available for use as a maintenance function where it is desired to limit writing to non-volatile memory only during system maintenance periods.

Rule 13.5.3.8.6-1: When writing to non-volatile memory, the J7 High Speed Electrical connector shall implement an external switch to close WR_EN and WR_EN_RTN together. Conformance Methodology (I)

Rule 13.5.3.8.6-2: The J7 High Speed Electrical connector shall enable write when the WR_EN and WR_EN_RTN circuit is closed. Conformance Methodology (I)

13.5.3.9 Class 3 Sensor J8-High Density RF Connector

Rule 13.5.3.9-1: Where required, the sensor system shall utilize a high-density RF connection between sensor elements as defined in Table 13.5.3.9-1. Conformance Methodology (I)

Rule 13.5.3.9-2: The J8 High Density RF Connector shall use a 21-11 insert pattern shown in Figure 13.5.3.9-1. Conformance Methodology (I)

Rule 13.5.3.9-3: The J8 High Density RF Connector shall assign pins in accordance with Table 13.5.3.9-1. Conformance Methodology (I)

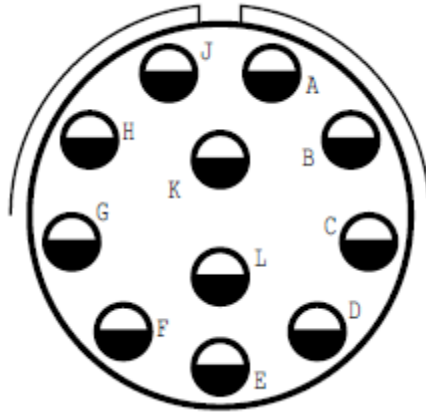


Figure 13.5.3.9-1: J8-RF Connector Pin Arrangement

Table 13.5.3.9-1: J8-RF Connector Pin Allocations

SOSA Electrical Interface J8-RF (21-11 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted per description below Sensor MIL-DTL-38999/**G11SN-LC (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*G11PN-LC (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
RF	A	Coax-50Ω	Ch1	Antenna	RF up to 50GHz		✓	✓	✓	✓
	B	Coax-50Ω	Ch2	Antenna	RF up to 50GHz		✓	✓	✓	✓
	C	Coax-50Ω	Ch3	Antenna	RF up to 50GHz		✓	✓	✓	✓
	D	Coax-50Ω	Ch4	Antenna	RF up to 50GHz		✓	✓	✓	✓
	E	Coax-50Ω	Ch5	Antenna	RF up to 50GHz		✓	✓	✓	✓
	F	Coax-50Ω	Ch6	Antenna	RF up to 50GHz		✓	✓	✓	✓
	G	Coax-50Ω	Ch7	Antenna	RF up to 50GHz		✓	✓	✓	✓
	H	Coax-50Ω	Ch8	Antenna	RF up to 50GHz		✓	✓	✓	✓
	J	Coax-50Ω	Ch9	Antenna	RF up to 50GHz		✓	✓	✓	✓
	K	Coax-50Ω	Ch10	Antenna	RF up to 50GHz		✓	✓	✓	✓
	L	Coax-50Ω	Ch11	Antenna	RF up to 50GHz		✓	✓	✓	✓

Rule 13.5.3.9-4: The J8 High Density RF connector receptacle shall utilize a MIL-DTL-38999 size 12 socket per SAE AS39029/56 with an SMPM pin interface. Conformance Methodology (I)

Rule 13.5.3.9-5: The J8 High Density RF connector SMPM pin interface dimensions shall conform to MIL-STD-348B (w/Change 3), in Figure 13.5.3.9-2. Conformance Methodology (I)

Rule 13.5.3.9-6: The J8 High Density RF connector receptacle SMPM pin and socket interface shall conform to MIL-STD-348B, Figure 313-2 (w/Change 3), in Figure 13.5.3.9-2. Conformance Methodology (I)

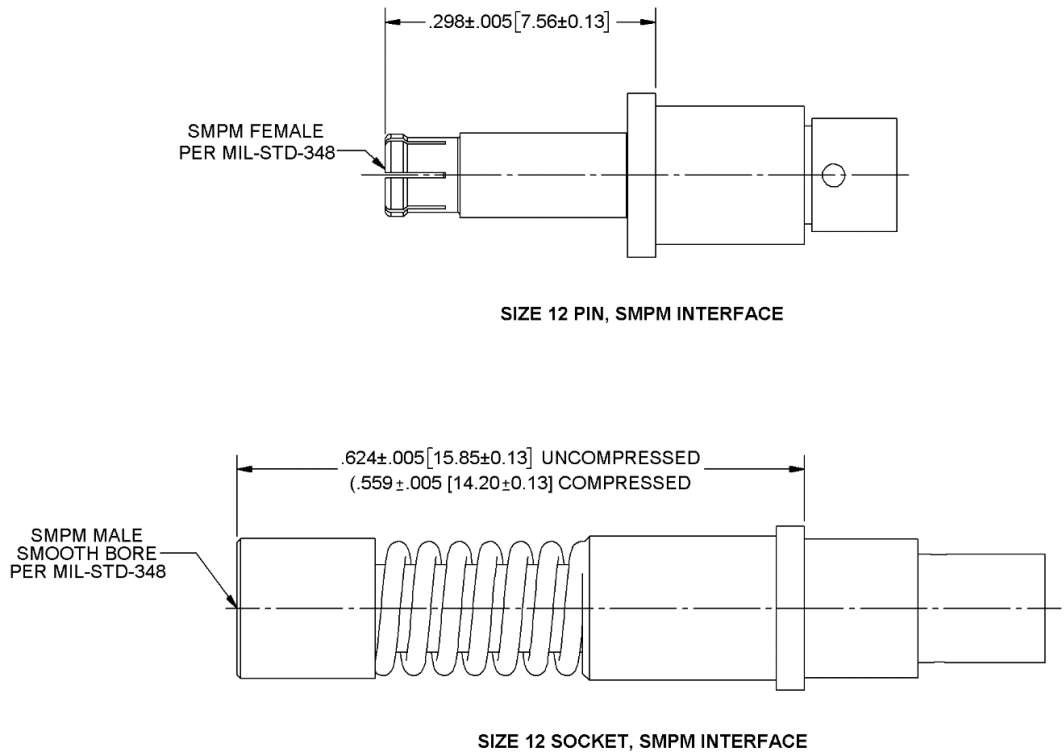


Figure 13.5.3.9-2: Size 12 Pin and Socket

13.5.3.9.1 High Density RF Performance Testing

Rule 13.5.3.9.1-1: The J8 High Density RF Connector size 12 mated pairs shall meet VSWR requirements per Table 13.5.3.9.1-1. Conformance Methodology (I)

Table 13.5.3.9.1-1: Size 12 Connector Frequency Range and VSWR Requirements

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
DC-18 GHz	1.25:1
18-26.5 GHz	1.30:1
26.5-40 GHz	1.40:1

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
40-50 GHz	1.60:1

13.5.3.10 Class 3 Sensor J9-Low Loss RF Connector

Rule 13.5.3.10-1: When a low loss RF connection is required, the J9 Low Loss RF Connector shall use values defined in Table 13.5.3.10-1. Conformance Methodology (I)

Rule 13.5.3.10-2: The J9 Low Loss RF Connector shall use a 25-8 insert pattern shown in Figure 13.5.3.10-1. Conformance Methodology (I)

Rule 13.5.3.10-3: The J9 Low Loss RF Connector shall assign pins in accordance with Table 13.5.3.10-1. Conformance Methodology (I)

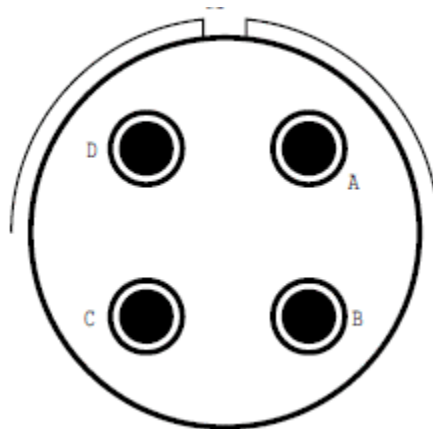


Figure 13.5.3.10-1: J9-Low Loss RF Connector Pin Arrangement

Table 13.5.3.10-1: J9-Low Loss RF Connector Pin Allocation

SOSA Electrical Interface J9-RF (21-75 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Connectors are ordered without contacts and coax contacts inserted per description below Antenna MIL-DTL-38999/**G75SN-LC (receptacle with socket inserts) Platform Umbilical MIL-DTL-38999/26*G75PN-LC (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
RF	A	Coax-50Ω	Ch1	Antenna	RF up to 22GHz		✓	✓	✓	✓
	B	Coax-50Ω	Ch2	Antenna	RF up to 22GHz		✓	✓	✓	✓
	C	Coax-50Ω	Ch3	Antenna	RF up to 22GHz		✓	✓	✓	✓
	D	Coax-50Ω	Ch4	Antenna	RF up to 22GHz		✓	✓	✓	✓

Rule 13.5.3.10-4: The J9 Low Loss RF Connector shall utilize a MIL-DTL-38999 size 8 socket per SAE AS39029/59 with a BMB pin interface. Conformance Methodology (I)

Rule 13.5.3.10-5: The J9 Low Loss RF Connector BMB pin dimensions (in Figure 13.5.3.10-2) shall conform to MIL-STD-348B (w/Change 3). Conformance Methodology (I)

Rule 13.5.3.10-6: The J9 Low Loss RF Connector BMB pin and socket interface shall conform to Figure 13.5.3.10-2. Conformance Methodology (I)

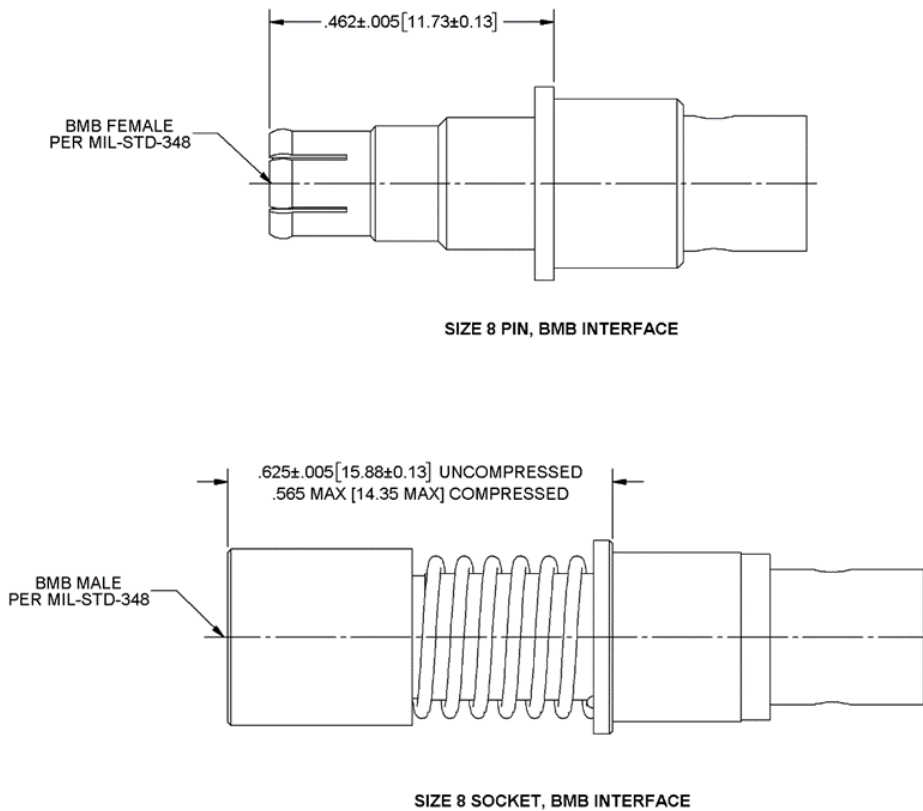


Figure 13.5.3.10-2: Size 8 Pin and Socket

13.5.3.10.1 Low Loss RF Performance Testing

Rule 13.5.3.10.1-1: The J9 Low Loss RF Connector mated pairs shall meet the VSWR requirements in Table 13.5.3.10.1-1. Conformance Methodology (I)

Table 13.5.3.10.1-1: Size 8 Connector Frequency Range and VSWR Requirements

Frequency Range (may be cable-limited)	VSWR MAX. Gated, Mated Pair
DC-22 GHz	1.40:1

13.5.3.11 Class 3 Sensor Auxiliary RF Connectors

Rule 13.5.3.11-1: When high-frequency discrete signals are required, the Auxiliary RF Connector shall use pin assignments in Table 13.5.3.11-1. Conformance Methodology (I)

Table 13.5.3.11-1: Auxiliary RF Connections

Auxiliary RF Connectors – Quantity is Application-Specific						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
TNC		RG142 50Ω		Antenna	RF up to 3 GHz	✓	✓	✓	✓	✓
SMA		RG174 50Ω		Antenna	RF up to 27 GHz		✓	✓	✓	✓
2.4 mm		Coax-50Ω		Antenna	RF up to 50 GHz		✓	✓	✓	✓
1.0 mm		Coax-50Ω		Antenna	RF up to 110 GHz		✓	✓	✓	✓

13.5.3.12 Class 3 Sensor J11 – High Voltage DC Power Connector

Rule 13.5.3.12-1: Where required, the Sensor System J11 High Voltage DC Power Connector shall have a 11-5 insert pattern as shown in Figure 13.5.3.12-1. Conformance Methodology (I)

Rule 13.5.3.12-2: Signals for the J11 High Voltage DC Connector shall be assigned to pins in accordance with Table 13.5.3.12-1. Conformance Methodology (I)

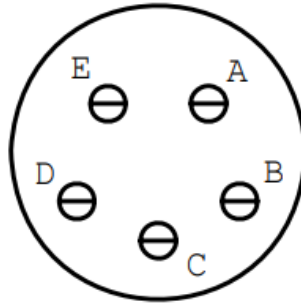


Figure 13.5.3.12-1: J11 High Voltage DC Connector Pin Arrangement

Table 13.5.3.12-1: J11 High Voltage DC Power Pin Allocations

SOSA Electrical Interface J11 High Voltage DC Power (11-5 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**B5PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*B5SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
270VDC	A	SC-AWG20	HVDC-1	Platform	270VDC@5A	✓	✓	✓	✓	✓

SOSA Electrical Interface J11 High Voltage DC Power (11-5 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**B5PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*B5SN (plug with sockets inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
	B	SC-AWG20	HVDC-1_RTN	Platform	270VDC RTN	✓	✓	✓	✓	✓
Safety Ground	C	SC-AWG20	Chassis Ground	Common	Ground	✓	✓	✓	✓	✓
Reserved	D,E		Reserved		Safety Interlock	✓	✓	✓	✓	✓

13.5.3.12.1 Power

Rule 13.5.3.12.1-1: Where utilized, the sensor system shall accept 270VDC power in accordance with one or more of the applicable standards per Table 13.5.3.2-1, at the pins listed in Table 13.5.4.3-1. Conformance Methodology (I)

Rule 13.5.3.12.1-2: Where a J11 Power Connector is used, the allowable inrush shall be specified by the procuring activity. Conformance Methodology (T)

Rule 13.5.3.12.1-3: The sensor shall isolate power returns from the chassis. Conformance Methodology (I)

13.5.3.12.2 Safety Ground

Rule 13.5.3.12.2-1: The sensor system ground contact shall be used to provide electrical continuity to the sensor system chassis in accordance with MIL-STD-1310 §3.20. Conformance Methodology (I)

13.5.3.12.3 Connectivity Materials and Wire Type

Recommendation 13.5.3.12.3-1: When enabling 270 VDC, power systems should incorporate polyimide-free SAE AS22759/70/75 wire types to prevent arc track events and potential fires caused by dielectric breakdown or damage. Conformance Methodology (I)

Recommendation 13.5.3.12.3-2: When considering connector contacts and wire compatibility, the design authority should evaluate wire size, termination, and environmental conditions to suppress corona. Conformance Methodology (A)

13.5.3.13 Class 3 Sensor J12 – Key Fill Connector, Non-GPS Devices

Rule 13.5.3.13-1: Where a DS-101 Interface is used to distribute security keys or similar data to non-GPS elements in the sensor, the sensor system shall employ a J12 chassis-mounted Key Fill Connector (NSA P/N 0N241775 or equivalent) in accordance with EKMS 308, as shown in Figure 13.5.3.13-1. Conformance Methodology (I)

Rule 13.5.3.13-2: When the J12 Key Fill Connector is used, the shell of the J12 connector shall make electrical contact with the sensor system chassis for grounding in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

Rule 13.5.3.13-3: The J12 Key Fill Connector signals shall be assigned to pins in accordance with Table 13.5.3.13-1. Conformance Methodology (I)

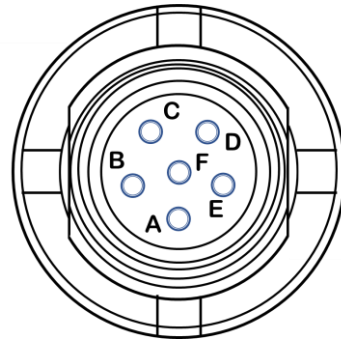


Figure 13.5.3.13-1: J12 Key Fill Connector Pin Arrangement

Table 13.5.3.13-1: J12 Key Fill Connector Pin Out Details

SOSA Electrical Interface J12 DS101 Key Fill Connector (non-GPS) NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Reference	A	Logic Reference	Reference	✓	✓	✓	✓	✓
Signal	B	Differential Side A (+)	TIA 485-A	✓	✓	✓	✓	✓
Signal	C	Wake Up	Logic	✓	✓	✓	✓	✓
Reserved	D	NC	N/A					
Signal	E	Differential Side B (-)	TIA 485-A	✓	✓	✓	✓	✓
Reserved	F							

Rule 13.5.3.13-4: The J12 Key Fill Connector electrical signals for connector positions B and E shall be differential lines in accordance with the EKMS 308 TIA 485-A Interface. Conformance Methodology (I)

Rule 13.5.3.13-5: Where a Wake-Up capability is supported, the J12 Key Fill Connector shall activate the Key Fill Interface upon detection of a Wake-Up signal from a ground in accordance with the EKMS 308 Interface. Conformance Methodology (I)

13.5.3.14 Class 3 Sensor J13 – Key Fill Connector, GPS Devices

Rule 13.5.3.14-1: Where a DS-101 Interface is used to distribute security keys or similar data to GPS devices within the sensor, the sensor system shall employ a J13 chassis mounted Key Fill

Connector (NSA P/N 0N241775 or equivalent) in accordance with EKMS 308 as shown in Figure 13.5.3.14-1. Conformance Methodology (I)

Rule 13.5.3.14-2: When the J13 Key Fill Connector is used, the shell of the J13 connector shall make electrical contact with the sensor system chassis for grounding in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

Rule 13.5.3.14-3: The J13 Key Fill Connector signals shall be assigned to pins in accordance with Table 13.5.3.14-1. Conformance Methodology (I)

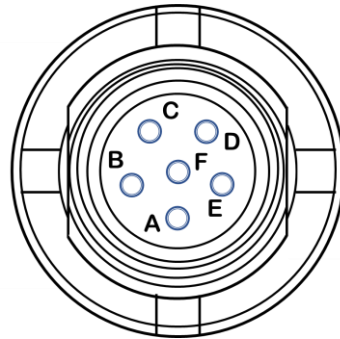


Figure 13.5.3.14-1: J13 Key Fill Connector Pin Arrangement

Table 13.5.3.14-1: J13 Key Fill Connector Pin Arrangement

SOSA Electrical Interface J13 DS101 Key Fill Connector (GPS only) NSA P/N 0N241775 Connector P/N U-283 (Mating Connector – NSA P/N 0N241774)				EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Signal Name	Signal Type	Used	Used	Used	Used	Used
Reference	A	GND	Reference	✓	✓	✓	✓	✓
Signal	B	RTS	TIA 232	✓	✓	✓	✓	✓
Signal	C	RX	TIA 232	✓	✓	✓	✓	✓
Signal	D	TX	TIA 232	✓	✓	✓	✓	✓
Signal	E	CTS	TIA 232	✓	✓	✓	✓	✓
Reserved	F							

Rule 13.5.3.14-4: The J13 Key Fill Connector electrical signals for connector positions C and D shall be single-ended lines in accordance with the EKMS 308 TIA 232 Interface. Conformance Methodology (I)

Rule 13.5.3.14-5: Signal position E is for Clear to Send for TIA 232 Protocol for the SOSA sensor’s Key Fill Activity. Signal position B is for Request to Send supporting the TIA 232 Interface in accordance with EKMS 308 for the SOSA sensor’s Key Fill Activity. Conformance Methodology (I)

13.5.3.15 *Class 3 Sensor J14 – Circular High-Density MT Connectors*

13.5.3.15.1 Common Rules for Circular High-Density MT Connectors

Rule 13.5.3.15.1-1: The Circular High-Density MT connectors shall comply with the following set of rules:

- Rule 13.5.3.5-3 Conformance Methodology (T)
- Rule 13.5.3.5-9 Conformance Methodology (I)
- Rule 13.5.2.16.1-2 Conformance Methodology (I)
- Rule 13.5.2.16.1-3 Conformance Methodology (T)
- Rule 13.5.2.16.1-4 Conformance Methodology (T)

13.5.3.15.2 Class 3 Sensor J14 Connector

Rule 13.5.3.15.2-1: The sensor system fiber J14 shall comply with the set of common rules defined in Rule 13.5.3.15.1-1. Conformance Methodology (I)

Rule 13.5.3.15.2-2: J14 High Density Fiber Connector shall have MT arrangement as shown in Figure 13.5.3.15.2-1. Conformance Methodology (I)

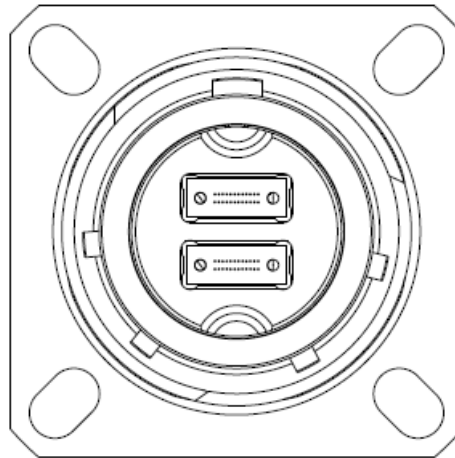


Figure 13.5.3.15.2-1: J14 High Density Fiber Connector (2 MT)

13.5.3.16 *Class 3 Sensor J15 – Circular High-Density MT Connectors*

Observation 13.5.3.16-1: Where the sensor requires to interconnect 24 optical fibers or less, connector J15 could be used.

Rule 13.5.3.16-1: The sensor system fiber J15 shall comply with the set of common rules defined in Rule 13.5.3.15.1-1. Conformance Methodology (I)

Rule 13.5.3.16-2: J15 High Density Fiber Connector shall have MT arrangement as shown in Figure 13.5.3.16-1. Conformance Methodology (I)

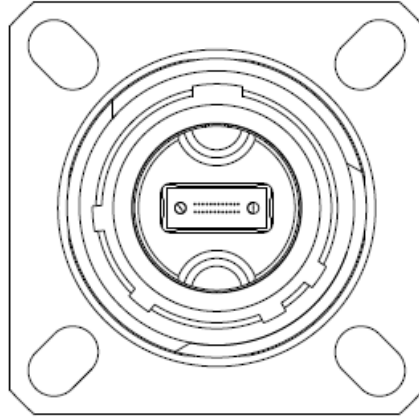


Figure 13.5.3.16-1: J15 High Density Fiber Connector (1 MT)

13.5.3.17 *Class 3 Sensor J16 – External Battery Connectors*

Rule 13.5.3.17-1: Where required, the sensor system J16 External Battery Connector shall have a 9-35 insert pattern with 6 contacts as shown in Figure 13.5.3.17-1. Conformance Methodology (I)

Rule 13.5.3.17-2: Signals for the sensor system J16 External Battery Connector shall be assigned to pins in accordance with Table 13.5.3.17-1. Conformance Methodology (I)

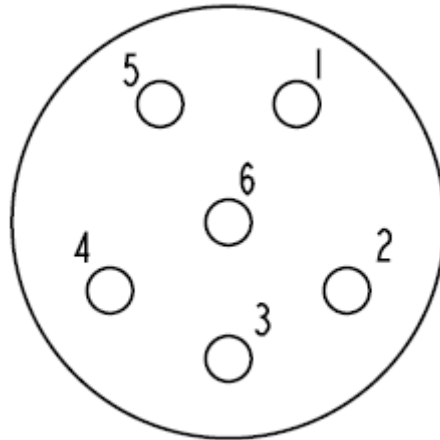


Figure 13.5.3.17-1: J16-External Battery Connector Pin Arrangement

Table 13.5.3.17-1: J16 External Connector Pin Arrangement

J16-VBAT (9-35 insert, N-Keying) For Part Numbers insert receptacle choice (20 or 24) and relevant plating finish Sensor MIL-DTL-38999/**A35PN (receptacle with pin inserts) Platform Umbilical MIL-DTL-38999/26*A35SN (plug with sockets inserts)						EO-IR Sensor	Radar/SA R Sensor	EW Sensor	SIGINT Sensor	Communi cations
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
EXT VBAT	1	AWG22	V_BATT	Platform	3.3VDC	✓	✓	✓	✓	✓
	5	AWG22	V_BATT_RTN	Platform	DC Return					
EXT ALT_V BAT	3	AWG22	ALT_V_BATT	Platform	3.9VDC	✓	✓	✓	✓	✓
	4	AWG22	ALT_V_BATT _RTN	Platform	DC Return					
Reserve	2									
	6									

13.5.3.17.1 VBAT Battery Power

Rule 13.5.3.17.1-1: The sensor system J16 shall support a low current battery power input to be provided by the platform to hold up services such as volatile memory and real-time clocks over power cycles. The maximum voltage is 3.5 VDC with a maximum current of 115 mA. Conformance Methodology (I)

13.5.3.17.2 ALT_VBAT Battery Power

Rule 13.5.3.17.2-1: The sensor system J16 shall support a low current battery power input to be provided by the platform to hold up services such as key fill devices over power cycles. The maximum voltage is 3.9 VDC with a maximum current of 115 mA. Conformance Methodology (I)

13.5.4 SOSA Class 5 Electrical Mechanical Interfaces

Class 5 end applications could be implemented as either a hardware sensor element or a top-level SOSA sensor. As such, this section will refer to “Class 5 devices” to generalize where that differentiation is not specifically required.

Class 5 devices are typically mounted on small expendable, fixed-winged platforms often referred to as Small Unmanned Aerial Systems (SUAS) and launched from a Common Launch Tube (CLT). Due to the small size, low weight, and cost goals, this class of sensor will utilize a single connector for power and signals. Due to the Class 5 device mounting scheme, and widely adopted commercial use, a D-Sub style connector is most appropriate.

13.5.4.1 Class 5 Types

Observation 13.5.4.1-1: Class 5 devices’ form factors are space-limited, and as such an all-encompassing electrical interface type is prohibitive. Thus, this section is present for the purpose of tracking the unique Class 5 types and defining which connectors are required for those types.

Only Class 5 devices of EO-IR type are included. If any type does not match a currently defined type with a Rule, a new Rule would be added to this section to properly associate the required connector to that type.

Rule 13.5.4.1-1: Where the Class 5 device is an EO-IR type, that device shall include a Class 5 J1 connector. Conformance Methodology (I)

13.5.4.2 *Class 5 J1 Connector*

Rule 13.5.4.2-1: The Class 5 J1 connector shall be a 25 pin Micro-D type connector with an electro-mechanical interface equivalent to and interoperable with that of MIL-DTL-83513/02-DN (receptacle with socket inserts) on the Class 5 device, conforming to all subsections of MIL-DTL-83513H §4.4. Conformance Methodology (I)

Rule 13.5.4.2-2: The Class 5 device shall have clearance around the J1 connector to accept a host platform umbilical equivalent to and interoperable with that of MIL-DTL-83513/01-DN plug with pin inserts), conforming to all subsections of MIL-DTL-83513H §4.4. Conformance Methodology (I)

Rule 13.5.4.2-3: The Class 5 J1 connector shall utilize the signal pin assignments in accordance with Table 13.5.4.2-1 per the pattern shown in Figure 13.5.4.2-1. Conformance Methodology (I)

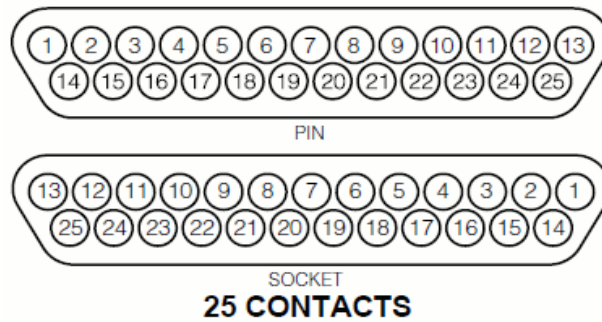


Figure 13.5.4.2-1: Class 3 J1 Pin Assignments

Table 13.5.4.2-1: Class 3 J1 Pin Locations

SOSA Electrical Interface										
Class 5 J1 connector – Micro-D type										
Sensor Device MIL-DTL-83513/02-DN (receptacle with socket inserts)										
Platform Umbilical MIL-DTL-83513/01-DN (plug with pin inserts)						EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Input Power	1	28AWG	PWR_IN	Host Platform/Hardware Processing Element	24V	✓				✓
	2		PWR_IN			✓				✓
	3		PWR_IN			✓				✓
	4		PWR_IN			✓				✓

SOSA Electrical Interface Class 5 J1 connector – Micro-D type Sensor Device MIL-DTL-83513/02-DN (receptacle with socket inserts) Platform Umbilical MIL-DTL-83513/01-DN (plug with pin inserts)						EO-IR Sensor	Radar/ SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Power Return	14	28AWG	PWR_RTN	Host Platform/Hardware Processing Element	24V	✓				✓
	15		PWR_RTN			✓				✓
	16		PWR_RTN			✓				✓
	17		PWR_RTN			✓				✓
Ethernet	5	100Ω UTP – AWG 24, CAT 5e, SAE AS6070/6 recommended	ETH_TX_DP	Sensor/Hardware Sensor Element	100BaseT (Optional 1000BaseT)	✓				✓
	6		ETH_TX_DM			✓				✓
	7		ETH_RX_DP	Host Platform/Hardware Processing Element		✓				✓
	8		ETH_RX_DM			✓				✓
Ethernet	18	100Ω UTP – AWG 24, CAT 5e, SAE AS6070/6 recommended	ETH_C_DP	Host Platform/Sensor Or Hardware Processing/Sensor Elements	Optional 1000BaseT	✓				✓
	19		ETH_C_DM			✓				✓
	20		ETH_D_DP			✓				✓
	21		ETH_D_DM			✓				✓
Signal Bus' Common Mode Ground	9	28AWG	GND_SIGNAL	Sensor/Hardware Sensor Element	Sensor Elec Interface's CM Ground	✓				✓
Serial	10	28AWG	RS485_Y (TX_DP)	Sensor/Hardware Sensor Element	RS-485 (terminated @ receiver)	✓				✓
	11		RS485_Z (TX_DM)			✓				✓
	12		RS485_B (RX_DM)	Host Platform/Hardware Processing Element		✓				✓
	13		RS485_A (RX_DP)			✓				✓
User- defined pins	22	28AWG	USER_DEFIN ED_GPI_RTN	Host Platform/Hardware Processing Element	User-defined GPI	✓				✓
	23		USER_DEFIN ED_GPI			✓				✓

SOSA Electrical Interface Class 5 J1 connector – Micro-D type Sensor Device MIL-DTL-83513/02-DN (receptacle with socket inserts) Platform Umbilical MIL-DTL-83513/01-DN (plug with pin inserts)						EO-IR Sensor	Radar/ SAR Sensor	EW Sensor	SIGINT Sensor	Comms
Conn/ Desc.	Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Laser Arming	24	28AWG	LASER_ARM_ RTN	Sensor/Hardware Sensor Element (for signal bias)	open/closed switch (on Platform side)	✓				✓
	25		LASER_ARM			✓				✓
Chassis	Shell	Braid/foil/ drain wire	CHASSIS_SEN SOR	Sensor/Hardware Sensor Element	Safety Ground	✓				✓

13.5.4.2.1 Power

Rule 13.5.4.2.1-1: The Class 5 device shall accept a nominal 24 VDC power source at the power pins in Table 13.5.4.2-1. Conformance Methodology (T)

Rule 13.5.4.2.1-2: The Class 5 device shall limit inrush to 2.5 Amps for each power input pair utilized (for full 4 power pairs then 4x at 10 Amps) for 1 second. Conformance Methodology (T)

Rule 13.5.4.2.1-3: The Class 5 device shall operate without damage or permanent degradation to power input bus spikes and surges as specified in MIL-STD-704F, Figure 13, with testing from MIL-HDBK-704-8 Method LDC105 as outlined in MIL-STD-704F §6.10.1. Conformance Methodology (T)

Rule 13.5.4.2.1-4: The Class 5 device shall operate without damage or permanent degradation to power input bus distortion (noise and ripple) up to 1/10 of the absolute levels specified in MIL-STD-704F, Figure 15, with testing from MIL-HDBK-704-8 Method LDC103 as outlined in MIL-STD-704F §6.10.1. Conformance Methodology (T)

Rule 13.5.4.2.1-5: The Class 5 device shall isolate power returns from the chassis by not allowing direct electrical connections between the current nets and the chassis ground. Conformance Methodology (I)

Rule 13.5.4.2.1-6: When the host platform power cycles the Class 5 device, the Class 5 device shall restart and return to a communicating state without an operator’s physical interaction with the device. Conformance Methodology (D)

13.5.4.2.2 Safety Ground

Rule 13.5.4.2.2-1: The Class 5 device shall provide electrical continuity from its conductive chassis to the Host Platform’s safety ground over J1 connector’s shell, in accordance with MIL-STD-464C §5.11.3. Conformance Methodology (T)

13.5.4.2.3 Signal Ground

Rule 13.5.4.2.3-1: The Class 5 device shall connect its electrical signaling interface’s common mode ground reference to the Signal Ground pin found in Table 13.5.4.2-1. Conformance Methodology (I)

Observation 13.5.4.2.3-1: The host platform could connect its signal interfaces' common mode ground to this signal, if, for instance, those grounds are also isolated from power return. The host platform integrator determines the most appropriate use for the end application.

13.5.4.2.4 Ethernet Databus (Copper)

Rule 13.5.4.2.4-1: The Class 5 device shall support 10/100Mb Ethernet across J1's pins 5-8, as identified in Table 13.5.4.2-1, using 100Base-TX type signaling (see IEEE 802.3-2012 §24 and §25). Conformance Methodology (I)

Rule 13.5.4.2.4-2: Where the Class 5 device has made connections to all 8 Ethernet signals (4 twisted-pair) on the J1 connector, per Table 13.5.4.2-1, the Class 5 device shall support 1 Gbit Ethernet, using 1000Base-T signaling (see IEEE 802.3-2012 §22). Conformance Methodology (I)

Rule 13.5.4.2.4-3: The Class 5 device shall support auto-negotiation of the Ethernet link speed to the fastest common speed with the host platform, regardless of the Class 5 device's utilization of 4 or 8 Ethernet signals (see IEEE 802.3-2012). Conformance Methodology (I)

13.5.4.2.5 Serial Communications

Rule 13.5.4.2.5-1: The Class 5 device's J1 serial ports shall be compliant to TIA/EIA RS-485. Conformance Methodology (I)

13.5.4.2.6 User-Defined Pins

The Class 5 device has an application-specific input for flexibility with the variety of payloads and use-cases intending to use this form factor.

Rule 13.5.4.2.6-1: The Class 5 device shall define the permanent, or software-configurable, purpose of this input signal for the Host integrator to determine applicability. Conformance Methodology (I)

Options, but not a limiting list, are as follows:

- Unused
- GPS Pulse Per Second (PPS) Input
- Low-latency trigger (e.g., for video marking, for camera snapshot)
- Low-latency enable (e.g., for pulsing laser)

Rule 13.5.4.2.6-2: Where the Class 5 device implements the user-defined pins with a fixed purpose per unit, the Class 5 device shall be defined with a unique orderable part number to identify a product's pin functionality among other interoperable Class 5 sensor elements. Conformance Methodology (I)

Rule 13.5.4.2.6-3: Where the Class 5 device implements the user-defined pins as a software-definable signal, the Class 5 device shall include a published list of available functions and supply a UI for the Host integrator to reconfigure the signal definitions. Conformance Methodology (I)

Options for the UI from the device's supplier could be, but are not limited to:

- A configuration utility
- Software API

Rule 13.5.4.2.6-4: Where the Class 5 device does not specify the use or functionality for the user-defined pins and the Host has no use for the user-defined pins, the Class 5 device shall leave the user-defined pins disconnected. Conformance Methodology (I)

Recommendation 13.5.4.2.6-1: Where the Class 5 device does specify the use and functionality for the user-defined pins but the Host has no use for the user-defined pins, the Host should follow the Class 5 device vendor's requirements for safe termination of the pins. Conformance Methodology (I)

Recommendation 13.5.4.2.6-2: The Class 5 device should define this input signal's electrical signaling properties, functional purpose(s), and applicable functional timing characteristics. Conformance Methodology (I)

13.5.4.2.7 LASER Arming

Rule 13.5.4.2.7-1: Where a Class 5 device supports the LASER_ARM signal input (see Table 13.5.4.2-1), the Class 5 device shall source a maximum current of 100 mA on the arming signal pair when the circuit is closed. Conformance Methodology (T)

Rule 13.5.4.2.7-2: Where a Class 5 device supports the LASER_ARM signal input (see Table 13.5.4.2-1), the Class 5 device shall have a maximum arming signal pair open circuit DC voltage equivalent to the Input Power voltage. Conformance Methodology (T)

Rule 13.5.4.2.7-3: When, and while, the LASER_ARM and LASER_ARM_RTN signals (see Table 13.5.4.2-1) are not shorted together, the Class 5 device shall disable the power to, and keep the power off to, any of its human safety risk emission elements. Conformance Methodology (T)

Rule 13.5.4.2.7-4: When, and while, the LASER_ARM and LASER_ARM_RTN signals (see Table 13.5.4.2-1) are shorted together, the Class 5 device shall enable the power to, and keep the power on to, any of its human safety risk emission elements. Conformance Methodology (T)

Recommendation 13.5.4.2.7-1: Where a Class 5 device's laser sub-system requires low-latency, high-rate, or specific tight timing response to a host platform input signal, the Class 5 device supplier should implement that functionality via user-defined pins of the Class 5 J1 connector referenced in Table 13.5.4.2-1. Conformance Methodology (I)

13.5.4.3 Class 5 J2 GPS RF Connector

Rule 13.5.4.3-1: Where Class 5 device has an integrated GPS receiver and requires an external antenna, the Class 5 device shall use this SMA connector, in accordance with pin assignments in Table 13.5.4.3-1. Conformance Methodology (I)

Recommendation 13.5.4.3-1: Where Class 5 device has the J2 GPS RF connector, the Class 5 device should be operable with GPS signals that have characteristics that comply with SAE AS6129 §A.6 (Additional Interface Requirements for GPS RF Signals), either via direct RF connection or through an external RF distribution buffer that must be specified by the SOSA

Class 5 vendor. The buffer shall be included by the vendor during any conformance testing demonstrating compliance with SAE AS6129 §A.6. Conformance Methodology (T)

Observation 13.5.4.3-1: The small, embedded GPS receivers used in this turret class could be of a type that favors certain antennas over others. As such, a SOSA Class 5 vendor could want to publish their receiver’s recommended antenna list, or independently validate a list of antennas and/or GPS signal strengths, to enhance appeal of their Class 5 device to host platform integrators.

Table 13.5.4.3-1: J2 GPS Connector Pin Allocation

SOSA Electrical Interface Recommendations					EO-IR Sensor	Radar/SAR Sensor	EW Sensor	SIGINT Sensor	Comms
J2-GPS Ant (SMA)									
Sensor – Receptacle									
Platform Umbilical – Plug									
Pin	Wire Type	Signal Name	Signal Source	Signal Type	Used	Used	Used	Used	Used
Coaxial	Coax-50Ω	GPS Antenna	Host	RF	✓				✓

13.5.5 SOSA Aperture Mechanical Interface Standard

13.5.5.1 Mechanical Classes

The Interface Standard defined in this section provides testable rules and conformance testing approaches for the physical interface between the SOSA sensor and its host platform, as defined by the SV-1 in Section 4.1. The SOSA sensor’s physical electrical interfaces (Section 13.5.5) and sensor mechanical interfaces define the physical interface.

The aperture refers to sensing elements, represented primarily by SOSA modules 2.1, 2.2, and 2.3, which sense electromagnetic radiation from the environment. The electromagnetic radiation represents a boundary of the SOSA Reference Architecture, and the apertures are typically the first physical instantiation of a SOSA component at this boundary.

SOSA components can refer to a self-contained physical package attached to the host platform, such as a Pod. They can also refer to a distributed physical package, where the apertures and various other hardware elements are distributed throughout the host platform, internally or externally. The SOSA component’s physical package refers to either of these cases. In addition, the aperture has a physical package type: turreted, non-turreted but gimballed, non-gimballed, or pod based. Lastly, the aperture can accommodate one or several of the sensing modalities: Comms, EO/IR, EW, Radar, or SIGINT.

An aperture can be represented by a mechanical form factor, a package type, a sensing modality, or a combination thereof. To facilitate interchangeability of apertures on host platforms, this document provides rules to classify apertures by mechanical class.

Mechanical classes are defined by industry standards or this document where applicable. Table 13.5.5.1-1 defines the mechanical classes for all apertures. A SOSA mechanical class is defined by four physical attributes: shape, largest axis on its mounting, weight, and center of gravity (CG). The mechanical class names are based on a schema of the physical attributes: Shape-Largest Axis-CG-Weight. For example, mechanical class s-36-30-2100 refers to a square mounting, where the diagonal distance from corner-to-corner (the largest mounting axis) is

greater than 36[in], the center-of-gravity is less than or equal to 30[in], and the weight is less than or equal to 2100 [lbs].

Rule 13.5.5.1-1: A SOSA sensor shall be assigned a mechanical class based on Table 13.5.5.1-1. Conformance Methodology (I)

Table 13.5.5.1-1: SOSA Sensor Mechanical Classes

Mechanical Class	SOSA Sensor Physical Attributes			
	Shape*	Largest Axis on Mounting	Center of Gravity (CG)†	Weight
Mechanical Class X-36-30-2100	X = s, rh, re, c, l	> 36 in	≤ 30 in	≤ 2100 lbs
Mechanical Class X-29-24-1100	X = s, rh, re, c, l	> 29 in	≤ 24 in	≤ 1100 lbs
Mechanical Class X-23-18-500	X = s, rh, re, c, l	> 23 in	≤ 18 in	≤ 500 lbs
Mechanical Class X-19-15-250	X = s, rh, re, c, l	> 19 in	≤ 15 in	≤ 250 lbs
Mechanical Class X-13-12-150	X = s, rh, re, c, l	> 13 in	≤ 12 in	≤ 150 lbs
Mechanical Class X-9-8-75	X = s, rh, re, c, l	> 9 in	≤ 8 in	≤ 75 lbs
Mechanical Class X-6-5-25	X = s, rh, re, c, l	> 6 in	≤ 5 in	≤ 25 lbs
Mechanical Class X-2-5-15	X = s, rh, re, c, l	> 2 in	≤ 5 in	≤ 15 lbs

* The shapes are s = square, rh = rhombus, re = rectangle, c = circle, l = line or rail.

† For an externally mounted, self-contained physical package, the CG is the normal distance from mounting mechanical interface, centered at the mount. For a distributed physical package, CG is the average of the masses and distances of all apertures that are part of a singular set of SOSA components. Similarly, weight is the sum of all apertures.

The physical attributes for the mechanical classes are derived primarily by consideration to airworthiness, based on existing sensors on the market. Because the numerical attributes do not include both upper and lower bounds, per class, it is possible that a single sensor could be considered part of several classes. This occurs when the large mounting axis is very large, but the CG and weight are very low. However, this is not indicative of the market and not recommended.

Recommendation 13.5.5.1-1: Given a mechanical class, the upper bound for the largest mounting axis should be that of the next highest mechanical class. Conformance Methodology (I)

For a turreted sensor, this Interface Standard follows one-to-one with the size, weight, and CG found in SAE AS6169A, with the name changes highlighted in Table 13.5.5.1-2. Note that Recommendation 13.5.5.1-1 follows the diameter bounding for the largest mounting axis found in the SAE AS6169A Turret Classes.

Rule 13.5.5.1-2: Turreted physical package SOSA sensors shall conform to the Turret Classes requirements of SAE AS6169A (§3.1, Table 2), which are equivalent to the Turreted SOSA classes outlined in Table 13.5.5.1-2. Conformance Methodology (I)

Table 13.5.5.1-2: SOSA Sensor Mechanical Classes

Turreted SOSA Sensor Mechanical Class	SAE AS6169A Turret Class
Mechanical Class c-19-15-250	Class I
Mechanical Class c-13-12-150	Class II
Mechanical Class c-9-8-75	Class III
Mechanical Class c-6-5-25	Class IV

Given a mechanical class, each sensor package type can have a mechanical mounting interface defined. Presently, the Interface Standard includes references to SAE AS6169A for turreted sensor package types and a mechanical interface for a mechanical class c-6-15-5 gimbaled sensor. It is expected that a future version of the Interface Standard could include additional fastener patterns and Computer Aided Design (CAD) drawings.

Additional mechanical classes could be proposed for inclusion in a future version of this document.

13.5.5.2 *SOSA Mechanical Class c-19-15-250 Sensor Mechanical Interfaces*

13.5.5.2.1 **Turreted Sensor Package**

Rule 13.5.5.2.1-1: All turreted sensor packages with no access hole in mechanical class c-19-15-250 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.1, Figure 6. Conformance Methodology (I, A)

Rule 13.5.5.2.1-2: All turreted sensor packages with access hole in mechanical class c-19-15-250 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.1, Figure 7. Conformance Methodology (I, A)

13.5.5.3 *SOSA Mechanical Class c-13-12-150 Sensor Mechanical Interfaces*

13.5.5.3.1 **Turreted Sensor Package**

Rule 13.5.5.3.1-1: All turreted sensor packages with no access hole in mechanical class c-13-12-150 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.2, Figure 8. Conformance Methodology (I, A)

Rule 13.5.5.3.1-2: All turreted sensor packages with access hole in mechanical class c-13-12-150 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.2, Figure 9. Conformance Methodology (I, A)

13.5.5.4 *SOSA Mechanical Class c-9-8-75 Sensor Mechanical Interfaces*

13.5.5.4.1 Turreted Sensor Package

Rule 13.5.5.4.1-1: All turreted sensor packages with no access hole in mechanical class c-9-8-75 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.3, Figure 10. Conformance Methodology (I, A)

Rule 13.5.5.4.1-2: All turreted sensor packages with access hole in mechanical class c-9-8-75 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.3, Figure 11. Conformance Methodology (I, A)

13.5.5.5 *SOSA Mechanical Class c-6-5-25 Sensor Mechanical Interfaces*

13.5.5.5.1 Turreted Sensor Package

Rule 13.5.5.5.1-1: All turreted sensor packages with no access hole in mechanical class c-6-5-25 shall mount to the host platform in accordance with SAE AS6169A §4.1.3.4, Figures 12, 13, or 15. Conformance Methodology (I, A)

Rule 13.5.5.5.1-2: All turreted sensor packages with access hole in mechanical class c-6-5-25 shall mount to the host platform in accordance with SAE AS6169 §4.1.3.4, Figures 14 or 16. Conformance Methodology (I, A)

13.5.5.6 *SOSA Mechanical Class c-2-5-15 Sensor Mechanical Interfaces*

13.5.5.6.1 Gimbaled EO/IR Sensor Package

Rule 13.5.5.6.1-1: All gimbaled EO/IR sensor packages in mechanical class c-2-5-15 shall mount to the host platform as detailed by Figure 13.5.5.6.1-1. Conformance Methodology (I, A)

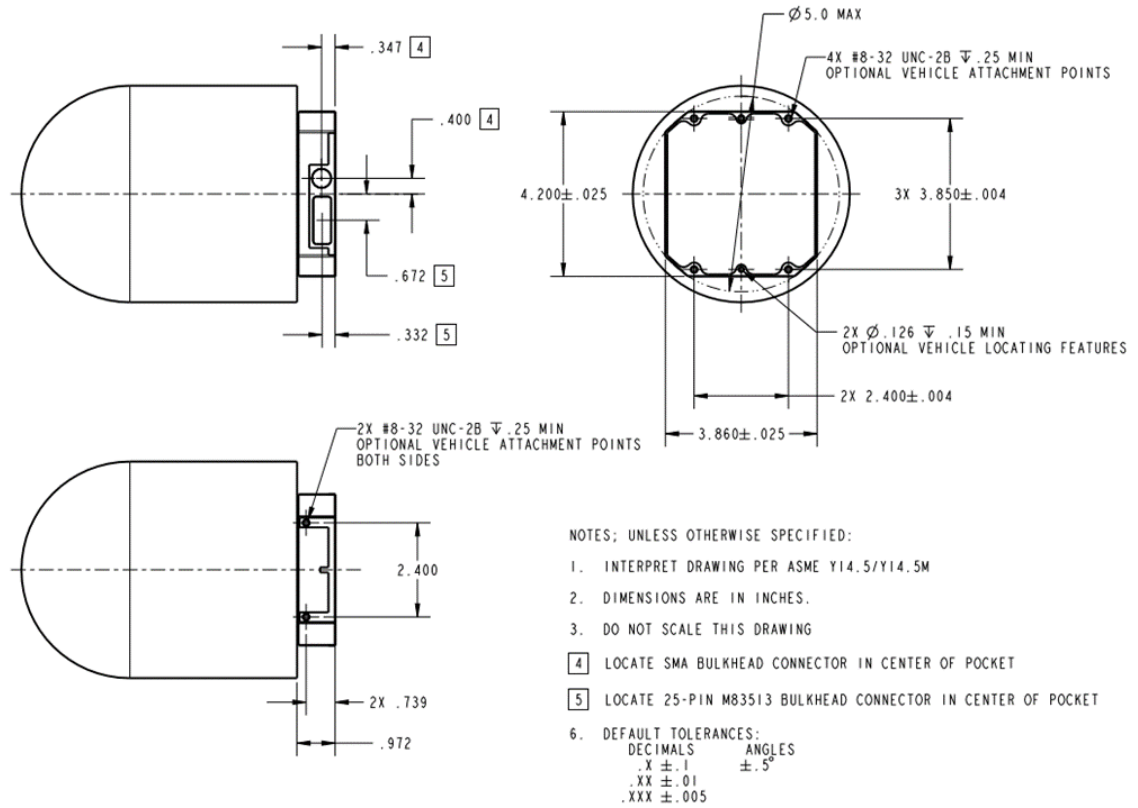


Figure 13.5.5.6.1-1: Mechanical Class c-2-5-15 Mounting Detail

14 SOSA Run-Time Environment

14.1 Overview

SOSA modules could contain a wide range of functions and many of these are accomplished through computer processing. SOSA modules can be realized in a variety of mediums: hardware, configurable devices (i.e., FPGAs), software, or a combination of these. A Run-time Environment (RTE) provides an executable software infrastructure within a general-purpose processor. To promote software portability of the open and standardized goals of the SOSA Technical Architecture, the RTE is specified for SOSA module software.

The SOSA RTE provides the execution environment for SOSA modules implemented as portable software, containers, or virtual machines. The SOSA RTE does not mandate a specific run-time implementation but specifies standardized interfaces. The key interfaces that are specified by the SOSA RTE are between the SOSA module software and the underlying RTE executing, as shown in Figure 14.1-1.

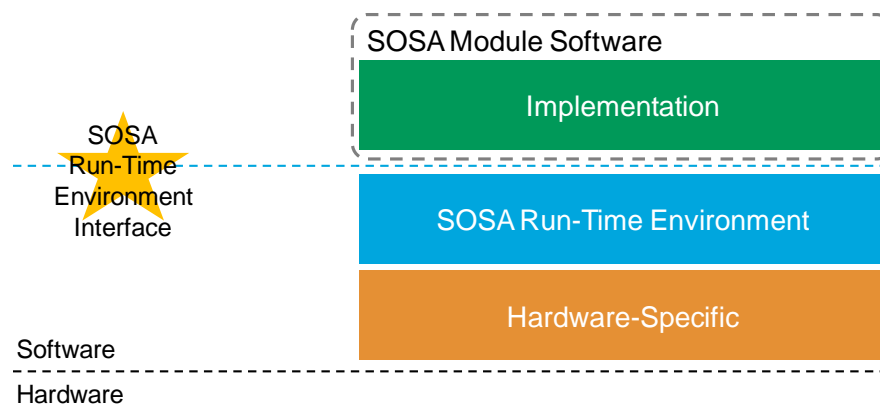


Figure 14.1-1: SOSA Run-Time Environment Interface

Several RTE profiles have been adopted in this document to give the SOSA module developers and system integrators the ability to select the best profile(s) for the modalities of the SOSA sensor being created. The SOSA module vendor and/or integrator could select which RTE profiles are supported. Not all profiles are needed. Table 14.1-1 describes the SOSA RTE profiles and rationale for use.

Table 14.1-1: SOSA Run-Time Environment Profiles

Run-Time Environment Profile	Usage/Rationale for Use
FACE Operating System Segment (OSS)	This document leverages the FACE Operating System Segment (OSS) profiles for portable software native processing on general-purpose processing hardware. All FACE OSS Profiles are allowed: General-Purpose, Safety, and Security. These profiles enable the porting of existing FACE software. Additionally, executing applications native enables use of real-time processing for high-performance/low-latency applications.
Container	The SOSA Container RTE profile enables support for additional programming languages and dependencies used in SOSA modules that could not align with the FACE OSS Profiles; for example, REDHAWK TOA.
Virtual Machine	The SOSA Virtual Machine RTE profile enables multiple operating systems to run simultaneously. This profile can be leveraged to enable partitioning of executing software for security or safety reasons.

SOSA systems integrators define the composition of SOSA modules to enable the desired modalities. As such, not all SOSA RTE profiles will be available for each SOSA module software and *vice versa*. Figure 14.1-2 illustrates the use of multiple SOSA RTEs within a variety of SOSA modules.

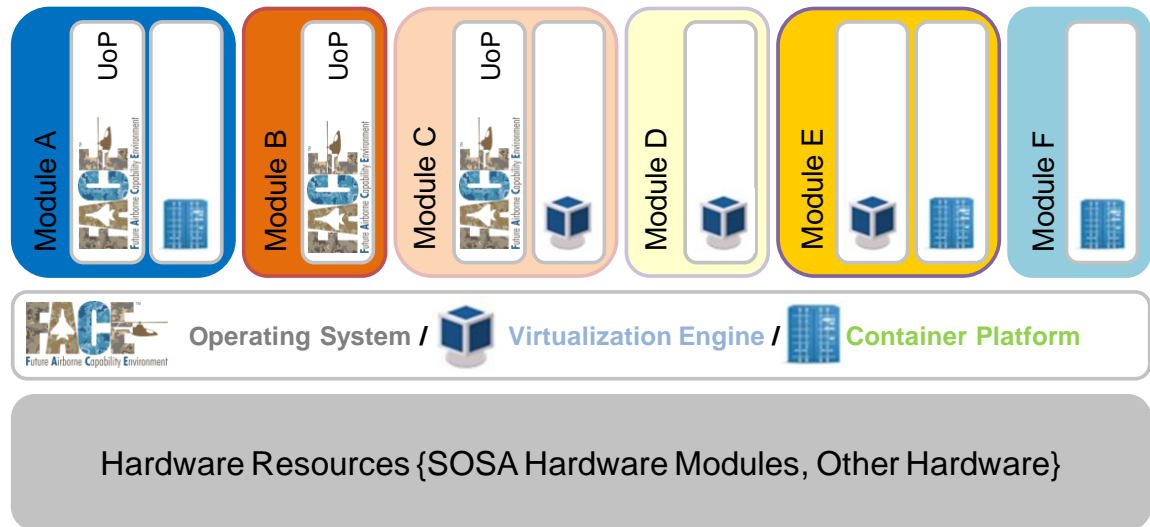


Figure 14.1-2: Sample SOSA Composition with Multiple RTE Profiles

The SOSA RTE profiles in this document can be encapsulated in one another such that the Virtual Machine RTE profile could execute a virtual machine which contains a container engine providing the Container RTE profile. Similarly, a Container RTE profile could execute a container which provides a FACE General-Purpose OSS Profile to run a FACE application. This document does not explicitly define rules when encapsulating SOSA RTEs.

Rule 14.1-1: Where a SOSA module is implemented by software using the operating system API to access operating system resources, the software shall execute in the FACE OSS RTE profile. Conformance Methodology (I)

Rule 14.1-2: Where a SOSA module is implemented by software running in a container engine, the software shall execute in the SOSA Container profile RTE. Conformance Methodology (I)

Rule 14.1-3: Where a SOSA module is implemented by software running in a hypervisor, the software shall execute in the SOSA Virtual Machine profile RTE. Conformance Methodology (I)

Rule 14.1-4: Where the SOSA Procurable Unit includes an RTE, the Procurable Unit shall provide at least one SOSA RTE profile: FACE OSS RTE profile, SOSA Container RTE Profile, or SOSA Virtual Machine RTE profile to execute SOSA module software. Conformance Methodology (I)

Observation 14.1-1: SOSA module software could be composed of multiple executables, containers, or virtual appliances, which span the SOSA RTE profiles. This document does not specify how this software communicates between the multiple executables, containers, or virtual appliances within the SOSA module.

14.2 SOSA Configuration Files

The goal is to assist interoperability by providing a high-level SOSA specific configuration file that can also reference or include lower-level configuration files specific to the RTE technology in use.

Configuration files are associated with software applications, containers, or virtual machines, and not the underlying operating system, container engine, or hypervisor.

Configuration files are used to provide information about the RTE and allow run-time decisions. Each RTE, regardless of profile, has a configuration file.

Observation 14.2-1: This version of the SOSA Technical Standard specifies the minimum content of the configuration file, but not the format.

Permission 14.2-1: When custom attributes are needed, additional fields may be added to the configuration file, provided they are distinguishable from other fields.

Observation 14.2-2: If a SOSA module developer or SOSA system integrator identifies a need for configuration file custom attributes, those attributes should be provided to The Open Group SOSA Technical Working Group for possible inclusion in a future version.

Recommendation 14.2-1: The configuration file format should be human-readable, such as XML, JSON, or YAML.

Permission 14.2-2: A configuration file may include a reference to another configuration file.

Rule 14.2-1: When multiple RTEs are implemented on the same PIC, each RTE shall have a configuration file. Conformance Methodology (I)

Rule 14.2-2: Each SOSA RTE configuration file shall contain one *ProfileType* field indicating one of the following: Conformance Methodology (I)

- FACE OSS profile
- Container profile
- Virtual Machine profile

Rule 14.2-3: Each SOSA RTE configuration file shall contain one *ImageLoad* field for each software item to load. Conformance Methodology (I)

Rule 14.2-4: Each SOSA RTE configuration file shall contain at least one *Resources* field indicating the processing resources are necessary for this RTE. The *Resources* field indicates the following: Conformance Methodology (I)

- Number of processing cores
- Amount of volatile memory
- Number and type of communication/networking ports

Rule 14.2-5: When a file system is used, each SOSA RTE configuration file shall contain at least one *FileSystem* field indicating the following: Conformance Methodology (I)

- Device to mount
- Mount point
- File system type

Rule 14.2-6: When multiple executables are used, each SOSA RTE configuration file shall contain at least one *StartOrder* field indicating the start-up execution order. Conformance Methodology (I)

Rule 14.2-7: Each SOSA RTE configuration file shall contain one *OrganizationName* field representing the organization that created the software item. Conformance Methodology (I)

Rule 14.2-8: Each SOSA RTE configuration file shall contain one *Version* field representing the release version number of the software item. Conformance Methodology (I)

Rule 14.2-9: Each SOSA RTE configuration file shall contain one *Date* field representing the release date of the software item. Conformance Methodology (I)

Rule 14.2-10: Each SOSA RTE configuration file shall contain one *Description* field representing the function and/or purpose of the software item. Conformance Methodology (I)

Rule 14.2-11: Each SOSA RTE configuration file shall contain one *SosaModuleId* field representing the functional SOSA module identifier of the software item. Conformance Methodology (I)

Rule 14.2-12: Each SOSA RTE configuration file shall contain one *SecurityEnclave* field representing the maximum-security enclave level of the software item. Conformance Methodology (I)

Rule 14.2-13: A SOSA RTE shall not instantiate its software application if any of the following attributes in the SOSA Configuration File are not satisfied, within its context: Conformance Methodology (T)

- ProfileType
- ImageLoad
- Resources
- FileSystem
- StartOrder
- SecurityEnclave

Rule 14.2-14: A SOSA RTE shall not instantiate its software application if any of its required SOSA Configuration File fields are not present. Conformance Methodology (T)

Rule 14.2-15: If a SOSA RTE is unable to instantiate any software application, it shall send an error notification using the system management interface as described in Section 6.2.8. Conformance Methodology (T)

Observation 14.2-3: The use of custom attributes is discouraged due to interoperability concerns.

Recommendation 14.2-2: Custom attributes should be used in separate product-specific configuration files, which can be referenced by the SOSA Configuration File. Conformance Methodology (T)

14.3 FACE OSS Run-Time Environment Profile

The FACE OSS RTE profile supports native execution of SOSA module software on general-purpose processing resources. This profile relies on the FACE OSS specification for its definition. The FACE Technical Standard (see [Referenced Documents](#)) recognizes that the APIs associated with the General-Purpose, Safety, and Security Profiles provide divergent capabilities. The profile selected should be appropriate for the application safety and security requirements and substantiated. The divergence of these capabilities could prevent or represent considerable safety or security risks, including simultaneous hosting of General-Purpose, Safety, and Security Profile OSS on the same computing platform. Figure 14.3-1 depicts the SOSA OSS RTE and SOSA module software.

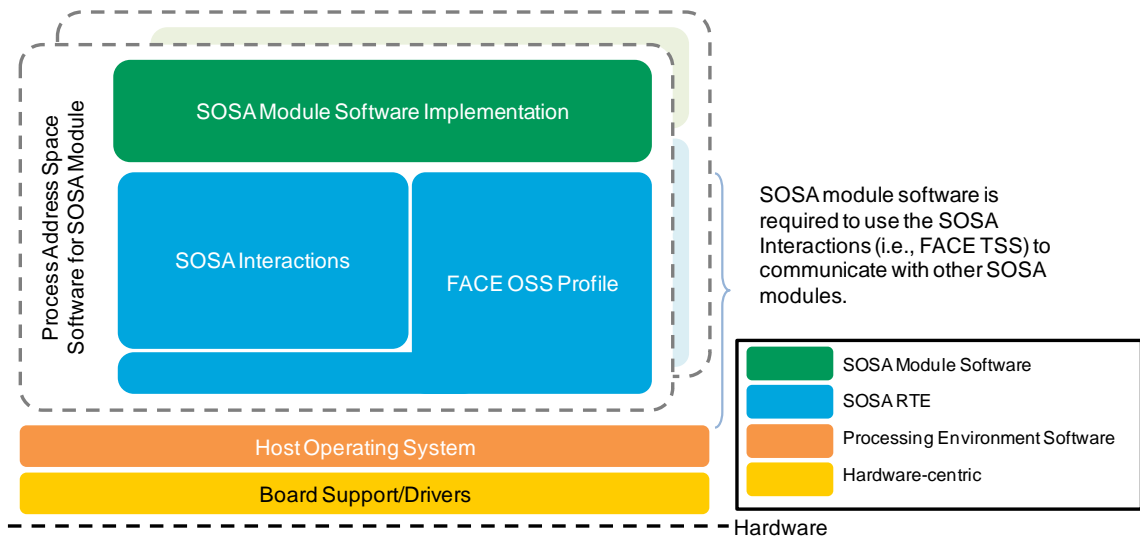


Figure 14.3-1: SOSA Operating System Run-Time Environment Profile

The FACE OSS RTE profile leverages the following FACE Profiles as defined in the FACE Technical Standard, Edition 3.1:

- FACE OSS Security Profile
- FACE OSS Safety Profile
- FACE OSS Safety Extended Profile
- FACE OSS General-Purpose Profile

And the following interface standards:

- ARINC 653
- POSIX™

With support for the following programming languages:

- Ada
- C
- C++
- Java®

The following sections detail the Rules and Recommendations for this profile.

14.3.1 FACE OSS Run-Time Environment

The FACE OSS RTE profile leverages the FACE OSS to provide and control access to the computing platform and software environment.

Rule 14.3.1-1: Where the FACE OSS profile is provided, the SOSA RTE shall be a FACE conformant OSS Unit of Conformance (UoC) with external networking and at least one programming language run-time.

14.3.2 FACE OSS Module Software

The FACE OSS Interface provides a standardized means for software to use the services within the operating system and other capabilities related to the OSS. This interface is provided by software in the OSS to software in other segments.

Rule 14.3.2-1: Where the FACE OSS profile is used, the SOSA module software shall use the operating system interface specified in the FACE Technical Standard, Edition 3.1 §4.2 (including all subsections), §A.6, and §A.7. Conformance Methodology (I)

Observation 14.3.2-1: SOSA module software implements one of the FACE OSS Interface Profiles of Security, Safety, Safety Extended, or General-Purpose, one interface standard of POSIX or ARINC 653, and at least one language Java, Ada, or C/C++.

14.3.3 FACE OSS Configuration File

The FACE OSS Profile uses the RTE configuration file to configure its operating environment. The common requirements for SOSA RTE configuration files are described in Section 14.3.1.

Rule 14.3.3-1: The FACE OSS RTE shall verify that the configuration file has the correct minimum content. Conformance Methodology (D)

Rule 14.3.3-2: The FACE OSS RTE shall only use the configuration file if the *ProfileType* is the FACE OSS Profile. Conformance Methodology (D)

Rule 14.3.3-3: The FACE OSS RTE shall load all software items identified by the *ImageLoad* fields. Conformance Methodology (D)

Rule 14.3.3-4: The FACE OSS RTE shall verify that all resources described by the *Resources* field are adequate. Conformance Methodology (D)

Rule 14.3.3-5: The FACE OSS RTE shall mount all devices described by the *FileSystem* field. Conformance Methodology (D)

Rule 14.3.3-6: The FACE OSS RTE shall start execution of software in the order described by the *StartOrder* field. Conformance Methodology (D)

14.4 SOSA Container Run-Time Environment Profile

The SOSA Container RTE profile supports a mechanism for supporting a variety of operating environments. A container could be used to “wrap” a legacy capability as a SOSA module and hide the software dependencies. The Container module interfaces are exposed to the SOSA inter-module communications network as SOSA interfaces defined by this document. A container could be used to wrap additional programming languages and dependencies used in SOSA modules that could not align with the FACE OSS Profiles. Examples of programming languages that could be used to build SOSA software components are C++17, Java 12, and Python™. An example of a capability which is needed by this document and does not align with the FACE OSS Profiles is REDHAWK.

The concept behind containers is to package software along with all its dependencies in a standardized way to allow for many applications to run on the same processing environment without the need for native support. Containers have gained a significant portion of the market because of their ability to avoid the issues that arise from complex dependency trees and interdependencies between applications running on the same native environment. Figure 14.4-1 depicts this RTE.

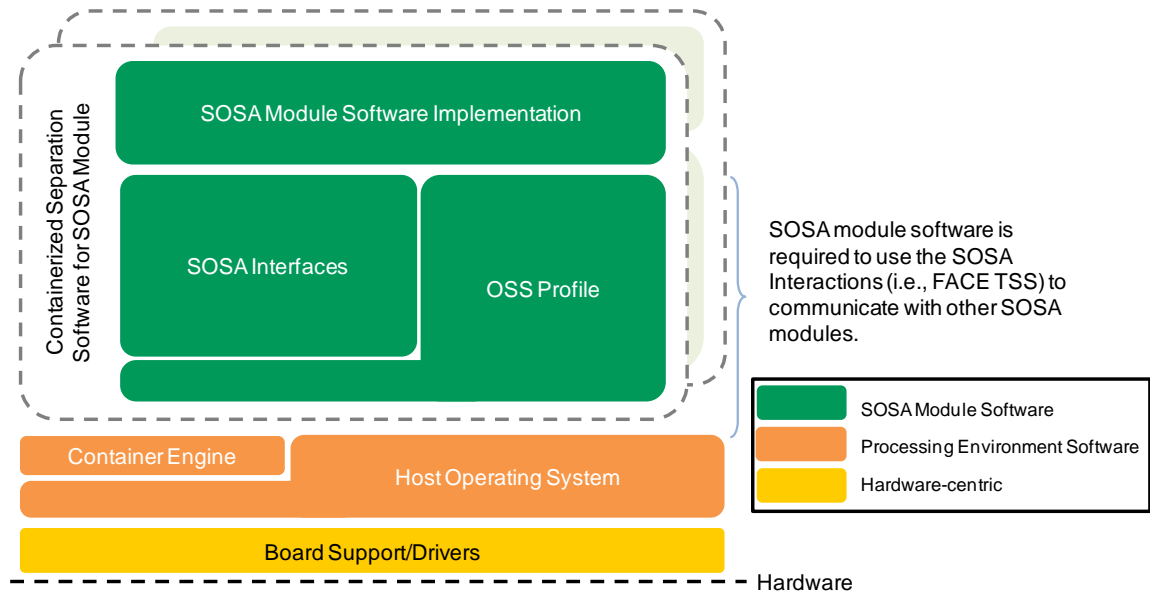


Figure 14.4-1: SOSA Container Run-Time Environment Profile

In support of containers, this document adopts the Open Container Initiative (OCI) image format for the deployment of containers. At this time, OCI is supported by many commercial container frameworks; however, not all features have been standardized so the SOSA RTE Container profile calls out specific minimum versions for support.

Observation 14.4-1: A container RTE could encapsulate a FACE OSS RTE profile by providing a container in which the provided OSS Profile meets the Rules and Recommendations as defined in Section 14.3 of this document.

14.4.1 SOSA Container Run-Time Environment

Observation 14.4.1-1: Use of the OCI Run-Time Specification limits the use of container engine support to the following operating systems: Linux[®], Microsoft[®] Windows[®], and Solaris[®].

Rule 14.4.1-1: Where the SOSA Container RTE profile is provided, the RTE shall provide a container engine that conforms to the OCI Run-Time Specification, Version 1.x to manage the lifecycle of the containers.

Rule 14.4.1-2: Where the SOSA Container RTE profile is provided, the RTE shall provide a container engine which allows access to the network interface(s) necessary for the container to interact with other SOSA modules.

Observation 14.4.1-2: At this time, this document is not requiring that access to any additional resources be provided to a container from the container engine. A future version of this

document could require access to additional resources such as file systems, block I/O, and RDMA devices.

Observation 14.4.1-3: Where an ARINC 653 profile (i.e., Security, Safety Base, Safety Extended, and/or General-Purpose with the ARINC 653 option) and Container profile are simultaneously provided, it is intended that each container be assigned one or more time windows. This document has not addressed the case where multiple containers are assigned the same partition time window.

Observation 14.4.1-4: This document has not addressed container security and permissions for access to host resources and it is up to the implementer to meet any requirements for security. A future version of this document could address security and permissions.

Observation 14.4.1-5: This document has not addressed container orchestration and management of multiple containers which could make up one SOSA module. The system integrator working with SOSA module providers must determine how containers are orchestrated. A future version of this document could include Rules and Recommendations for container orchestration.

14.4.2 SOSA Module Software for Container Profile

Rule 14.4.2-1: Where the SOSA Container RTE is used, SOSA module software shall implement the OCI Run-Time Specification, Version 1.x for the bundled container image.

Observation 14.4.2-1: The OCI Image Specification is specified to enable the creation of interoperable tools for building, transporting, and preparing a container image to run. At this time, this document is only requiring that container images be delivered as run-time bundles and not as images required to be built.

Rule 14.4.2-2: Where the SOSA Container RTE is used, SOSA module software shall utilize network interface(s) to communicate with other SOSA modules through SOSA interactions.

Observation 14.4.2-2: SOSA module software packaged as containers still needs to be compliant to the SOSA inter-module interactions when communicating to other SOSA modules. This document does not specify how multiple containers that make up a single SOSA module communicate with each other.

Observation 14.4.2-3: Refer to NIST SP 800-190, Application Container Security Guide and applicable SRGs for cybersecurity controls necessary to operate containers securely. It is up to the container provider to understand which security controls could be required in a deployed sensor.

Observation 14.4.2-4: Linux container kernels have less complexity as a native operating system and as a container operating system than non-Linux-based kernels.

Recommendation 14.4.2-1: A Linux container kernel should be compatible with the FACE OSS when combining the FACE Profile and containers.

Observation 14.4.2-5: DoD-approved example containers already exist upon which new container software can be built.

14.4.3 SOSA Container Configuration File

The SOSA Container profile uses the RTE configuration file to configure its operating environment. The common requirements for SOSA RTE configuration files are described in Section 14.3.

Rule 14.4.3-1: The Container RTE shall verify that the configuration file has the correct minimum content. Conformance Methodology (D)

Rule 14.4.3-2: The Container RTE shall only use the configuration file if the *ProfileType* is the Container profile. Conformance Methodology (D)

Rule 14.4.3-3: The Container RTE shall load all software items identified by the *ImageLoad* fields. Conformance Methodology (D)

Rule 14.4.3-4: The Container RTE shall verify that all resources described by the *Resources* field are adequate. Conformance Methodology (D)

Rule 14.4.3-5: The Container RTE shall mount all devices described by the *FileSystem* field. Conformance Methodology (D)

Rule 14.4.3-6: The Container RTE shall start execution of software in the order described by the *StartOrder* field. Conformance Methodology (D)

14.5 SOSA Virtual Machine Run-Time Environment Profile

The SOSA Virtual Machine RTE profile supports additional real-time operating systems, programming languages, and dependencies used in SOSA modules that could not align with the FACE OSS Profiles. Additionally, the Virtual Machine profile allows for hypervisors which supports hard partitioning of processing for safety and security functions. For example, this profile can enable aggregating of safety-critical processing on the same hardware as non-safety-critical functions.

There are two types of virtual machine architectures, which are described in Table 14.5-1.

Table 14.5-1: Virtual Machine Types

Virtual Machine Type	Description
Type 1 Hypervisor	This type of hypervisor provides a bare metal or native processing for the sole purpose of launching virtual machines. This type is only able to run virtual machines of the same hardware architecture (i.e., ia64 or arm).
Type 2 Hypervisor	This type of hypervisor is hosted on a host operating system and encapsulates virtual machines through emulation. This type of hypervisor can run virtual machines of different hardware architectures.

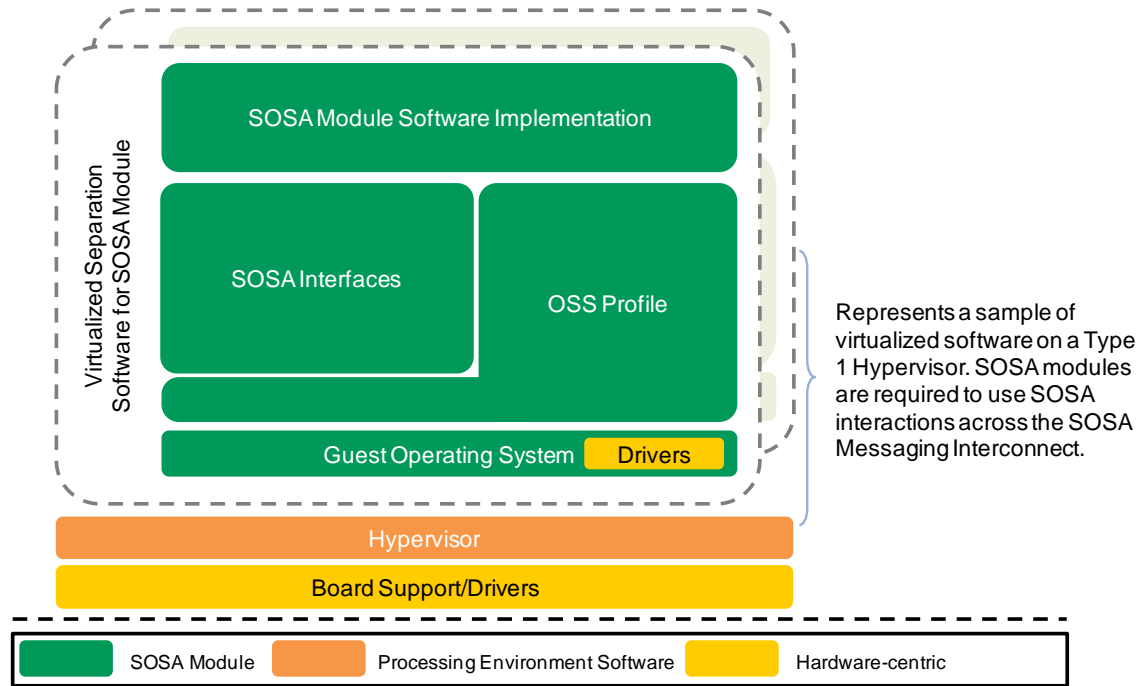


Figure 14.5-1: Type 1 Hypervisor

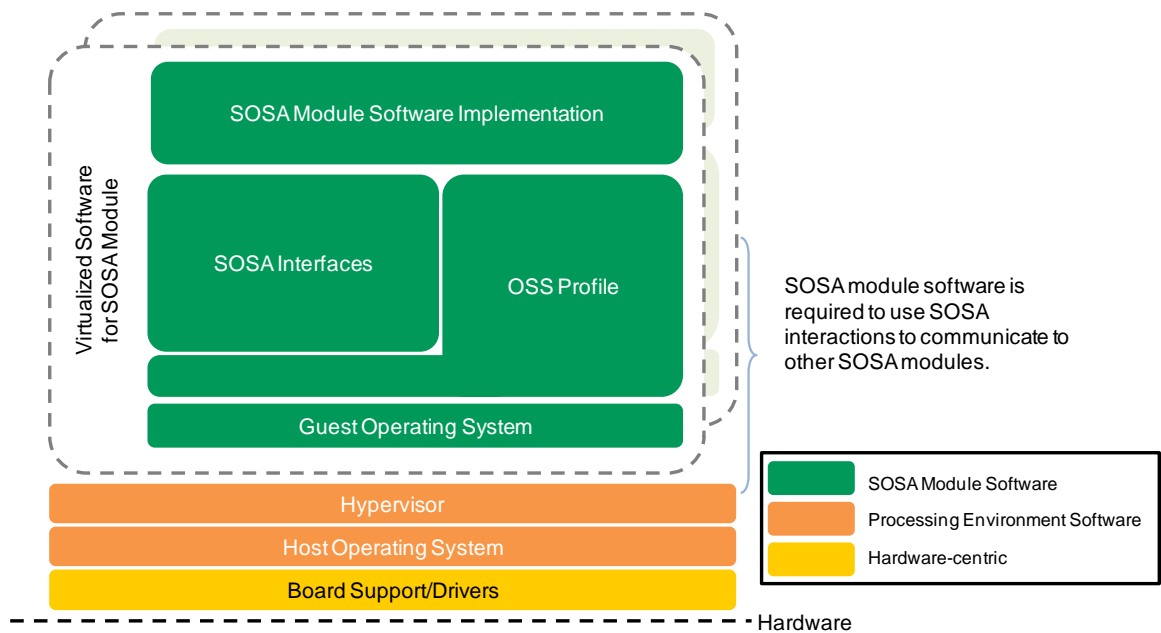


Figure 14.5-2: Type 2 Hypervisor

Observation 14.5-1: A Virtual Machine RTE could encapsulate a FACE OSS RTE profile by providing a virtual machine in which the provided operating system profile meets the Rules and Regulations as defined in Section 14.3 of this document.

14.5.1 SOSA Virtual Machine Run-Time Environment

Rule 14.5.1-1: Where the SOSA Virtual Machine RTE is provided, the RTE shall provide a hypervisor capable of running a virtual appliance packaged in the Distributed Management Task Force (DMTF) Open Virtualization Format (OVF), Version 2.x.

Rule 14.5.1-2: Where the SOSA Virtual Machine RTE profile is provided, the RTE shall provide a hypervisor which allows access to the network interface(s) necessary for the software application executing in the virtual machine to interact with other SOSA modules.

Observation 14.5.1-1: At this time, this document is not requiring access to any additional resources be provided to a virtual machine from the hypervisor. A future version of this document could require access to additional resources such as file systems, block I/O, and RDMA devices.

Observation 14.5.1-2: Where an ARINC 653 profile (i.e., Security, Safety Base, Safety Extended, and/or General-Purpose with the ARINC 653 option) and Virtual Machine profile are simultaneously provided, it is intended that each virtual machine be assigned one or more time windows. This document has not addressed the case where multiple virtual machines are assigned the same partition time window.

14.5.2 SOSA Module Software for Virtual Machine Profile

Rule 14.5.2-1: Where the SOSA Virtual Machine RTE is used, the SOSA module software shall be distributed as a virtual appliance using the DMTF OVF, Version 2.x.

Rule 14.5.2-2: Where the SOSA Virtual Machine RTE interface is used, SOSA module software shall utilize network interface(s) to communicate with other SOSA modules through SOSA interactions.

Observation 14.5.2-1: SOSA module software packaged as virtual machines still need to be compliant to the SOSA inter-module interactions when communicating to other SOSA modules. This document does not specify how multiple virtual machines that make up a single SOSA module communicate with each other.

Observation 14.5.2-2: Refer to NIST SP 800-125, Guide to Security for Full Virtualization Technologies and applicable Security Technical Implementation Guides (STIGs) for cybersecurity controls necessary to operate virtual machines securely. It is up to the virtual machine appliance supplier to understand and implement the required security controls in a deployed sensor.

14.5.3 SOSA Virtual Machine Configuration File

The SOSA Virtual Machine profile uses the RTE configuration file to configure its operating environment. The common requirements for SOSA RTE configuration files are described in Section 14.3.

Rule 14.5.3-1: The Virtual Machine RTE shall verify that the configuration file has the correct minimum content. Conformance Methodology (D)

Rule 14.5.3-2: The Virtual Machine RTE shall only use the configuration file if the *ProfileType* is the Virtual Machine profile. Conformance Methodology (D)

Rule 14.5.3-3: The Virtual Machine RTE shall load all software items identified by the *ImageLoad* fields. Conformance Methodology (D)

Rule 14.5.3-4: The Virtual Machine RTE shall verify that all resources described by the *Resources* field are adequate. Conformance Methodology (D)

Rule 14.5.3-5: The Virtual Machine RTE shall mount all devices described by the *FileSystem* field. Conformance Methodology (D)

Rule 14.5.3-6: The Virtual Machine RTE shall start execution of software in the order described by the *StartOrder* field. Conformance Methodology (D)

14.6 Mixed Run-Time Environments

The previous sections have defined three possible software RTEs; however, it is possible to combine these RTEs to create more complex SOSA module implementations.

Permission 14.6-1: A FACE General-Purpose Profile RTE may include a container engine and one or more containers that comply with Section 14.4.

Permission 14.6-2: A FACE General-Purpose Profile RTE may include a hypervisor and one or more virtual machines that comply with Section 14.5.

Observation 14.6-1: Many permutations of mixed RTEs are technically possible; however, integrators should carefully analyze resources, performance, and security considerations.

15 Inter-Module Interactions

15.1 Interactions on the SOSA Message Interconnect

SOSA modules and hardware elements interoperate via interactions. A list of interaction types is shown in Table 15.1-1. An interaction is composed of an operation (or action) relating to the function the interaction supports, and parameters that are described by DIV-2 Data Entities. Parameters are the inputs and outputs of the operation being accomplished by the interaction.

An interaction occurs between two or more modular entities, with each one playing a role in the interaction. The types of roles vary based upon the interaction type, but generally one party to the interaction plays the role of *provider*, or *service*, and one or more others play the role of *user*, *consumer*, or *client*.

SOSA sensor component interactions that involve the exchange of digital information will often be implemented on a SOSA Message Interconnect or a SOSA Wideband Low-Latency Interconnect, which provide network messaging services. These interactions will be implemented by the exchange of network messages in which parameters are encoded in network payloads. Interactions in which messages are exchanged between two or more SOSA modules in a pattern are described by a message protocol.

SOSA sensor component interactions that do not require determinism, extreme high bandwidth, or very low latency are implemented by network messages on a SOSA Message Interconnect. Some classes of interactions, such as those that support in-band system management, do not have challenging performance requirements, and thus are mapped to a SOSA Message Interconnect.

When SOSA sensor implementation requirements are such that SOSA module interactions must be implemented with determinism, latency, throughput, or other QoS attributes that cannot be supported by a SOSA Message Interconnect, they are mapped to a SOSA Wideband Low-Latency Interconnect. Examples are digital RF signals (sample streams, etc.) and interactions that send control messages to adjust RF electronics.

When performance or other program requirements cannot be met using the two default interconnects, SOSA module interactions could be implemented using other interconnects. For example, SOSA modules could be implemented across multiple hardware elements, and for performance reasons could leverage other interconnects to implement the internal communications within the module boundaries. Because these interactions are not defined by the SOSA Technical Standard, this document does not specify or evaluate conformance of these intra-module interactions.

Table 15.1-1: Interaction Types

Interaction Type	Description	Default Interconnect
Analog Distribution	Distribute analog signals point-to-point or point-to-multi-point (fan out), usually carried on copper coaxial, but sometimes on other media such as optical fiber.	Analog Medium (e.g., coax, twisted pair, fiber)
Digital Signal Stream	Send digital signal (I/Q samples) or data product (e.g., signal environment snapshot) streams. It is implicit that these tend to be either high volume or require low latency. Configurable QoS (e.g., dependability, data delivery confirmation, retry) options allow implementation to meet design specific needs.	SOSA Wideband Low-Latency Interconnect
Digital Signal Context	Metadata related to a digital signal stream.	SOSA Wideband Low-Latency Interconnect
Signal Layer Control	Dynamic control of signal layer electronics. These require low latency, as they occur during execution of a task, and could be within the application control loop.	SOSA Wideband Low-Latency Interconnect
Virtual Discrete	Interaction to implement discrete signals via network messages. Discrete signals have traditionally been implemented by fixed-purpose signals (HW lines). The intent is to allow discrete signals to be replaced by network-based interactions when it is possible based on system safety and security requirements.	SOSA Wideband Low-Latency Interconnect
Publish-Subscribe	Interaction to share data between a set of publishers and a set of subscribers. The publish-subscribe interaction is a many-to-many interaction that shares structured data in the form of messages.	SOSA Message Interconnect
Request-Response	Interaction between a service (provider) and a client (user) interaction endpoint, in which the client interaction endpoint sends a request to the service interaction endpoint to which the service interaction endpoint responds. The intent could be to get data from the service, to transfer data to the service, or to affect change to the mode or state of the service. The notable uniqueness of request-response interactions is that they are initiated by the user, and the temporal pattern is not assumed to be regular.	SOSA Message Interconnect

Interaction Type	Description	Default Interconnect
Event Notification	Interaction to send an immediate notification of a key event in a module or system. Examples are mode or state changes and faults. The mechanism is a special subset of publish-subscribe interactions, in that notifications are not published unless an event occurs. For example, a notification is sent immediately when a fault event occurs. Also, notifications could be “acknowledgeable”, meaning that it persists until explicitly acknowledged.	SOSA Message Interconnect
File Transfer	An interaction to send a block of data from a data provider to one or more data consumers. The file transfer mechanism involves a single data provider (the writer) sending the block of data by writing to a file, and the consumers (readers) receiving the data by opening and reading the file once the writer has completed the write and published the location of the file. Until the writer has published the location of the file, the readers should not assume the data is complete and consistent. File transfer interactions assume that readers and writers all have access to the file system where the files are to be written, and both know the location and names of the files.	SOSA Message Interconnect

Additional description is provided for the interaction types that are most relevant to the following technical discussions.

15.2 Application Programming Interface (API)

The SOSA Architecture is based on a set of loosely-coupled modular entities that interact with the underlying operating environment and with each other via their logical interfaces.

In cases where portable software is a primary goal, SOSA modules can be instantiated as SOSA implemented by software using the Operating System API to access operating system resources and the Transport API to access communication resources. In this case, the SOSA module will leverage an Application Programming Interface (API) provided by the underlying Run-time Environment Interface (REI); e.g., I/O, processing, storage, communication, etc.

In addition to the API used, SOSA module implementations will also interoperate by exchanging well-defined standardized messages.

This section defines both the API and message-based standard interfaces for inter-module interactions.

Rule 15.2-1: Where a SOSA module is instantiated as a SOSA module implemented by software using the Transport API to access communication resources, it shall use the Transport Service Capability, Distribution Capability, Configuration Capability, and the QoS Management Capability of the FACE Technical Standard, Edition 3.1 for interactions on the SOSA Message Interconnect and the SOSA Wideband Low-Latency Interconnect. Conformance Methodology (T)

Observation 15.2-2: The details of the how the FACE Transport Services Segment (TSS) will be configured will be defined in a future version of this document. FACE TSS capabilities not listed in Rule 14.2-1 are not precluded.

15.3 Quality of Service (QoS)

To enable portability, standardizing the method in which Quality of Service (QoS) is described and its corresponding parameters is essential. For this document, a common nomenclature for QoS is established. This QoS nomenclature identifies a set of configurable QoS attributes, enumerates the available options within each attribute, and specifies units and ranges where necessary. How QoS is implemented will be discussed in a future version of this document. It should be noted that sensor to sensor QoS is outside the scope of this document. Table 15.3-1 enumerates the available QoS policies for each QoS attribute and provides units and ranges. Details of the QoS attributes appearing in Table 15.3-1 are described next.

QoS

Given a set of SOSA modules, QoS is the shared characterization of data flows such that producers (Data Writer) and consumers (Data Reader) of data can describe, agree to, and determine their behavior.

- QoS is a shared vocabulary to characterize data flows
- QoS attributes make up a QoS policy
- QoS policies make up a contract between what is offered by a producer and expected by a consumer; this enables the infrastructure to ensure compatibility between producers and consumers, and alert when incompatibilities exist

Reliability

Indicates whether samples lost by the network should be repaired by the middleware.

Reliability can be implemented as BEST_EFFORT or RELIABLE – the default policy is BEST_EFFORT:

- BEST_EFFORT: no resources will be used to monitor or guarantee that the data sent by a Data Writer is received by a Data Reader
- RELIABLE: ensures that all data from the Data Writer is received reliably by the Data Readers; data is sent as many times as needed until the Data Reader receives it

Deadline

Maximum duration within which an instance is expected to be updated.

Duration

- Measured in microseconds and valid for values greater than 0
- The default duration is infinite

Durability

Specifies how to store and deliver previously published data to new/late-joining Data Readers.

Durability can be implemented as VOLATILE, TRANSIENT_LOCAL, TRANSIENT, OR PERSISTENT – the default policy is VOLATILE:

- VOLATILE: no data samples will be kept
- TRANSIENT_LOCAL: some samples are kept for new/late-joining Data Readers; these samples are stored in the memory of the Data Writer that wrote the data and the data is not required to survive the Data Writer
 - *history_depth*: number of data samples to keep in memory
- TRANSIENT: some samples are kept for new/late-joining Data Readers; these samples are stored in the memory and not in permanent storage and the data is required to survive the Data Writer
 - *history_depth*: number of data samples to keep in memory
- PERSISTENT: data samples are kept in permanent storage and outlive the system session
 - *history_depth*: number of data samples to keep in permanent memory

Liveliness

Control mechanism that allows Data Readers to detect when matching Data Writers become disconnected/dead.

Liveliness can be implemented as AUTOMATIC – the default *lease_duration* is infinite:

- AUTOMATIC: signal liveliness for Data Writers at least as often as specified by *lease_duration*
 - *lease_duration*: measured in microseconds

Ownership

Specifies if a Data Reader can receive new samples for an instance of data from multiple Data Writers at the same time.

Ownership can be implemented as SHARED, EXCLUSIVE, or SHARED_EXCLUSIVE – the default policy is SHARED:

- SHARED: multiple Data Writers are allowed to update the same instance of data and all the updates are made available to all the Data Readers; this implies that there is no concept of an “owner” for data instances
- EXCLUSIVE: each data instance can only be owned by one Data Writer, but this owner can change dynamically
- SHARED_EXCLUSIVE: multiple Data Writers can write the same instance of the data, and how many of these modifications should be permitted

Priority

Specifies the priority of the Data Writer.

- *priority*: a range [0, X] with 0 being the lowest priority
- The default *priority* is 0

Table 15.3-1: SOSA QoS Attribute Units and Ranges

QoS Attribute	QoS Policy	Parameters	Units	Range
Reliability	BEST_EFFORT	N/A	N/A	N/A
	RELIABLE	N/A	N/A	N/A
Deadline	N/A	duration	microseconds	> 0
Durability	VOLATILE	N/A	N/A	N/A
	TRANSIENT_LOCAL	history_depth	message	>= 1
	TRANSIENT	history_depth	message	>= 1
	PERSISTENT	history_depth	message	>= 1
Liveliness	AUTOMATIC	lease_duration	microseconds	> 0
Ownership	SHARED	N/A	N/A	N/A
	EXCLUSIVE	N/A	N/A	N/A
	SHARED_EXCLUSIVE	N/A	N/A	N/A
Priority	N/A	priority	N/A	[0,X]

15.4 Data Product and Task Management Interaction Implementation

To enable interoperability between SOSA sensor components in a way that is agnostic to the sensor component implementation technology, this document establishes a suite of interaction bindings. Interaction bindings specify how interactions are realized as messages on the SOSA Message Interconnects. The choices for interaction bindings for the SOSA Message Interconnect are listed in Table 15.4.2-1, and the details of each interaction binding choice are described in subsequent sections.

15.4.1 Interaction Implementation Concepts

Interaction bindings define the way the interactions are realized as messages on the network. This document allows for multiple patterns for implementing modules, with a standard interaction infrastructure and API, and without. The interaction infrastructure promotes portable software by providing an API that abstracts the software from the interaction bindings. In that case, the interaction infrastructure is responsible for implementing the interaction bindings to

provide on-the-wire interoperability. When SOSA modules are implemented without the interaction infrastructure, the module implementation is responsible for implementing the on-the-wire interoperability for all interactions implemented by that SOSA module.

Data Definition

A programming language-neutral representation of the data, including its structure, breakdown into individual data parameters, and the semantics of the data. This information is defined in a semantic data model.

Data Encoding

The transformation of the in-memory representation of a data object into a format suitable for storage or transmission. This is sometimes referred to as serialization or marshaling, and the encoded data could be referred to as the message payload. The opposite process is decoding, or deserialization.

Encapsulation

The process of putting the encoded data into one or more transport units, which could involve breaking the encoded data into multiple pieces (fragmentation) and/or adding an application-specific header (encapsulation) and writing the encapsulated fragments (transport payloads) into the transport payloads.

Transport

Provides communication services between the interaction endpoints for applications. Provides communication service options such as connection-oriented or connectionless communication patterns, point-to-point or point-to-multipoint delivery, reliable (automatic drop detection and retries) or non-reliable delivery, flow control, and multiplexing.

Network

Responsible for packet forwarding including routing through intermediate routers.

15.4.2 Interaction Binding Technology Selections

These are specific selections for Data Encoding, Encapsulation, Transport, and Network implementation choices that implement interactions between SOSA sensor components on SOSA interconnects. The interaction binding is how interactions moving data described by the Data Definitions are implemented using a specific set of technology choices.

Table 15.4.2-1 lists the interaction bindings that the SOSA Technical Standard defines as acceptable on the SOSA Message Interconnect, and their relevance to interaction types that default to the SOSA Message Interconnect. Note that Table 15.4.2-1 is not a complete listing of all technology bindings and interaction types and does not imply exclusion of these technologies on the other SOSA interconnects.

Table 15.4.2-1: Interaction Bindings and Interaction Types on the SOSA Message Interconnect

Technology Binding	Publish-Subscribe	Request-Response	Event Notification	File Transfer
OMG DDS	Y	Y	Y	N
Protobuf + AMQP	Y	N	Y	N
Protobuf + ZMTP	Y	Y	Y	N
NFS Transfer	N	N	N	Y

Note: RoCE, Version 2 is expected to be included in a future version of this document for Data Products and Task Management.

15.4.3 OMG DDS Technology Binding Rules

Rule 15.4.3-1: Where interactions between SOSA sensor components are implemented using the OMG DDS technology binding on a SOSA Message Interconnect, the interaction message Data Definition shall be defined using OMG IDL 4.0 or higher and Xtypes.

Rule 15.4.3-2: Where interactions between SOSA sensor components are implemented using the OMG DDS technology binding on a SOSA Message Interconnect, the interaction Data Encoding and Encapsulation shall be implemented using DDS/RTPS v1.4 or higher.

Rule 15.4.3-3: Where request-response interactions between SOSA sensor components are implemented using the OMG DDS technology binding on a SOSA Message Interconnect, the interaction shall be implemented using DDS-RPC v1.0 or higher.

Rule 15.4.3-4: Where interactions between SOSA sensor components are implemented using the OMG DDS technology binding on a SOSA Message Interconnect, the interaction shall be implemented using UDP at the Transport layer.

Rule 15.4.3-5: Where interactions between SOSA sensor components are implemented using the OMG DDS technology binding on a SOSA Message Interconnect, the interaction shall be implemented using IPv4 or IPv6 at the Network layer.

15.4.4 Protobuf + AMQP Technology Binding Rules

Rule 15.4.4-1: Where interactions between SOSA sensor components are implemented using the Protobuf + AMQP technology binding on a SOSA Message Interconnect, the interaction message Data Definition shall be defined using the IDL of Protobuf v3.0 or higher.

Rule 15.4.4-2: Where interactions between SOSA sensor components are implemented using the Protobuf + AMQP technology binding on a SOSA Message Interconnect, the interaction message Data Encoding shall be implemented using Protobuf v3.0 or higher.

Rule 15.4.4-3: Where interactions between SOSA sensor components are implemented using the Protobuf + AMQP technology binding on a SOSA Message Interconnect, the interaction message Encapsulation shall be implemented using AMQP v1.0 or higher.

Rule 15.4.4-4: Where interactions between SOSA sensor components are implemented using the Protobuf + AMQP technology binding on a SOSA Message Interconnect, the interaction shall be implemented using TCP at the Transport layer.

Rule 15.4.4-5: Where interactions between SOSA sensor components are implemented using the Protobuf + AMQP technology binding on a SOSA Message Interconnect, the interaction shall be implemented using IPv4 or IPv6 at the Network layer.

15.4.5 Protobuf +ZMTP Technology Binding Rules

Rule 15.4.5-1: Where interactions between SOSA sensor components are implemented using the Protobuf + ZMTP technology binding on a SOSA Message Interconnect, the interaction message Data Definition shall be defined using Protobuf v3.0 or higher.

Rule 15.4.5-2: Where interactions between SOSA sensor components are implemented using the Protobuf + ZMTP technology binding on a SOSA Message Interconnect, the interaction message Data Encoding shall be implemented using Protobuf v3.0 or higher.

Rule 15.4.5-3: Where interactions between SOSA sensor components are implemented using the Protobuf + ZMTP technology binding on a SOSA Message Interconnect, the interaction message Encapsulation shall be implemented using ZMTP v3.0 or higher.

Rule 15.4.5-4: Where interactions between SOSA sensor components are implemented using the Protobuf + ZMTP technology binding on a SOSA Message Interconnect, the interaction shall be implemented using TCP at the Transport layer.

Rule 15.4.5-5: Where interactions between SOSA sensor components are implemented using the Protobuf + ZMTP technology binding on a SOSA Message Interconnect, the interaction shall be implemented using IPv4 or IPv6 at the Network layer.

15.4.6 NFS Transfer Technology Binding Rules

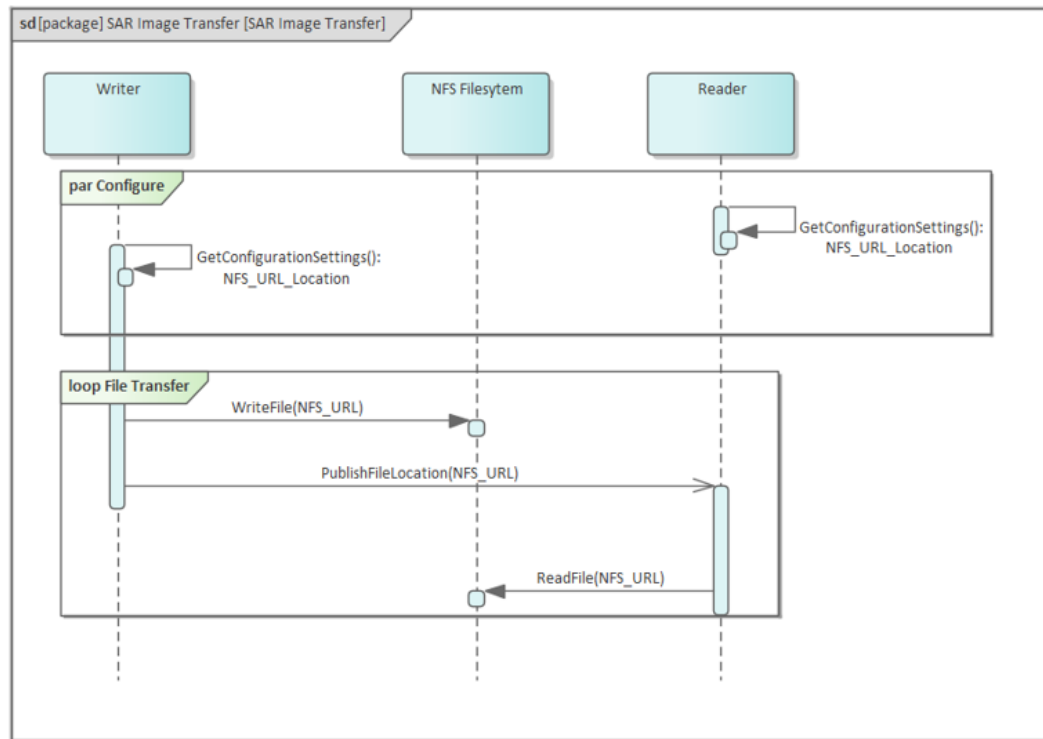


Figure 15.4.6-1: Sequence Diagram of General Flow of the File Transfer Interaction Type between the Writer and the Reader

Rule 15.4.6-1: Where a *sendImageProducts()* interaction is conducted on the SOSA Message Interconnect, that interaction shall be implemented using file transfer interaction type via NFS Version 3.x or greater.

Rule 15.4.6-2: Where a *sendImageProducts()* interaction is sending a SAR image, the SAR image shall be formatted using NITF 2.1.

Rule 15.4.6-3: Where a SOSA sensor component implements the role of Writer in a file transfer interaction, the SOSA sensor component shall publish the NFS file location written, using a publish-subscribe interaction type.

Rule 15.4.6-4: Where a SOSA sensor component implements the role of Writer in a file transfer interaction, the SOSA sensor component shall retrieve the file write location parameter from its configuration parameters and write all files into a path rooted at that location.

Rule 15.4.6-5: Where a SOSA sensor component implements the role of Reader in a file transfer interaction, the SOSA sensor component shall subscribe to the NFS file location publication and read the files from the location(s) specified.

Rule 15.4.6-6: Where a file transfer interaction type is implemented, the file location shall be formatted as per IETF RFC 2224.

Observation 15.4.6-1: The existence of an overarching file cleanup mechanism is unspecified.

Observation 15.4.6-2: The general flow of file transfer interaction type between the Writer and Readers is described in Figure 15.4.6-1.

Observation 15.4.6-3: Where a SOSA sensor component implements the role of Reader in a file transfer interaction, the SOSA sensor component can retrieve the file write location parameter for preparations such as creating file mounts prior to the file location being published.

15.4.7 Default Technology Binding Rules

Rule 15.4.7-1: Where an interaction between SOSA sensor components is conducted on the SOSA Message Interconnect using an interaction infrastructure with standard API and the interaction binding is not otherwise specified in another section of this document, the interaction infrastructure shall implement the interaction using one of the interaction bindings named in the column “Technology Binding” of Table 15.4.2-1 and for which the row for that technology binding contains a “Y” in the column relevant to the interaction type being implemented, and conforming to the rules defined in the relevant Technology Binding Rules section.

Rule 15.4.7-2: Where an interaction between SOSA sensor components is conducted on the SOSA Message Interconnect not using an interaction infrastructure with standard API and the interaction binding is not otherwise specified in another section of this document, the SOSA module shall implement the interaction using one of the interaction bindings named in the column “Technology Binding” of Table 15.4.2-1 and for which the row for that technology binding contains a “Y” in the column relevant to the interaction type being implemented, and conforming to the rules defined in the relevant Technology Binding Rules section.

15.5 Inter-Module Abstraction Overview

The SOSA Architecture is based on a set of loosely-coupled modular entities (known as SOSA modules) that interact with the underlying operating environment and with each other via well-defined logical interfaces.

15.6 Module Interaction Types

15.6.1 Security for Inter-Module Interactions

Securability is an important SOSA quality attribute that impacts many portions of this document. An important component of the securability of SOSA sensors is the ability for SOSA modules to securely interact with one another. The security guarantees for SOSA inter-module interactions are confidentiality, integrity, and authenticity. Confidentiality means that message content can only be viewed by those that are authorized. Integrity means that message content has not been altered. Authenticity means that the author of the message is who they say they are; i.e., that the message has not been forged by someone else. Any combination of these guarantees could be required or desired within a SOSA system for messages.

Certain messages within a SOSA system require security guarantees to minimize attack surface and guard the system against malicious acts designed to negatively impact the system and its mission. Security applied to messages that support the setup and execution of security controls ensures these security controls operate correctly. These include distribution of encryption keys, requests for authorization to access a critical resource or service, and handling of authentication information. Another purpose of inter-module interaction security is to provide an option for a

defense-in-depth strategy. While security is built into numerous aspects of SOSA systems, no system is completely immune from attacks and therefore a defense-in-depth strategy could be employed in case of partial system compromise.

There are certain nuances to providing confidentiality, integrity, and authenticity of messages for different interaction types that must be considered. All three security guarantees for request-response interactions can be accomplished by using symmetric keys. Confidentiality is provided by using an appropriate encryption algorithm. Integrity is provided by using either a Message Authentication Code (MAC) or an authenticated encryption cipher. Authenticity is also provided by a MAC or authenticated encryption. Integrity and authenticity can also be provided by using digital signatures.

For publish-subscribe and event notification interactions, a symmetric key must be shared between all publishers and subscribers of a message type to achieve confidentiality. Integrity can be achieved by using a single symmetric key shared between all publishers and subscribers if the intention is to protect against modification of messages by non-publishers and non-subscribers. Otherwise, receiver-specific symmetric keys must be used to compute MACs. If receiver-specific symmetric keys are used, the MAC also provides authenticity guarantees. Integrity and authenticity can also be achieved for these types of interactions using digital signatures.

Transport Layer Security (TLS) and Datagram TLS (DTLS) were selected to provide a means for providing confidentiality and integrity for inter-module interactions. This provides a minimum standard for protection for SOSA module interactions. Allowing TLS and DTLS to be enabled or disabled by the system integrator or acquirer promotes interoperability but still retains flexibility for systems that do not require that level of security or in cases where security is provided by other means. This version of the technical standard does not specify how configurability is achieved other than to permit different software or firmware loads which can be important in certain configurations to save on hardware resources.

Rule 15.6.1-1: Where inter-module interactions occur over TCP/IP and data-in-transit security is required, SOSA modules shall be configurable to enable or disable TLS 1.2 or higher. Conformance Methodology (D)

Rule 15.6.1-2: Where inter-module interactions occur over UDP/IP and data-in-transit security is required, SOSA modules shall be configurable to enable or disable DTLS 1.2 or higher. Conformance Methodology (D)

Note: Whether data-in-transit security is required is signified by the appropriate column in the interaction tables of each SOSA module.

Permission 15.6.1-1: Configurability may be achieved via different software or firmware loads for the same hardware.

15.6.2 Interaction Endpoints and Roles

As described earlier, interactions occur between SOSA modules and hardware elements. Table 15.1-1 describes the various types of interactions. Table 15.6.2-1 provides additional information related to the interaction types.




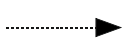
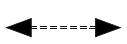

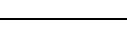

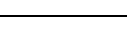
Each interaction type could be represented in diagrams with different line types or symbols (see the column titled “Symbol”). Interactions have two or more endpoints, represented by the left and right ends of the symbols in Table 15.6.2-1.

The SOSA module or hardware elements participating in an interaction play a specific role in the interaction, which is graphically indicated by which end of the symbol is connected to that module or elements in the drawing.

For example, consider a publish-subscribe interaction, described in Section 15.6.4. The module or element playing the role of publisher (or service) would have an attachment to the blunt end of the line, while those playing the role of subscribe (or client) would have an attachment to the arrow end of the line. In this case the direction of data flow is from the publisher to the subscriber, or with the arrow.

As a second example, consider the request-response interaction, described in Section 15.6.4. The SOSA module or hardware element that is making the request plays the role of requestor (or client). The SOSA module or hardware element to which the request is being made plays the role of responder (or server). The requestor is attached to the end of the line with the diamond, and the responder is attached to the end with the arrow. Note that the direction of data flow in this case depends upon the operation being requested. Possible operations include *set()* and *get()*. If the operation is *set()*, the data flow is toward the arrow (data is being provided by the requestor to the responder). If the operation is *get()*, the data flow is toward the diamond (from the responder to the requestor). Note that additional operations will be defined as needed.

Table 15.6.2-1: Interaction Roles, Endpoints, and Symbols

Interaction Type	Symbol	Left Endpoint Role	Right Endpoint Role	Direction of Data Flow
Analog Distribution		Sender	Receiver	With arrow
Digital Signal Stream		Sender	Receiver(s)	With arrow
Digital Signal Context		Sender	Receiver(s)	With arrow
Signal Layer Control		Controller	Subordinate(s)	N/A
Discrete		Writer(s)	Reader(s)	Bi-directional
Publish-Subscribe		Publisher(s) or Service(s)	Subscriber(s) or Client(s)	With arrow
Request-Response		Requestor or Client	Responder or Server	If Set; with arrow If Get: with diamond
Event Notification		(Event) Publisher or Server	(Event) Subscriber or Client	With arrow
File Transfer		Writer	Reader(s)	With arrow

An *interaction endpoint* is the part of a module or element that implements its role in the interaction. For example, a software module that publishes health information on a publish-subscribe interaction would implement a data publisher endpoint, while a module or element that is to receive that health data would implement a data subscriber endpoint.

Referring to Table 15.1-1, each interaction type has been assigned a default interconnect, which indicates which of the interconnects shown in Table 15.6.2-1 it will be mapped to by default. The following sections describe the interactions that are by default mapped to the Wideband Low-Latency Interconnect and the SOSA Message Interconnect.

15.6.3 Interactions on a Wideband Low-Latency Interconnect

Digital Signal Stream Interactions

Digital signal stream interactions are those where digital data is streamed between module interfaces. These interactions can be point-to-point (one interface sends a digital data stream and one interface receives the stream) or point-to-multi-point (one interface sends a digital data stream and multiple interfaces receive the same stream). One use-case for this type of interaction is streaming digital data between module interfaces with very low latency (on the order of 1usec). Examples of digital data streams include digital RF signals (e.g., real, or complex sample sequences), digital video streams, and temporal sequences of digital data products (e.g., power spectral density snapshots). These interactions will often be transported on the SOSA Wideband Low-Latency Interconnect (see Table 15.1-1). As shown in Table 15.6.2-1, the interaction endpoint roles are sender and receiver and the direction of the flow of data follows the arrow direction. There could be more than one receiver of a digital signal stream, as indicated by the (s) on the receiver endpoint role name.

Digital Signal Context Interactions

Digital signal context interactions carry data that describes the context of the digital signal streams. The metadata will often be transported on the same interconnection or incorporated with the digital signal stream or could be a separate interconnection and separate from the digital signal stream (e.g., ANSI/VITA 49.2 RF signal metadata). In some cases, the context metadata could be updated at a lower rate than the signals. As with the digital signal stream there could be more than one receiver.

Signal Layer Control Interactions

Signal layer control interactions are low-latency, very compact messages used to dynamically adjust parameters of the signal layer electronics that operate on raw signals. These must be transported on the Wideband Low-Latency transport. These interactions do not transport signal data, but affect the processing performed on the signals. As shown in Table 15.6.2-1, the signal layer control interaction roles are controller and subordinate. Controller(s) are connected to the blunt end, and subordinate(s) are connected to the arrow end. The direction of the arrow indicates the direction of control, not the flow of data. A signal layer control interaction could be used to control multiple subordinates, as indicated by the (s) in the signal layer control row in Table 15.6.2-1.

Discrete Interactions

Discrete interactions are intended to be used to minimize dedicated discrete signals between modular entities with virtual discrete registers, which are kept coherent through the exchange of low-latency, very compact messages over a network. Due to the use-case, these could only be feasible when implemented on a low-latency, dependable transport. Discrete interactions have endpoints with the role writer (which could both read and set the discrete value), and reader

(which could only read the discrete value). Two or more modules and/or elements participate in the discrete interaction to share the current value of the discrete interaction, simulating the behavior of a hard-wired signal with one or more writer and one or more reader.

Note that the network-based discrete values could only be used when performance or other requirements can be met using that technique. In cases where system safety and security requirements mandate them, physical discrete signals could still be implemented.

15.6.4 Interactions on a SOSA Message Interconnect

Publish-Subscribe Interactions

Publish-subscribe interactions are those where structured digital data is shared on a network between modules. These interactions are many-to-many, meaning a set of one or more module interfaces publishes (sends) data, and zero or more module interfaces subscribes (receives) data. This is a common interaction pattern supported in modern middleware. The digital data structure to be shared must be uniquely identified in the system. The data is published to a *topic*, to which multiple module interfaces can publish, and to which any number of module interfaces can subscribe. The topic is used to uniquely identify the data stream in the system to differentiate between the streams.

The structure and semantic of the shared data in publish-subscribe interactions is fixed and known *a priori* to execution. Referring to Table 15.6.2-1, one or more *publisher* modules or elements could send data to one or more *subscriber* modules. Graphically, this is shown as the blunt end of the arrow attached to the publisher(s), and the arrow end of the arrow attached to the subscriber(s). The direction of the data flow follows the direction of the arrow.

There are many methods of implementing the unique identifiers (topics), such as using unique ports and multicast addresses, or using industry standard middleware such as the OMG DDS middleware standard. This document has not yet determined how the publish-subscribe interactions will be implemented.

Request-Response Interactions

Request-response interactions follow a Service-Oriented Architecture (SOA) pattern, in which a module interface *provides* a service, *accepts requests*, acts upon the requests, and provides a *response*. This pattern is very commonly used in managing network-based systems and is supported by ubiquitous technologies such as Simple Network Management Protocol (SNMP), Simple Object Access Protocol (SOAP), and Representational State Transfer (REST) (otherwise known as RESTful web services).

These kinds of interactions are conceptually different from data exchanges, in that they are intentional, meaning that an operation is to be performed. These interactions are not naturally applicable to transferring large quantities or continuous streams of data, but instead are good-fit management operations. Referring to the graphical representation, the *requestor* module interface sends a *get request* or *set request* message (with a set of *request parameters*) to the end of the interaction with the diamond. The *responder* module interface receives the request from the end of the interaction with the arrow, acts upon it, and sends a *response* message back to the *requestor* module interface (possibly containing *response parameters*). The direction of the arrow follows the direction of the *operation*, not the flow of data.

Note that there are variables that exist in the implementation space for the request-response interaction protocol, including whether the interaction is blocking or non-blocking, and whether the interaction is point-to-point (between one user and one provider) or not. For some modules, an existing standard has been adopted, and thus the specific technologies and properties are defined by that existing standard. For example, the signal layer modules have adopted the Modular Open Radio Frequency Architecture (MORA) and Vehicular Integration for C4ISR/EW Interoperability (VICTORY) architecture standards. These request-response interactions are implemented using an SOA technology.

However, this document does not yet describe how all request-response interactions will be implemented. That will be done in a future version.

Event Notification Interactions

Event notification interactions are like publish-subscribe interactions except that they are sent only when important system or operational events occur, such as system faults and warnings, configuration changes, mode or state changes, and threat detections. The *publisher* role is *notification publisher*, and its operation is called *publish notification*. The subscriber role is *notification subscriber*, and its operation is called *subscribe to notification*. SOSA event notifications follow a publish-subscribe pattern. Event notifications are published as they occur. The publisher, or provider, *publishes notifications* to the end of the interaction with the closed circle, and the *subscriber*, or user, *subscribes to notifications* from the end of the interaction with the arrow. The direction of the arrow follows the direction of the notification.

File Transfer Interactions

File transfer interactions transfer data from one provider (writer) to one or more consumers (readers) using files written to a shared file system. The data provider writes an entire block of data to a file, then initiates a publish-subscribe interaction indicating the completion of the file write operation and location of the resulting file. Readers subscribe to and receive the published announcement that the file is ready to be read and open the file and read the data. This interaction type assumes that the writer and readers all have access to a shared file system that is in an arbitrary location accessible on the SOSA Message Interconnect. The interaction protocol is based on the shared understanding between writer and readers that the data is not complete or consistent until the notification with the file location has been published. This interaction does not specify any specifics of file locking, file name or location schemes, or whether or by whom the files are removed.

15.7 SvcV-3b: Services-Services Matrix

Planned for a future version of this document.

A AV-2 Integrated Dictionary

The SOSA AV-2 Integrated Dictionary, shown in Table 13.5.3.3.3-1, provides a unified set of definitions for terms that are either unique to the SOSA enterprise or could have different interpretations in different contexts. The SOSA AV-2 is not intended to be encyclopedic (not every term used in this document is included; omitted are terms which are well understood by practitioners in the field, or for which there are widely available definitions). The SOSA AV-2 is to be considered the single source of definitional truth for the SOSA enterprise.

Table 13.5.3.3.3-1: AV-2 Integrated Dictionary (Master Glossary of SOSA Terminology)

Term	Definition
Analysis	An element of verification that uses generally accepted technical methods, including mathematical models or simulations, algorithms, charts, graphs, circuit diagrams, data, or other scientific principles and procedures to determine conformance with specified requirements. “Generally accepted”, in this context, means in accordance with common design engineering practices.
Architecture	A set of descriptive representations of the fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.
Assignment	A request from inside the sensor system to a module to perform a mission-relevant function.
Audit Event	An event generated by a SOSA module that provides information that could be logged.
Behavior	The response (output data and resulting interactions generated) provided by a sensor system or module based on a particular set of stimuli.
Capability	A description of tasks or assignments a sensor system or module can do given its current health and configuration.
Closed Interface	Privately controlled system/subsystem boundary descriptions that are not disclosed to the public or are unique to a single supplier.
Cohesion	How well the hardware and software elements relate to the same abstraction and are necessary to implement that abstraction.
Collector Module	A module that receives audit events for the purposes of storage and/or analysis.
Compatibility	The ability of systems or elements to coexist without conflict or impairment or to be integrated or used with another system of its type.
Compliance	The degree to which a system, element, or interface adheres to an architecture or standard (the SOSA Consortium uses conformance instead).

Term	Definition
Configuration	How a sensor system or module is “set up” to operate.
Conformance	Whether a system, element, or interface completely adheres to an architecture or standard; conformance is the limiting case of 100% compliance.
Coupling	The strength of logical interconnectedness between elements, and the resulting impact that a change to one element has on other elements.
Cross-Sensor Cueing	The process whereby data or information from one sensor is used to direct (or bound) the target search of another sensor, regardless of whether the sensors are on the same vehicle or elsewhere.
Data Model	A depiction of the format and structure of the data elements and their logical interrelationships, as documented in DIV-1 (Conceptual Data Model), DIV-2 (Logical Data Model), and DIV-3 (Physical Data Model).
Data Products	Raw/unprocessed or minimally processed digital output, generally from a sensor, ideally structured to enable reuse (see Information Products).
Data Rights	An entity’s license rights to IP in the form of technical data and computer software.
Demonstration	An element of verification that involves the qualitative exhibition of functional performance. While test equipment might be required as part of the demonstration setup, measurements are typically not required. Demonstration might also be used when requirements or specifications are given in statistical terms (e.g., average power consumption, mean time to repair, etc.).
Deprecation	Equipment built to a legacy profile that is submitted for certification after that profile has been removed from the standard.
Detection	An observation that is determined to be differentiated from the ambient background (e.g., above a threshold for certain types of RF systems).
Directly Managed Sensor Component	A managed sensor component implemented with the in-band system management interfaces and capabilities <i>built-in</i> to the component itself to enable <i>direct</i> management of the component by the SOSA Module 1.1 System Manager.
Element	A basic hardware, software, or logical unit, component, or constituent of a system or subsystem.
Hardware Element	An all-encompassing term for hardware that is incorporated into a SOSA sensor.
Health	The collection of status, faults, and warnings describing the condition of a sensor system or module.
Heartbeat	A periodic signal sent between hardware and/or software modules to indicate normal (or abnormal) operation.
Indirectly Managed Sensor Component	A sensor component that is not directly managed, but for which in-band system management interfaces and capabilities are provided by a proxy (a second directly managed sensor component) in an <i>indirect</i> but still conformant manner.

Term	Definition
Information Products	Processed or reduced digital output, generally from a Processing Exploitation and Dissemination (PED) or mission system, ideally structured to enable reuse (see Data Products).
Inspection	An element of verification that involves an examination of the item/system or drawing form. Drawing forms are any controlled document that defines the product configuration for design, assembly, or test. Inspection could include gauging or measurement.
Interaction	The exchange of resources (signal or data) and behavioral responses between SOSA modules or hardware elements.
Interface	The region where two systems or elements interact.
Interoperability	The ability of systems, elements, or interfaces to provide data/information to – and accept the same from – other systems, and to use the data/information so exchanged to enable them to operate effectively together.
Legacy	Items that will be removed from the standard in a future version. See Section 13.2.13 for details.
Logging	The act of capturing data about the sensor, such as health, status, mode, and states in persistent storage for later retrieval and use.
Managed Sensor Component	A SOSA conformant entity that can be supervised via the capabilities and in-band system management interfaces of the SOSA Module 1.1 System Manager.
Metadata	Data about the data; ancillary information used to provide contextual information (e.g., position, orientation, timing, area of regard, and other state information).
Mode	A description of the discrete condition of a sensor system or SOSA module or hardware element in which the expected behavior is known. Modes are well-defined and finite.
Model	A representation of a system, element, or interface (and possibly its environment) often presented as a combination of drawings and text, or by using a modeling language.
Modular Open Systems Approach (MOSA)	The DoD’s approach to OSA. Based on five core elements including: establishing an enabling environment, employing a modular design, designation of key interfaces, use of open standards, and conformance testing. The preferred OSD acquisition term is Open Systems Architecture (OSA).
Modularity	The degree to which a system or element is composed of individually distinct physical and functional elements that are loosely coupled with well-defined interface boundaries.
Module	An architectural entity that has open, specified functional behaviors and interfaces, could be instantiated using hardware elements and/or software components and conforms to the complete definition (functionality, behavior, and interfaces) as defined in the SOSA Technical Standard.

Term	Definition
Notification	An interaction in which a sensor system or module reports the occurrence of an event when it occurs.
Open Architecture	An architecture in which stakeholders (or members of a community or open organization) have a say in the makeup and content of the architecture, and there exists a governance process to ensure that it is maintained, kept relevant, and meets the needs of the stakeholders, and a means to verify a system adheres to it.
Open Business Model	A business approach which requires doing business transparently to leverage the collaborative innovation of numerous participants across the enterprise permitting shared risk, maximizing asset reuse, and reducing total ownership costs.
Open Interface	An interface which conforms to an open standard (or architecture).
Open Source	Pertaining to or denoting software whose source code is available to the public to use, copy, modify, sublicense, or distribute.
Open Standard	A published standard in which stakeholders (or members of a community or open organization) have a voice in the makeup and content of the standard, and there exists a governance process to ensure that it is kept relevant and meets the needs of the stakeholders.
Open Systems Architecture	An architecture in which all components (modules) and their relationships (interfaces) are defined and documented in a way that is (1) accessible to all within the stakeholder community, (2) developed and governed by a consensus-driven body or bodies consisting of all interested parties, and (3) subject to conformance (or compliance) verification.
Platform	Refers to one of three things, which are context-dependent: a device (comprised of sensors and supporting environment), a vehicle (host), or computing infrastructure (comprising hardware and software). When the term is used, it must be preceded by phrasing that indicates the context.
Plug-and-Play	The property of a system, hardware, or software element to recognize that a component has been introduced and subsequently use it without the need for manual device configuration or operator intervention.
Plug-In Card	General: Any hardware element that is a circuit card that plugs into a backplane. Specific: A SOSA PIC is a PIC that conforms to a SOSA Slot Profile.
Pod	An integral part of a sensor that has elements from one or more SOSA sensors mounted in/on it.
Portable	An attribute that describes the reuse of existing (as opposed to the creation of new) hardware or software when moving hardware or software elements from one environment (physical or computing) to another.
Published Architecture (or Standard)	An architecture for which the interfaces (data model and interchange protocols) are widely known, used, or available to the target audience.

Term	Definition
Publish-Subscribe	A type of interaction in which one or more producers (publishers) make data available for sharing with zero or more consumers (subscribers).
Quality of Service	Shared characterization of data flows between SOSA modules such that producers and consumers of data can describe, agree to, and determine their behavior.
Real-time	Pertaining to, or consistent with, meeting the data, information, and event needs of time-critical or deterministic processes (as embodied in specified time constraints/deadlines).
Reconfigure	A process by which a hardware, software, or system element is reversibly modified in response to a mission or operational need.
Relay Event	A filter that processes an incoming audit event. The Relay module could forward the event to other Relay modules or Collector modules, or it could drop the event as a function of Relay module policies, which could be a function of other factors.
Request-Response	A kind of interaction in which a client module sends a “request message” to a service module, which acts upon the request, and replies with a “response message”.
Resilience	The ability of a system to continue or return to normal operations in the event of some disruption, natural or man-made, inadvertent or deliberate, and to be effective with graceful and detectable degradation of function.
Reuse	A benefit of standards-based hardware or software elements to be used again; for example, in a different system or environment from which it was designed, or to add new functionalities to a system with slight or no engineering development.
Safety-critical	A condition, event, operation, process, or item whose mishap or degradation could result in loss of system, vehicle, mission, or human life.
Scalable	The ability of an architecture to be used (1) from large to small platforms or (2) with few to many hardware and software elements, platforms, etc.
Secure	The property of a system such that its design renders it largely protected/inviolable against acts designed to (or which could) impair its effectiveness and operation and prevents unauthorized persons or systems from having access to data/information contained within.
Security Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence.
Sensor	A device or system that actively and/or passively estimates properties of another entity and produces quantitative data that will be subsequently processed or used (e.g., radar, sonar, IR focal plane, seismometer, etc.) and consist of one or more sensor element(s) mounted within or on the same host platform.
Sensor Management	The combination of functions and interactions that enable the SOSA sensor to accomplish its designated tasks and instantiated using the System Manager and Task Manager modules and their associated interfaces.

Term	Definition
Software Application	A software executable designed to allow a user to complete tasks.
Software Component	A unit of software that is incorporated into a SOSA sensor.
Standardized Interfaces	Interfaces for which the physical structure, electronic signaling, and/or logical (format, protocol) product are codified in the SOSA Consortium products.
State	One of a set of top-level conditions from the operational lifecycle of a module or sensor system.
Status	A description of the condition related to the performance or health of a module or sensor system.
Subsystem	See System.
SYSLOG	A standard for logging events, defined by IETF RFC 5424 (March 2009).
System	A group or collection of elements that together compose a useful capability. Systems can also relate to other systems in a system-of-systems context or be hierarchically arranged in system-subsystem combinations. A system in one context can be a subsystem in another.
Target	An entity of interest, possibly the result of a detection.
Task	A request from outside the sensor system to perform a mission-relevant function.
Test	An element of verification designed to provide data on functional features, performance, or equipment operation under fully controlled and traceable conditions. Tests generally use special instrumentation or test equipment to obtain accurate quantitative data for analysis. The data is used to evaluate quantitative characteristics. Testing implicitly requires analysis of the resulting test data.
Unmanaged Sensor Component	A SOSA conformant entity that is not capable of being supervised via the capabilities and in-band system management interfaces of the SOSA Module 1.1 System Manager.
Verification	The act of measuring/assessing conformance (or compliance, depending on the situation).

B SOSA Data Model and OpenAPI Specifications (Normative)

B.1 SOSA Data Model (DIV-1, DIV-2, and DIV-3)

The SOSA Domain-Specific Data Model for content related to the DIV-1 Conceptual Data Model, the DIV-2 Logical Data Model, and the DIV-3 Physical Data Model can be found in the following file:

- SOSA_TechStd_V2_SS1_DSDM

The IDL is available in the following file:

- SOSA_TechStd_v1_DSDM_IDL

B.2 System Manager In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- System Manager-SysMan-API.json

B.3 Generic SOSA Module In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- Module-SysMan-API.json

B.4 Security Services In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- SecurityServices-SysMan-API.json

B.5 Chassis Manager In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- ChassisManager-SysMan-API.json

B.6 PIC In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- PIC-SysMan-API.json

B.7 PIC with SW RTE In-Band System Management Interface OpenAPI Specification Definition

The OpenAPI Specification for this interface can be found in the attached file:

- PIC with SW RTE-SysMan-API.json

C Security Attributes SOSA Security Module Overlay for Specialty Signals (Available on the Air Force VLD Website)

Security Attributes SOSA Security Module Overlay for Specialty Signals is available on the US Air Force VLD website for the SOSA Technical Standard at:

https://restricted.vdl.afrl.af.mil/xythoswfs/webview/_xy-7055996_1

Acronyms and Abbreviations

2LM	2 Level Maintenance
AC	Alternating Current
ACK/NAK	Acknowledgement/Negative Acknowledgement
ADC	Analog to Digital Conversion
AFLCMC	Air Force Life Cycle Management Center
AJ	Anti-Jam
AMPS	Alternate Module Profile Scheme
AMQP	Advanced Message Queuing Protocol
AMTI	Air Moving Target Indicator
ANS	Alternate Naming Structure
API	Application Programming Interface
ARINC	Aeronautical Radio Inc.
ARP	Address Resolution Protocol
ARX	Receive RF Chain
ASIC	Application-Specific Integrated Circuit
AT	Anti-Tamper
ATX	Transmit RF Chain
AWG	Architecture Working Group
AVL	Approved Vendor List
BIOS	Basic Input/Output System
BIST	Built-In Self-Test
BIT	Built-In Test
BMB	Blind Mate Bullet
BSP	Board Support Package

C4ISR	Command, Control, Communications, Computers (C4), Intelligence, Surveillance, and Reconnaissance (ISR)
C5ISR	Command, Control, Communications, Computers, Cyber (C5), Intelligence, Surveillance, and Reconnaissance (ISR)
CAD	Computer-Aided Design
CDS	Cross-Domain Solution
CG	Center of Gravity
ChMC	Chassis Management Controller
CIK	Crypto Ignition Key
CLT	Common Launch Tube
CMI	Chassis Management Interface
CMM	Chassis Management Module
COTS	Commercial Off-the-Shelf
CoV	Certificate of Volatility
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CSfC	Commercial Solutions for Classified
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSP	Critical Security Parameter
CTS	Conformance Test Suite (FACE Technical Standard)
DAC	Digital to Analog Conversion
DARE	Data-At-Rest Encryption
DDS	Data Distribution Service
DiTE	Data-in-Transit Encryption
DMTF	Distributed Management Task Force
DoD	Department of Defense (United States)
DoDAF	Department of Defense Architecture Framework
DRD	Digital Receive Data
DTLS	Datagram TLS

EA	Electronic Attack
ECU	End Cryptographic Unit
EFI	Extensible Firmware Interface
EIA	Electronic Industries Alliance
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EO/IR	Electro-Optical/Infrared
ESC	Energy Storage Card
ESD	Electrostatic Discharge
ESM	Electronic Support Measure
EW	Electronic Warfare
FACE	Future Airborne Capability Environment
FCI	Flow Control In
FCO	Flow Control Out
FIPS	Federal Information Processing Standard
FOV	Field of View
FP	Fat Pipe
FPGA	Field-Programmable Gate Array
FRU	Field Replaceable Unit
GMTI	Ground Moving Target Indicator
GOTS	Government Off-The-Shelf
GPGPU	General-Purpose Graphics Processing Unit
GPIO	General-Purpose Input/Output
GPS	Global Positioning System
GPU	Graphics Processing Unit
HOST	Hardware Open Systems Technology
HPA	High-Power Amplifier

HTTP	Hyper Text Transmission Protocol
HWE	Hardware Element
HWG	Hardware Working Group
ICD	Interface Control Document
IDL	Interface Definition Language
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IGMP	Internet Group Management Protocol
IMI	Inter-Module Interface
I/O	Input/Output
IOSS	I/O Services Segment (FACE Technical Standard)
IP	Intellectual Property
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMC	Intelligent Platform Management Controller
IPMI	Intelligent Platform Management Interface
iSCSI	Internet Small Computer Systems Interface
ISR	Intelligence, Surveillance, and Reconnaissance
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
JTNC	Joint Tactical Networking Center
KMI	Key Management Infrastructure
LNA	Low Noise Amplifier
LO	Local Oscillator
LOS	Line-of-Sight
LRU	Line Replaceable Unit
LVC MOS	Low Voltage Complementary Metal Oxide Semiconductor

LVDS	Low Voltage Differential Signal
MAC	Message Authentication Code
MBSE	Model-Based Systems Engineering
MDM	MORA Data Message
MISB	Motion Imagery Standards Board
ML2B	MORA Low Latency Bus
MLD	Multicast Listener Delivery
MORA	Modular Open RF Architecture
MOSA	Modular Open Systems Approach
MOSC	Mission Operations Subcommittee
MWIR	Mid-Wave Infra-Red
NAVAIR	Naval Air System Command
NDA	Non-Disclosure Agreement
NEZ	No Emit Zone
NFS	Network File System
NIST	National Institute of Standards and Technology
NITF	National Imagery Transmission Format
NSA	NATO Standardization Agreement
NSA	National Security Agency
NVMe	Non-Volatile Memory Express
NVMRO	Non-Volatile Memory Read Only
OAS	Open API Specification
OCI	Open Container Initiative
OMG	Object Management Group
OMS	Open Mission System
OSA	Open Systems Architecture
OSD	Office of the Secretary of Defense
OSS	Operating System Segment (FACE Technical Standard)
OTNK	Over-the-Network Key

O-TTPS	Open Trusted Technology Provider Standard
OVF	Open Virtualization Format
PCB	Printed Circuit Board
PCIe	Peripheral Computer Interface Express
PED	Processing Exploitation and Dissemination
PEO	Program Executive Office
PIC	Plug-In Card
PICP	Plug-In Card Profile
PMD	Physical Medium Dependent
PNT	Position Time Navigation
PPS	Pulse Per Second
PSC	Power Supply Card
PSSS	Platform-Specific Services Segment (FACE Technical Standard)
PTTI	Precise Time and Time Interval
PXE	Preboot Execution Environment
QoS	Quality of Service
RAS	Reliability, Availability, and Serviceability
RDMA	Remote Direct Memory Access
REDI	Ruggedized Enhanced Design Implementation
REI	Run-time Environment Interface
REST	Representational State Transfer
RF	Radio Frequency
RIG	Reference Implementation Guide
RMF	Risk Management Framework
RMS	Root Mean Square
RoCE	RDMA over Converged Ethernet
RoT	Root of Trust
RTE	Run-Time Environment
RTM	Rear Transition Module

RTPS	Real-Time Publish Subscribe
Rx/Tx	Receive/Transmit
SAE	Society of Automotive Engineers
SAR	Synthetic Aperture Radar
SATA	Serial AT Attachment
SBC	Single Board Computer
SDK	Software Development Kit
SDM	Shared Data Model
SE	Single-Ended
SFF	Small Form Factor
SFFSC	Small Form Factor Subcommittee
sFPDP	Serial Front Panel Data Port
SIEM	System Information and Event Manager
SIGINT	Signals Intelligence
SLE	Support Level Ethernet (1 and 2)
SMA	SubMiniature, Version A
SMPM	SubMiniature Push-on Micro
SMTI	Surface Moving Target Indicator
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOSA	Sensor Open Systems Architecture
SSR	Solid State Relay
STANAG	Standardization Agreement
STAP	Space-Time Adaptive Processing
STIG	Security Technical Implementation Guide
SUAS	Small Unmanned Aerial System
SWaP	Size, Weight, and Power
SWIR	Short Wave Infra-Red

TCP	Transmission Control Protocol
TIA	Telecommunications Industrial Association
TIG	Technical Implementation Guide
TIM	Thermal Interface Material
TLS	Transport Layer Security
TNC	Threaded Neill-Councilman
TOA	Tactical Open Architecture
TSS	Transport Services Segment (FACE Technical Standard)
TWG	Technical Working Group
UART	Universal Asynchronous Receiver/Transmitter
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCI	Universal Command & Control Interface
UCS	UAV Control System
UDDL	Universal Domain Description Language
UDP	User Datagram Protocol
UI	User Interface
UoC	Unit of Conformance
USAF	United States Air Force
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTP	Ultra-Thin Pipe
VBAT	Voltage Battery
VDB	VICTORY Data Bus
VDC	Voltage Direct Current
VDD	Version Description Document
VICTORY	Vehicular Integration for C4ISR/EW Interoperability
VRT	VITA Radio Transport
VSWR	Voltage Standing Wave Ratio

XMC	Express Mezzanine Card
XML	eXtensible Markup Language
YAML	Yet Another Markup Language
ZMQ	ZeroMQ Message Transport Protocol

Index

2LM.....	104	DiTE.....	173
AFLCMC	1	DIV-1	36, 37
aircraft equipment.....	34	DIV-2	36, 37
airworthiness	35	DIV-3	36, 37
airworthiness certification	33	DMTF OVF.....	367
AMPS	203, 205, 227	DoD.....	1
AMPS String	227	DoD AT TIG.....	35
ANS	227	DoD RMF	35
ANSI/VITA 46.11	102	DoDAF.....	3
architecture principles	12	DTLS.....	380
ARP	243	EFL.....	200
ASIC.....	29	electrical interface	266
audit event	160	EMC/EMI	277
authentication service	166	Emitter/Collector.....	131, 137
authenticity	379	Encoded Data Extractor	155
authorization service.....	169	encryption.....	380
AV-2.....	3	encryption cipher.....	380
BSP.....	200	Encryptor/Decryptor	172
C5ISR	1	EO/IR	1
CAD	353	EO/IR sensor types.....	149
Calibration Service	178	event notification.....	384
CDS	162	EW	1
Chassis Manager	77, 80	External Data Ingestor.....	155
ChMC	103	FACE CTS	37
Class 1 & 2 connector	267	FACE OSS	357
Class 3 connectors	310	FACE OSS Interface	362
Class 5	345	FACE OSS Profile	362
CLT	345	FACE OSS RTE profile	360, 361
CMM	103	FACE TSS.....	37, 372
Compressor/Decompressor.....	179	FACE UoC.....	361
Conceptual Data Model.....	36	file transfer	384
Conditioner-Receiver-Exciter.....	129, 134	FPGA	104
confidentiality.....	379	general mechanical requirements	186
configuration file	358	Generic SOSA module	62, 65
conformance certification	5	GPGPU	210
Conformance Product Set.....	6	GPU.....	104
Container RTE profile	362	Guard/Cross-Domain	177
Convey	159	hardware PICP	183
cooling method.....	190	Host Platform Interface	180
CoV	204	ICD.....	35
CPLD.....	201	IDL.....	391
CSP.....	170	IDS	160
CV-1	1	Image Pre-Processor.....	152
cybersecurity	35	IMI	120
DARE.....	157	Impact Assessor & Responder	157
digital signal context	382	in-band system management	41
digital signal stream.....	382	in-band system management	46
digital signatures	380	in-band system management	84
discrete (interaction).....	383	integrity	379

interaction	38	PMD	239
interaction binding	374, 375	PNT	212
interaction endpoint	133, 382	Power	182
interactions	369, 380	Power Enable	278, 320
IPMB	102	Process Signals/Targets	150
IPMC	30, 102	procurable unit	31
IPMI/IPMB	30	protocol field	227
iSCSI	173	protocol modifier	227
J1-DC Power Connector	270	PSC	103
J2-Signal Connector	272	PSC general rules	191
J3-Video Connector	323	publish-subscribe	383
JSON	46, 358	PXE	158
key management	163	QoS nomenclature	372
KMI	164	qualification	35
legacy	224	quality attributes	10
legacy PICP	224	RAS	103
Logical Data Model	36	Relay	160
LOS	279	Reporting Services	159
LVC MOS	201	request-response	383
LVDS	242	resilience	35
MAC	122, 380	REST	383
Maintenance Console Port	200	RF Signal Layer	132, 133, 140
MDM	135	RIG	3, 5
mechanical interface	266, 351	RoCE	173
mezzanine card	200	RoT	121
mission equipment	34	RTE	29, 356
ML2B	243	RTE profile	356
module state	116	sanitization	170
MORA	133, 384	SATA	173
MOSA	1, 29	SBC	205
MOSC	7	SDM	36
Nav Data Service	178	securability	379
NAVAIR	1	security	35
NDA	204	Security Manager	36
Network Subsystem	177	Security Services	160
NEZ	279	Security Services module	67, 73
NVMRO	107	sensor component	6
OAS	37	sensor interconnect	38
OCI	363	sensor state	111
OMS	35	SFF	253
OpenAPI Specification	391	SFFSC	7
OpenVPX	183	SIEM	161
OTNK	164	SIGINT	1
O-TTIPS	35	signal layer control	382
out-of-band hardware		Signal/Object Characterizer	151
management	101	Signal/Object Detector &	
out-of-band system management	41	Extractor	150
overlay	202	Situation Assessor	156
PCIe	173	SLE1	242
PEO	1	SLE2	242
Physical Data Model	36	SNMP	383
PIC	21, 88, 92	SOA	383
PIC electrical requirements	184	SOAP	133, 383
PIC state	113	software package verification	171
PIC with SW RTE	92	SOSA AV-2	385
PICP	30, 205	SOSA Business Guide	4

SOSA Certification Register	6	symmetric keys	380
SOSA Conformance Certification		SYSLOG	160
Policy	4	system management	32, 40
SOSA Conformance Program	4	System Manager.....	42, 47, 55
SOSA Contracting Guide	4	Task Manager.....	125
SOSA Data Model.....	36	taxonomy.....	31
SOSA ecosystem	3	thermal interface	258
SOSA hardware element	21	TIA 232	201
SOSA host platform	21	TIM	258
SOSA module.....	31	Time & Frequency Service	179
SOSA modules	35	TLS	380
SOSA Reference Architecture.....	3	transmission/reception.....	129
SOSA RTE	356	UART.....	201
SOSA sensor	20	UCI.....	180
SOSA sensor component.....	29	USAF	1
SOSA sensor pod	21	UTC.....	162
SSR.....	278	Utility Plane	184
start-up sequence	119	Verification Authority Register.....	6
state management	111	VICTORY	384
Storage/Retrieval Manager.....	157	VICTORY architecture	133
SUAS.....	345	Virtual Machine profile	367
supplier	6	Virtual Machine RTE profile	365
SV-1	19	VNX+.....	183, 253
SvcV-1.....	21	XML.....	133, 358
SvcV-2.....	27	YAML.....	358
SvcV-3b.....	384	zeroization	170
SvcV-4.....	43		