NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

NGA.SP.0009.04_1.0.1_SIFTDDIL
2019-08-02

National System for Geospatial Intelligence (NSG)
and
United States MASINT System (USMS)
Sensor Integration Framework (SIF)
Standards Profile (SP)
Technical View 3 – Tactical DDIL IP Environment

(2017-08-02)

Version 1.0.1

NATIONAL CENTER FOR GEOSPATIAL INTELLIGENCE STANDARDS

Change Log

Version	Approval Date	POC	Change Description
1.0.0	12/14/17	C. Heazel	Initial Release
1.0.1	08/02/19	C. Heazel	Updated ontology references, clarified conformance classes and enterprise mapping.

Forward

Sensing systems come in many shapes and sizes. From complex space-based telescopes which measure the background radiation of the Universe, to disposable stick-on thermometers. Likewise the degree of access to sensing systems varies widely. From direct connections to the high-speed Internet to hanging off the end of a low-speed, low quality, intermittent communications link. Yet, it is highly desirable that any authorized user should have access to any sensor and the data that it produces, from anywhere, and at any time. Clearly there is no single suite of technology which can do that. Likewise there is no single set of standards which can support that goal. This is the problem that the Sensor Integration Framework Standards Profile (SIF-SP) attempts to solve.

The SIF-SP establishes an architecture framework to decompose sensing systems into their constituent parts, and identify standards suitable for each of those parts. This framework is defined at two levels. The Reference View (RV) provides an abstract architecture framework. This level is agnostic to any specific technology. It captures the essence of what a sensor system needs to do regardless of how it is implemented and what domain it targets. Technical Views (TV) apply the Reference View architecture framework to a specific technology environment. TVs not only provide specific instruction on how to implement the SIF using a specific technology, they also specify how that implementation maps back into the Reference View. By tracing every Technical View back to the Reference View, the ability to achieve interoperability across technology environments is greatly enhanced.

This specification is Technical View #3 of the SIF-SP. It describes the implementation of the SIF architecture within the constraints of the Tactical DDIL (Denied, Degraded, Intermittent, or Limited bandwidth) IP (Internet Protocol) communications environment.

Table of Contents

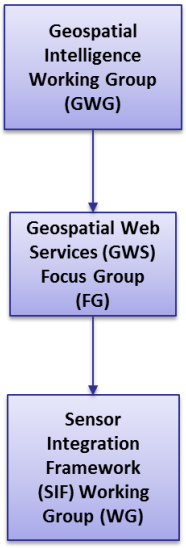
1 Introduction

1.1 Background

The purpose of this document is to provide guidance required for sensor data producers and consumers to implement a sensor information enterprise that meets operational requirements, achieves United States (U.S.) Department of Defense (DoD) and Intelligence Community (IC) Chief Information Officer (CIO) goals, and conforms to applicable policy. Additionally, this profile shall define conditions, specifically those applicable to defense computing environments limited by functional mission areas. This profile, while originating from the National Systems for Geo-Spatial Intelligence (NSG) and U.S. MASINT System (USMS) communities, is designed to accommodate the broadest range of sensor information use cases possible. Sensor information implementers can expect this document to 1) identify a collection of necessary standards; 2) constrain those standards to an adequate level of detail; 3) extend those standards as needed; 4) provide overall guidance to employ those standards together.

1.2 Scope

This Sensor Integration Framework Standards Profile (SIF-SP) is produced by the Sensor Integration Framework Working Group (SIFWG) of the Geospatial Web Services (GWS) Focus Group (FG) of the Geospatial-Intelligence Standards Working Group (GWG). The GWG serves as a U.S. Department of Defense (DoD), Intelligence Community (IC), Federal, and Civil community-based forum to advocate for IT standards and standardization activities related to GEOINT. The GWG performs two major roles:



1) As a Technical Working Group (TWG) of the DoD and IC CIO Joint Enterprise Standards Committee (JESC); and

2) As a coordinating body for the GEOINT community to address all aspects of GEOINT standards.

The SIF-SP describes an architecture and standards framework for the integration of sensors and sensor systems across all deployment environments. As such, the scope of the SIF-SP is overarching among the community and reaches across multiple areas of interest horizontally rather than vertically. It provides a framework which is applicable to all sensors, regardless of the intelligence discipline. Since almost all sensors have a spatial-temporal component, the GWG was chosen as the most appropriate authority to manage this work.

The purpose of the SIF-SP is to define a framework for the integration of standards-based capabilities. This profile is built around an architecture which is representative of sensing systems and the systems that use them. Standards are then mapped onto that Architecture providing the specifications needed for implementation.

The SIF architecture is documented in two levels:

- The Reference View presents an architecture which is independent of any implementing technology, the concepts presented apply to any implementation environment.
- Technical Views present architectures within the constraints of specific technology implementations. As there are multiple environments where sensing systems are deployed, so also

there are many Technical Views. Each Technical View is scoped to the technology constraints of a specific implementation environment.

The Technical View specified herein defines how the Reference View should be implemented by systems operating in the tactical environment with Denied, Disconnected, Intermittent, and Limited bandwidth (DDIL) communications environment constraints.

2 Context

This Technical View defines how the SIF-SP Reference View should be implemented for tactical IP-based sensors operating under DDIL constraints. This view leverages the Integrated Sensor Architecture (ISA). ISA is an Army solution that provides a distributed service-based architecture that enables sensors and systems to readily integrate into existing networks and to dynamically share information and capabilities to improve situational awareness within the tactical DDIL constraints. ISA has been leveraged for the Army Common Operating Environment solution for the Sensor Computing Environment. ISA-using systems communicate and behave as specified in the ISA Interface Control Document and ISA Component Requirements, and ISA infrastructure components communicate and behave as specified in these documents plus the ISA Controller Requirements.

2.1 Tactical DDIL IP Environment

The tactical DDIL IP environment has the following characteristics, which have motivated the architecture, capabilities and technologies employed for ISA:

- **Secure**: Tactical domain necessitates authentication of communicating components, authorization of requested actions and confidentiality of in-transit communications.
- **Disconnected**: Subject to interruption of communication and inability to establish connectivity, requiring an ability to operate properly when disconnected from other nodes.
- **Low Bandwidth**: Significantly constrained communication throughput, necessitating use of bandwidth-efficient data encoding and limitations on the size and frequency of data transmission.
- **Segmented**: Both the entire environments and subsets of sensors and nodes will be limited in ability to maintain access within the environment and with the enterprise.
- **Unreliable**: Packet loss and corruption is common, requiring use of reliable communication mechanisms.
- **Mobile**: Tactical environment requires support to both static and mobile nodes. Mobility may impact and exacerbate security, bandwidth, connectivity, and reliability.

In selecting whether to adopt the Tactical DDIL IP technical view or another technical view, users must provide a holistic assessment of the suitability of each for the systems to be employed. Individual parameters such as bandwidth availability will inform, but not determine, technical view selection and must be considered in conjunction with other parameters. For example, bandwidth that is sufficient for a single sensor's feed may not be sufficient for multiple feeds or when overall network load is considered. The ultimate selection of this technical view is a program/system decision.

2.2 Integrated Sensor Architecture (ISA)

The information that is communicated for the ISA solution is defined in the ISA data model. ISA information is exchanged by passing messages between components. Two main forms of message passing are supported: Publish-Subscribe and Request-Response.

ISA provides a service that achieves Publish-Subscribe message passing. Components create subscriptions with the service to establish criteria that defines which published messages are desired. When a message is published, the service compares the message against all established selection criteria. Whenever there is a match, a copy of the message is sent to the corresponding subscriber.

ISA supports Request-Response message passing through routing of messages between requesters and performers. A requester constructs a request message that indicates what task is being requested, contains any inputs to that task and is addressed to the targeted performer. ISA checks if the request is authorized and, if so, routes the request to the performer. The performer receives the message, performs any required processing, and returns one or more response messages containing the results of the processing. ISA routes the response message(s) to the requester. More than one response message would be generated if a request is queued for execution or if the request is for an ongoing task (e.g., monitoring an area).

ISA supports various schemes for encoding messages, but the encoding scheme that must be used in a tactical DDIL environment is Google Protocol Buffers (ProtoBuf). ProtoBuf provides a bandwidth-efficient encoding technique, which is essential given the commonly limited bandwidth of this environment

3 Conformance

3.1 Introduction

What is conformance?

An organization complies with NSG Directive 3201, The Geospatial Intelligence (GEOINT) Functional Manager Standards Assessment (GFMSA) Program, when that organization assesses an item, and asserts the degree to which that item conforms to GEOINT standards.

What is the definition of conformance?

ISO 19105-2000 (r2006) Geographic Information – Conformance and Testing defines conformance as: “The fulfilment of specified requirements.”

An item conforms to a GEOINT standard when it fulfills:

- The mandatory requirements of the standard, and
- The conditional requirements of the standard (when the stated conditions apply), and
- Those optional requirements of the standard needed to enable the purpose of the item.

Conformity assessment is a demonstration, whether directly or indirectly, that specified requirements relating to a product, process, system, person, or body are fulfilled. Conformity assessment includes sampling and testing, inspection, supplier’s declaration of conformity, certification, and management system assessment and registration. Conformity assessment also includes accreditation of the competence of those activities.

Why is conformance important?

- The objectives of standardization cannot be completely achieved unless data and systems can be assessed to determine whether they conform to the relevant GEOINT standards.
- The ability of devices to work together relies on data and services conforming to standards in the same way.
- Promotes consistency of interpretation and implementation of GEOINT standards.
- Reduces risk that undetected defects will have adverse operational impact.
- Raises user confidence that GEOINT data and services are dependable and trusted.
- Promotes DoD/IC objectives for competition in acquisition among multiple suppliers.

3.2 SIF-SP TV-3 Conformance

The SIF-SP Reference View provides an architecture framework which is agnostic to the implementing technology. This SIF Technical View extends that architecture within the technical constraints of the Tactical DDIL IP networking environment as supported by the Integrated Sensor Architecture (ISA).

Conformance with this Technical View is defined by two conformance classes.

- **Integrated Sensor Architecture (ISA).** The first conformance class defines conformance with the technology infrastructure as defined by the ISA body of specifications. This is required of any implementation which claims conformance with SIF-SP TV-3.
- **Sensor Web Enablement (SWE) Bridge.** The second conformance class defines conformance with the specifications for integration of ISA systems with the Enterprise domain. Conformance with this class is required of any ISA node which will serve as an intermediary between the Tactical DDIL and Enterprise environments.

Details on the specific requirements for each Conformance Class and corresponding abstract tests are provided in Annex A.

4 Related Specifications

4.1 Normative Specifications

- ASPRS, LAS Specification Version 1.4-R13, 15 July 2013
- CIPA DC-008-2016, Exchangeable image file format for digital still cameras: Exif Version 2.3.1, July 2016
- IETF RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace, July 2005
- ISA Component Requirements, Release 6.0, Revision 2, 6 September 2016
- ISA Controller Requirements, Release 6.0, Revision 2, 6 September 2016
- ISA Data Model Specification, Release 6.0, Revision 3, 6 September 2016
- ISA Interface Control Document, Release 6.0, Revision 3, 6 September 2016
- ISO/IEC 15444-1:2016, Information technology -- JPEG 2000 image coding system: Core coding system, October 2016
- ISO/IEC 15444-2:2004, Information technology -- JPEG 2000 image coding system: Extensions, May 2004

- ISO/IEC 15948:2004, Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification, March 2004
- ITU-T Rec. X.667, Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components, September 2004
- ITU-T T.808, JPEG 2000 Interactive Protocol (Part 9 – JPIP), January 2005
- MIL-STD-2500C, National Imagery Transmission Format (Version 2.1), 01 May 2006
- MIL-STD-2500C, National Imagery Transmission Format (Version 2.1) Change Notice (CN) 1, 01 February 2017
- MISP-2019.1, Motion Imagery Standards Profile (MISP), November 2018
- NGA.SP.0009.01_1.0.1_SIFR, National System for Geospatial Intelligence (NSG) Sensor Integration Framework Standards Profile (SIF-SP) Reference View, 2 August 2019.
- ODNI IC.ID.V1, Intelligence Community Identifier (GUIDE ID) v1, 10 April 2013
- OGC 07-036, OGC Geography Markup Language v3.2 (also published as ISO 19136:2007, Geographic information — Geography Markup Language), 27 August 2007
- OGC 10-004, OGC Observations and Measurements v2.0 (also published as ISO/DIS 19156:2010, Geographic information — Observations and Measurements), 17 September 2013
- OGC 12-000, OGC® SensorML: Model and XML Encoding Standard v2.0, 4 February 2014
- OGC 12-006, OGC® Sensor Observation Service Interface Standard v2.0, 16 April 2012
- OGC 09-000, OGC® Sensor Planning Service Implementation Standard v2.0, 28 March 2011
- OGC 08-094, OGC® SWE Common Data Model Encoding Standard v2.0, 4 January 2011
- OGC 06-121, OGC® Web Services Common Implementation Specification v2.0, 7 April 2010
- OGC 09-001, OpenGIS® SWE Service Model Implementation Standard v2.0, 21 March 2011
- OSGeo, GeoTIFF Format Specification, Version 1.8.2, Revision 1.0, 10 November 1995
- SIF-SP Ontology, https://github.com/ngageoint/Sensor_Integration_Framework
- SIF-SP UML Model, https://github.com/ngageoint/Sensor_Integration_Framework

4.2 Informative Specifications

- Google Protocol Buffers, https://developers.google.com/protocol-buffers/
- ISA Background and Motivation, Release 6.0, Revision 3, 6 September 2016
- ISA Software Design Document, Release 6.0, Revision 3, 6 September 2016
- ISA Technical Overview, Release 6.0, Revision 3, 6 September 2016

5 Terms and Definitions

The SIF-SP Terms and Definitions can be found in Annex B .

6 Abbreviations

The SIF-SP list of abbreviations can be found in Annex C.

7 Information Viewpoint

7.1 Descriptions

The SIF concept of descriptions is fundamental to how ISA operates. Upon joining an ISA environment, an ISA-compliant component declares its capabilities, specifically information it can report about its state (properties), information it can report about observations it can make (observables) and tasks that it can be requested to perform (commands). This full set of ISA declarations maps to the SIF concept of a Performer Description, with ISA property, observable and command declarations mapping to SIF Property, Observable and Command Descriptions, respectively. ISA declarations are communicated via the ISA Config message.

7.1.1 Resource Description

The general concept of a SIF Resource Description defined for the SIF-SP Reference View is not relevant to ISA.

7.1.2 Property Description

ISA properties are information that an ISA component can report about its own state. Standard ISA properties are defined in Section 3.1 of the ISA Data Model Specification. A component declares support for ISA properties in an ISA Config message using the data structure presented in Table 1, as specified in Section 7.0 of the ISA Data Model Specification. ISA property declarations map to SIF Property Descriptions.

Field	Data Type	#	Description
name	String	1..1	Name of the property.
description	String	1..1	Description of the property.
type	Type	1..1	Data type used to capture the property value.
mutability	Mutability	1..1	Whether the property is read-only, write-only, or read-write.
structure	Structure	1..1	Whether the property is a single value or a list of values
range	Range Declaration	0..1	If present, defines validity rules for the value of the property. The value must lie within bounded ranges or be equal to discrete ranges.
threshold	Threshold Declaration	0..1	Thresholds for the property value that will cause Status messages to be emitted (regardless of the status interval).

Table 1: ISA Property Declaration

7.1.3 Observable Description

ISA observables are information that an ISA component can report about observations that it is capable of making. Standard ISA observables are defined in Section 3.2 of the ISA Data Model Specification. A

component declares support for ISA observables in an ISA Config message using the data structure presented in **Error! Reference source not found.**, as specified in Section 7.0 of the ISA Data Model Specification. ISA observable declarations map to SIF Observable Descriptions.

Field	Data Type	#	Description
name	String	1..1	Name of the observable.
description	String	1..1	Description of the observable.
type	Type	1..1	Data type used to capture the observable value.
structure	Structure	1..1	Whether the observable is a single value or a list of values
range	Range Declaration	0..1	If present, define validity rules for the value of the observable. The value must lie within bounded ranges or be equal to discrete ranges.

Table 2: ISA Observable Declaration

7.1.4 Command Description

ISA commands are tasks that an ISA component is capable of performing upon request. Standard ISA commands are defined in Section 3.3 of the ISA Data Model Specification. A component declares support for ISA commands in an ISA Config message using the data structure presented in **Error! Reference source not found.**, as specified in Section 7.0 of the ISA Data Model Specification. ISA command declarations map to SIF Command Descriptions.

Field	Data Type	#	Description
name	String	0..1	Name of the command.
args	Parameter Declaration	0..n	Input values to the function associated with this command.
description	String	0..1	Description of the command.
results	Result Declaration	0..n	Return values that can be expected when invoking this command.

Table 3: ISA Command Declaration

7.1.5 Parameter Description

As presented in Section 7.1.4, ISA commands can have arguments that serve as inputs to the functionality invoked by the command and can have results of the invocation. The argument and result details of the ISA commands supported by an ISA component are described within the command declarations provided in the component's Config message. Specifically, argument details are described via the ISA Parameter Declaration data type, and result details are described via the ISA Result Declaration data type. Both data types map to the SIF Parameter Description.

7.1.6 Performer Description

An ISA component captures its full set of declarations of supported properties, observables and commands in a single document called a Component Capability Description (CCD). A CCD is created using the data types defined in Section 7.0 of the ISA Data Model Specification. An ISA component advertises its CCD via an ISA Config message sent at the beginning of a session. The message also contains the "ready" and "reporting" states of the declared capabilities. The ready state indicates if an implemented capability is enabled or disabled. The reporting state indicates if the reporting of an

implemented property or observable is enabled or disabled. An ISA component reports any changes to its CCD, ready states and reporting states via subsequent ISA Config messages.

The structure of the ISA Config message is defined in Section 6.0 of the ISA Data Model Specification, and is presented in Table 4 for convenience.

Field	Data Type	#	Description
source	UCI	1..1	Component that supports the declared capabilities.
identifier	Integer	1..1	Conversation-unique identifier for the message.
priority	Priority	0..1	Priority of a given message. 0 is highest. The default value is 80.
time	UTC	1..1	The time of the message creation.
stale	UTC	0..1	Time at which data contained in the message should be regarded as invalid.
ccd	Capability Declaration	0..1	Declarations of the properties, observables and commands supported by the component.
property states	Property State	0..n	Ready and reporting state of each declared property.
observable states	Observable State	0..n	Ready and reporting state of each declared observable.
command states	Command State	0..n	Ready state of each declared command.
extras	Name Value Pair	0..n	Additional information determined to be useful to provide.

Table 4 : ISA Config Message

An ISA Config message maps to a SIF Performer Description. Table 5 illustrates the mapping between these constructs.

SIF Performer Description		ISA Config Message		
Element	**#**	**Field**	**#**	**Comments**
definition	0..1	none		Not applicable
identifier	1..1	source	1..1	Identifier of the component whose capabilities are described in the message
name	0..n	none		ISA captures a component's name as an ISA property, which is reported via the ISA Status message.
security	0..1	none		Not applicable
commands (Command Description)	0..n	ccd (Capability Declaration) / commands	0..n	See Section **Error! Reference source not found.** for a mapping of ISA commands to SIF concepts
		command states	0..n	
extent	0..1	none		Not applicable
observables (Observable Description)	0..n	ccd (Capability Declaration) / observables	0..n	
		observable states	0..n	
pointOfContact	0..n	none		ISA captures point-of-contact information as ISA properties, which are reported via the ISA Status message.
position	0..1	none		ISA captures a component's position as an ISA property, which is reported via the ISA Status message.

SIF Performer Description		ISA Config Message		
Element	**#**	**Field**	**#**	**Comments**
properties (Property Description)	0..n	ccd (Capability Declaration) / properties	0..n	
		property states	0..n	
describes	0..1	none		Not applicable
executes	0..n	none	0..0	Not applicable
hasComponent	0..n	none	0..0	Not applicable
isPartOf	0..1	none		Not applicable

Table 5 : Mapping Between SIF Performer Description and ISA Config Message

7.1.7 Activity Descriptions

ISA Capability Declarations do not explicitly describe the Activities supported by the component.

7.2 Component Properties

SIF Component Properties map to ISA properties, representing the status of the ISA component itself. Standard ISA properties are defined in Section 3.1 of the ISA Data Model Specification. ISA properties are reported via the ISA Status message, the structure of which is defined in Section 6.0 of the ISA Data Model Specification, and is presented in Table 6 for convenience.

Field	Data Type	#	Description
source	UCI	1..1	Component for which status is being reported.
identifier	Integer	1..1	Conversation-unique identifier for the message.
priority	Priority	0..1	Priority of a given message. 0 is highest. The default value is 80.
time	UTC	1..1	The time of the message creation.
stale	UTC	0..1	Time at which data contained in the message should be regarded as invalid.
properties	Name Value Pair	0..n	Values of the component properties.

Table 6 : ISA Status Message

Each relevant SIF Component Property maps to the *properties* field of the ISA Status message, using the *name* and *type* elements from the SIF Property Description for the particular property.

7.3 Observables, Observations, and Measurements

Observables, Observations, and Measurements represent three levels of abstraction for the results of sensing and processing activities. Each level builds on the information captured by the previous levels. As a result, the boundaries between these three concepts are rather porous. Different technologies may draw the lines a little differently. But in all cases implementations of these concepts should form a coherent whole.

7.3.1 Observables

The phenomena that an ISA component can detect and report on are described by the observable declarations (Table 2) provided in the component's Config message. These declarations not only serve as descriptive metadata, they also provide a template for use when populating a sensor observation. A Chemical Reading, for example, will always be captured using a single entity of type Chemical Reading. Chemical Reading type is a complex data structure containing the sensor output, derived measures, and support metadata necessary to understand the first two items. Every chemical reading collected by a component will conform to this structure.

7.3.2 Observations

Observations are instantiations of observables. In ISA, observations/observables are reported via the ISA Event message, the structure of which is defined in Section 6.0 of the ISA DMS (presented in Table 7 for convenience). ISA Event messages provide context for a collection event. The information collected by the component for an observation are reported through the observables field. This field is a set of name-value pairs where the name is the observable name and the value is a data element of the appropriate type for that observable. Standard ISA observables are defined in Section 3.2 of the ISA Data Model Specification.

Field	Data Type	#	Description
source	UCI	1..1	Component that generated and/or recorded the observation information contained in this message.
identifier	Integer	1..1	Conversation-unique identifier for the message.
priority	Priority	0..1	Priority of a given message. 0 is highest. The default value is 80.
time	UTC	1..1	The time of the event occurrence.
stale	UTC	0..1	Time at which data contained in the message should be regarded as invalid.
event ID	Event ID	1..1	Integer key, unique per component, which allows that event to be updated and referred to at a later point.
event reference	Event Reference	0..1	Unique ID that can be used to update the event information.
type	Event Type	1..1	In general terms, the reason this event was created. The default value is Other.
observables	Name Value Pair	0..n	Set of fields published within any Event message.
detector properties	Name Value Pair	0..n	Properties of the detector when the event occurred if those properties are different from the last status.

Table 7: ISA Event Message

The mapping of ISA Event message fields to SIF Observation elements is provided in Table 8. Since an ISA Event message can contain multiple observables, a single Event message can report multiple SIF Observations.

SIF Observation		ISA Event Message		
Element	**#**	**Field**	**#**	**Comments**
identifier	1..1	event ID	1..1	Identifier of observation, which is unique for the component
position	1..1	detector properties / Position	0..1	Retrieve the position property from the message. If a position property is not contained in the message, use the position most recently received in a Status message.

SIF Observation		ISA Event Message		
Element	**#**	**Field**	**#**	**Comments**
phenomenonTime	1..1	time	1..1	Note that this is the time that the message was created. For ISA sensors the two should be equivalent.
resultTime	1..1			
validTime	0.1	stale	0..1	
NA		detector properties	0..n	Properties of the component when the observation was made, if those properties changed since the last Status message and are relevant to the observation.
resultQuality	0..1	none		Each measured ISA observable includes an error field that captures the quality of the measurement. ResultQuality can be calculated from this data if desired.
producedThrough	1..1	source	1..1	The identifier of the ISA component that made the observation.
target	1..1	observables	0..n	Observables are name-value pairs where the name is from a controlled vocabulary of Observable types. These types approximate the Target/Observed Property concepts. Values correlate with the value half of the name-value pair.
Observed Property	1..1			
Values	1..1			
reports	0..n	event reference	0..1	Key value which is unique for the component
NA		type	1..1	Identifies the type of event: Alarm, Alert, Detection, Measurement, Other. Default value is “Other”.

Table 8: Mapping Between SIF Observation and ISA Event Message

7.3.3 Measurements

The primary purpose of a sensor system is to provide a digital representation of a real-world phenomenon. Just as there are many different types of phenomenon, there are many ways of representing phenomenon digitally. Measurements are the digital representations of observed phenomena. The SIF-SP Reference View provides the taxonomy of digital representations (Measurements) illustrated in Figure 1.

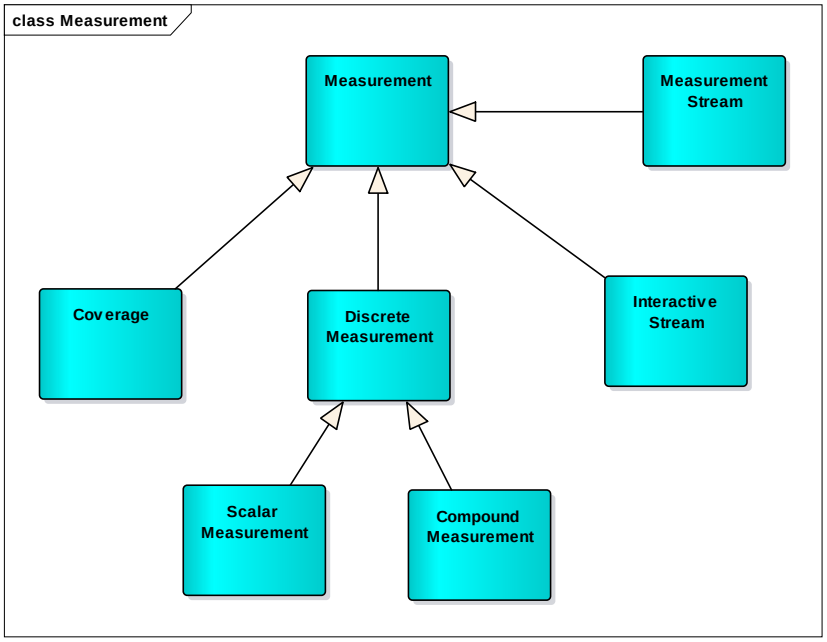


Figure 1: Measurement Taxonomy

SIF Measurements by themselves are just a collection of one or more values. To be useful, users also need to know the context and conditions under which the Measurement was taken. This information is captured in measurement metadata. Therefore, each SIF Measurement definition must also address how the measured value is associated with its' supporting metadata.

ISA reports SIF Measurements using Event messages, which are described in Section 4.3.2. Typically, the observables field of the Event message would capture the Measurement, and the rest of the Event message fields are metadata describing the content and conditions under which the Measurement was collected. Hence, for most SIF Measurements, the Measurement would be embedded with the metadata, inherently associating the Measurement and metadata.

However, the ISA Media observable is a special case. Rather than provide a measured value, the Media observable identifies where and how the Measurement can be retrieved. The Measurement itself is a resource that exists separate from the Event message. The ISA Media observable provides identifying information that includes a description of the resource type and a Uniform Resource Locator (URL) to where the resource can be accessed. While this approach can be used for any SIF Observable type, it is particularly applicable to Streaming and Coverage measurements.

The ISA Media observable imposes an additional requirement on the Measurement. Since the Measurement is a separate resource, it cannot rely on the Event message to supply metadata. The measurement metadata must be packaged with the Measurement itself. Not every encoding format can support that requirement. Therefore, Table 9 lists the standards and specifications to be used for each of the SIF Measurement types.

SIF Measurement Type	Specification	Comments
Measurement Stream	MISP	A multiplexed stream consists of one MPEG essence stream with at least one MPEG metadata stream.
Interactive Stream	JPIP	
Scalar Measurement	ISA DMS	

SIF Measurement Type	Specification	Comments
Compound Measurement	ISA DMS	
Coverage	Multiple	See Table 10

Table 9: Media Observable Standards and Specifications

There are a number of data formats that can be used for the Coverage Measurement Type. Table 10 provides a list of coverage formats that should be used and why.

Format	Name	Description
JP2 / JPX	JPEG 2000	Required for JPIP access
Exif	Exchangeable image file format	Industry standard for commercial and consumer-grade cameras. Rich metadata support.
PNG	Portable Network Graphics	Yes if the Exif metadata chunk is populated. Else No since there is not sufficient metadata support.
NITF	National Imagery Transmission Format	NSG standard for Earth Observation imagery
GeoTIFF	Georeferenced Tagged Image File Format	Preference is to use the NSG version since it has a more rigorous metadata model.
LAS	LASer File Format	For point clouds

Table 10 : Coverage File Formats

7.4 Spatial-Temporal

The SIF concepts for space and time are captured in the SIF-SP Ontology. The ISA concepts for space are identical to those in the Ontology. ISA temporal concepts, however, are a subset. The mapping between ISA and SIF Spatial-temporal concepts is provided in Table 11.

SIF Concept	ISA Element	Comments
GeographicArc	GeographicArc	
GeographicEllipse	GeographicEllipse	
GeographicPolygon	GeographicPolygon	
GeographicPolyline	GeographicPolyline	
GeographicPosition	GeographicPosition	
TemporalInstance	UTC	
TemporalPeriod	none	Concept does not appear in the ISA Data Model

Table 11: Mapping Between SIF and ISA for Spatial-Temporal Elements

8 Computational Viewpoint

8.1 Messaging

The primary means of message exchange within ISA is Publish-Subscribe, which is employed for the Config message presented in Section 4.1.5, the Status message presented in Section 4.2 and the Event message presented in Section 4.3.2. The other primary means of message exchange is Request-Response, which is used for command invocation. The ISA Request message is used to request the execution of a command, and the ISA Response message is used by the executing component to provide the status and results of the execution. The standard ISA commands are defined in Section 3.3 of the ISA Data Model

Specification. For each command, the command name, input parameters (if any) and result data (if any) are specified.

The structure of the ISA Request and Response messages are defined in Section 6.0 of the ISA Data Model Specification, and are presented in Table 12 and Table 13, respectively, for convenience.

Field	Data Type	#	Description
source	UCI	1..1	Component that is making the request.
identifier	Integer	1..1	Conversation-unique identifier for the message.
priority	Priority	0..1	Priority of a given message. 0 is highest. The default value is 80.
time	UTC	1..1	The time of the message creation.
stale	UTC	0..1	Time at which data contained in the message should be regarded as invalid.
request id	Integer	1..1	Reference uniquely identifying the request
command	String	1..1	Name of the command to be invoked.
parameters	Name Value Pair	0..n	Input parameters to the command execution.
access control	Name Value Pair	0..n	Parameters used to evaluate authorization of the request, as dictated by policy.

Table 12: ISA Request Message

Field	Data Type	#	Description
source	UCI	1..1	Component that was requested to execute a command.
identifier	Integer	1..1	Conversation-unique identifier for the message.
priority	Priority	0..1	Priority of a given message. 0 is highest. The default value is 80.
time	UTC	1..1	The time of the message creation.
stale	UTC	0..1	Time at which data contained in the message should be regarded as invalid.
reference	Integer	1..1	Identifier of the Request message to which this Response message corresponds.
type	Response Code	1..1	Status of the execution of the command.
values	Name Value Pair	0..n	Return values due to the execution of the command, if applicable.
error	String	0..1	Human-readable error description, if applicable

Table 13: ISA Response Message

Each relevant SIF Command maps to the ISA Request and Response messages. The *name* and *inputs* elements of the SIF Command Description map to the *command* and *parameters* fields, respectively, of the ISA Request message. The *outputs* element of the SIF Command Description maps to the *values* field of the ISA Response message.

The standard ISA commands map to the various SIF Capabilities specified in the SIF-SP Reference View. Table 14 presents the standard ISA commands that map to the SIF Messaging Capability.

ISA Command	Description
Add Subscription	Accepts a data filter script and uses it to control the data being sent to the subscribing component
Remove Subscription	Removes a currently active subscription.

Table 14: ISA Commands for SIF Messaging Capability

8.2 Discovery

The SIF-SP Reference View decomposes the Discovery capability into four activities. Those activities are described in Table 15.

SIF Activity	Description
Browse	The act of discovering new resources by following associations between the metadata cards.
Describe	The act of drilling down from a metadata card into more detailed information about a specific resource.
Register	The act of creating metadata for a resource and submitting that metadata to a Discovery Service.
Submit Query	The act of submitting selection criteria to a Discovery Service and receiving metadata cards in response.

Table 15: SIF Discovery Activities

The primary means of performing discovery in an ISA environment is to subscribe to ISA Config and Status messages. ISA Config messages are sent when a component joins the network and whenever a CCD or capability state (ready/reporting) changes. ISA Status messages are sent at regular intervals. Each message identifies the component that originated the message, when the message was originated, and the current configuration or status. In order to save bandwidth, Status messages only report information that has changed since the last report.

There are also a number of discovery-related ISA commands that are defined in the ISA Data Model Specification. These commands map to SIF Discovery Activities specified in the SIF-SP Reference View, as presented in Table 16.

SIF Activity	ISA Command	ISA Command Description
Submit Query	Discover	Accepts a data query that determines which messages and ucis are returned.
Describe	Get Config	Retrieves the current configuration of the receiving component.
Describe	Get Last Operation State	Retrieves the last operation state that matches the provided state.
Describe	Get Operation State History	Get the past operation states for the component
Describe	Get Property	Retrieves the value of the named property.
Describe	Get Status	Retrieves the current status of the receiving component
Submit Query	History	Accepts a data query and returns a resource where the user can access the data that satisfies that query.

Table 16: Mapping Between SIF Discovery Activities and ISA Commands

8.3 Delivery

The SIF-SP Reference View identifies three SIF Delivery Capabilities, as illustrated in Figure 2. Each of the SIF Delivery Capabilities is narrow in scope and includes few Activities. For the purposes of mapping SIF concepts, Delivery Capabilities and Activities can be considered synonymous.

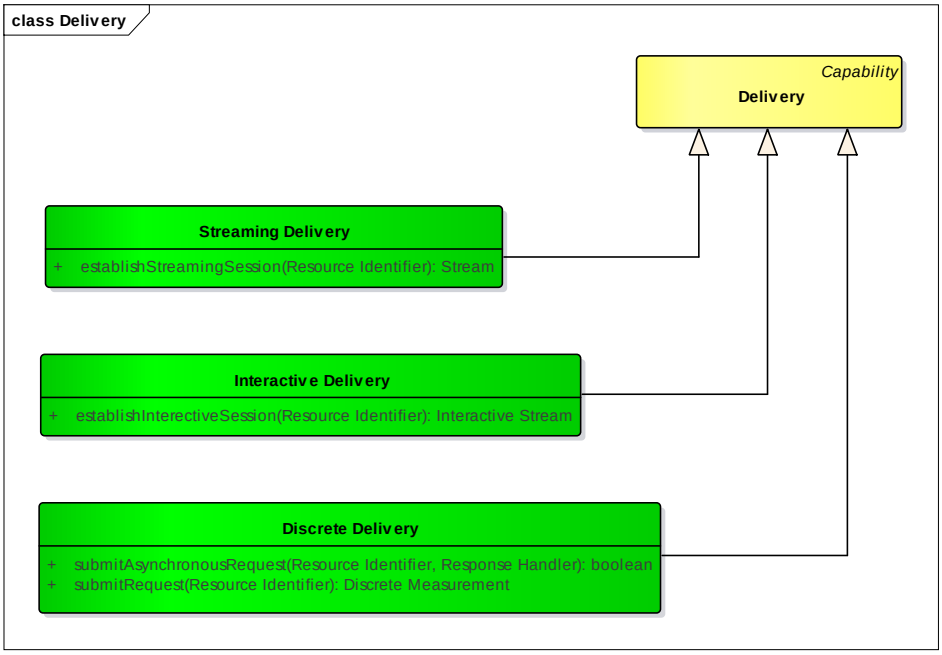


Figure 2 : SIF Delivery Capabilities

Observations are delivered through ISA Event messages. Consumers subscribe to Event messages through a subscription request, as documented in Section 5.1. These requests include a query expression to use in selecting Event messages to deliver to the subscriber.

8.4 Command

The SIF-SP Reference View decomposes the SIF Command Capability into nine Activities. Those Activities are described in Table 17.

SIF Activity	Description
Activate	The act of issuing a command to start a sensor Measure, Identify, Detect, or Classify activity.
Deactivate	The act of issuing a command to stop a sensor Measure, Identify, Detect, or Classify activity.
Get Observable	A command to retrieve an Observable from the sensor system.
Get Property	A command to retrieve a Property from the sensor system.
Get State	A command to retrieve the current State of the sensor system.
Process	Many sensor systems include considerable processing capabilities. The act of issuing a process command takes advantage of those capabilities by instructing the sensor system to execute on-board processing of the detection data prior to delivery.
Set Property	A command to set or modify a Property of the sensor system.
Task	The act of issuing a request to start a sensor Collect activity. This activity differs from triggering a collection in that the command is not sent to the sensor. Rather it goes to a sensor management system which may accept or reject the tasking request.
Trigger	The act of issuing a command to execute a single Collection or Actuator activity.

Table 17: SIF Command Activities

ISA supports a set of commands that is much larger than the nine Activities defined in the SIF-SP Reference View. However, most of those commands are instances of one of the SIF Command Activities. A mapping of SIF Command Activities to ISA commands is provided in Table 18.

SIF Command Activity	ISA Command	ISA Command Description
Set Property	Add IP Address	Adds an interface and IP Address to the component. Duplicate interfaces are not allowed, see the description of the IP Addresses property for information on adding multiple addresses to the same interface.
None	Add Subscription	Accepts a data filter script and uses it to control the data being sent to the subscribing component. See Section 5.1
Set Property	Add Zone	Adds a zone to a component. The zones will be added to the list of zones currently understood by the component, replacing any previously existing areas with the same name
Task	Adjust <property>	Adjusts the <property> of the component by the amount, rate, and period of time specified in the command.
Activate	Arm	Causes the component to move from the unarmed state to the armed state.
None	Authorize Registration	Determines whether or not the given client is allowed to register to the given server. See Section **Error! Reference source not found.**
None	Authorize Request	Determines whether or not the given request is allowed to be invoked on the given subject. See Section **Error! Reference source not found.**
Process	Calibrate	Performs any necessary initialization routine(s). Many times, this process is required before the device can be made operational.
Deactivate	Cancel	Instruct the receiver to cancel a command that is either being executed or is present in the request queue. A response of success indicates the command was successfully cancelled. A response of failed indicates the component was unable to cancel the request.
Set Property	Change <property>	Change the current <property> of the component.
Set Property	Clear Property	Clears a property that was previously set with Set Property (transitions it to Not Ready)
Get Observable	Create Zip Archive	Creates a zip archive of the results and makes that archive retrievable
Task	Designate	Tells a designator to perform the action of designating a target.
Deactivate	Disarm	Causes the component to move from the armed state to the unarmed state.
Get State, Get Property	Discover	Accepts a data query that determines which messages and ucis are returned.
Get State	Get Config	Retrieves the current configuration of the receiving component
Get State	Get Last Operation State	Retrieves the last operation state that matches the provided state.
Get State	Get Operation State History	Get the past operation states for the component.
Get Property	Get Property	Retrieves the value of the named property

SIF Command Activity	ISA Command	ISA Command Description
Get State	Get Status	Retrieves the current status of the receiving component.
Get Observable, Get State, Get Property	History	Accepts a data query and returns a resource where the user can access the data that satisfies that query.
Task	Illuminate	Instructs a component capable of Illumination to turn on the illuminator for the specified amount of time
Process	Initiate NUC	Initiate the Non-Uniform Correction process
None	Lock	Attempts to lock the specified components and commands so that only lock holders can use them. A form of access control. See Section **Error! Reference source not found.**
none	Menu Navigation	Navigation command for on-screen menu systems
Task	Move	Instructs the component to move from the current position to the destination position.
Task	Observe	Instructions the component to observe a position with any available sensors. The observation may begin at any time between receiving the command and the stale time. The observation may end at any point after the end time
none	Ping	Establishes whether communication with a component still exists. Components, upon receiving this no-op command, simply respond with an acknowledgement of receiving the command.
Set Property	Point Orientation	Tells a gimbaled component to point at a location expressed as a relative orientation
Set Property	Point Position	Tells a gimbaled component to point at a location expressed as a position.
Get Observable	Recommend Video Stream	When provided with the URL of a video stream, return a recommended resource that allows access to the same content (possibly transcoded) that is bandwidth appropriate.
Set Property	Remove IP Address	Removes an interface and IP Address from the list of IP Addresses.
None	Remove Subscription	Removes a currently active subscription. See Section 5.1
Set Property	Remove Zone	Invoked by a requester, removes a named zone from the component.
Process, Deactivate	Render Useless	Defines or initiates the actions (process) required to render the device useless. A device rendered useless becomes permanently nonfunctioning
Deactivate, Activate	Reset	Tells the component to return to its original state. The particulars of this command are specifically dependent on what can be modified by the component. For components that can have their pointing angle changed, this will tell the component to move to its home position. For components that have an alarm state (such as UGS), this will reset the state to unset
Process	Sanitize	Executes process to remove all unique application data from the device that could be used for a security attack.
Task	Scan Area	Scan the area contained within the points until the stop time.
Task	Scan Points	Scan the provided points until the stop time

SIF Command Activity	ISA Command	ISA Command Description
Process	Self Test	Requests that the device perform its internal diagnostics procedure.
Activate, Deactivate	Set Observable Reporting	Sets the reporting state of an individual observable. If true the observable will be published as part of an event message, if false the observable will not be reported. If a particular observable is not part of an event it will not be reported regardless of the reporting state.
Set Property	Set Property	Sets the value of a named property if the component is not able to determine the values itself.
Activate, Deactivate	Set Property Reporting	Sets the reporting state of an individual property. If true the property will be published as part of a status message, if false the property will not be reported.
Process, Deactivate	Shutdown	Invoked by another component, causes the component to perform its shutdown sequence. Upon receiving this command, the component should immediately enter the deregistration phase to remove itself from any clusters to which it currently belongs, perform whatever necessary actions are required to shut down and, if possible, physically power off the device.
Task	Slew Percent	Tells a gimbaled component to begin rotating in the direction specified at the speed specified (as a percentage of max speed) until directed to stop or the time duration has elapsed. The component can be stopped by issuing a command with all 0 percent.
Task	Slew Velocity	Tells a gimbaled component to begin rotating in the direction specified at the speed specified (as an absolute speed) until directed to stop or the time duration has elapsed. The component can be stopped by issuing a command with all 0 velocities.
Activate	Start Data Input	Start a data transfer input to the component. Success indicates the transfer has started. Updates should be retrieved from the Data Inputs property.
Deactivate	Stop Data Input	Stop a data transfer input to the component. Success indicates the transfer has started. Updates should be retrieved from the Data Inputs property.
Activate	Start Data Output	Start a data transfer output from the component. Success indicates the transfer has started. Updates should be retrieved from the Data Outputs property.
Deactivate	Stop Data Output	Stop a data transfer output from the component. Success indicates the transfer has started. Updates should be retrieved from the Data Outputs property.
Trigger	Take Picture	Causes the camera to generate an image of its current field of view
Trigger	Take Range	Invokes whatever mechanism is responsible for determining the distance to target. The command may only be available when an Armed property is set to true.
None	Unlock	Attempts to unlock the specified component and commands. Relaxes access controls. See section 5.7
Process	Zeroize	Perform a process to remove all accumulated unique application data from the device

Table 18: Mapping between SIF Command Activities and ISA Commands

8.5 Sensing

The SIF-SP Reference View decomposes the Sensing Capability into five Activities, which are described in Table 19.

SIF Activity	Description
Classify	Similar to Identify except that the goal is to identify the type of the observed entity, not the identity.
Collect	The act of collecting multiple measurements which will be processed into the reported observation. Examples include remote imagery, LIDAR, and SIGINT.
Detect	The act of determining that a pre-defined criteria has been met and issuing an alert that this is the case. This criteria is typically a threshold such as a maximum or minimum temperature. Detections can be sent directly to a sensor management system or distributed through a publish-subscribe capability. A common Detect case is detection of a physical entity/event, such as a Radar detecting a plane, a gunshot detector detecting a gunshot, and a seismic sensor detecting a vehicle driving by.
Identify	The act of collecting an observation and comparing that observation against a set of patterns or templates with known identities. If a match is observed, then the identity of the observed individual or item is reported. Biometrics are one form of Identifying activity.
Measure	The act of measuring a physical quantity such as temperature.

Table 19 : SIF Sensing Activities

The ISA Data Model Specification defines ISA commands that would directly trigger a SIF Sensing Activity. A mapping between these ISA commands and SIF Sensing Activities is provided in Table 20.

SIF Activity	ISA Command	ISA Command Description
Collect	Observe	Instructions the component to observe a position with any available sensors. The observation may begin at any time between receiving the command and the stale time. The observation may end at any point after the end time.
Collect	Scan Area	Scan the area contained within the points until the stop time.
Collect	Scan Points	Scan the provided points until the stop time
Collect	Take Picture	Causes the camera to generate an image of its current field of view
Measure	Take Range	Invokes whatever mechanism is responsible for determining the distance to target. The command may only be available when an Armed property is set to true.

Table 20 : Mapping Between SIF Sensing Activities and ISA Commands

8.6 Human-Computer Interface

Human-computer interface is not addressed by the ISA architecture.

8.7 Information Assurance

Information assurance in an ISA environment is based on X.509 certificates and PKI services. At a connection level, PKI certificates issued by trusted certificate authorities are used (after verification and revocation checking) to establish a secure connection over which ISA messages are passed, entailing communication endpoint authentication and connection encryption. At an application level, ISA checks the claimed identity of a component that is requesting to join an ISA network against the identity included in the component's PKI certificate, thereby performing component authentication. ISA applies access control rules to determine if a component is authorized to join an ISA network and authorized to request that a particular ISA command be executed by a targeted component.

The ISA Data Model Specification defines ISA commands that support the SIF Information Assurance Capability. A mapping between the ISA commands and SIF Information Assurance Capabilities is provided in Table 21.

SIF Capability	ISA Command	ISA Command Description
Access Control	Authorize Registration	Determines whether or not the given client is allowed to register to the given server.
Access Control	Authorize Request	Determines whether or not the given request is allowed to be invoked on the given subject
Access Control	Lock	Attempts to lock the specified components and commands so that only lock holders can use them. A form of access control.
Access Control	Unlock	Attempts to unlock the specified component and commands. Relaxes access controls.

Table 21 : Mapping Between SIF Information Assurance Capabilities and ISA Commands

9 Enterprise Mapping

In order to expose sensor data and information available in the tactical DDIL environment to the enterprise domain, ISA networks must be integrated with the Defense Intelligence Information Enterprise (DI2E). The SIF presence on the DI2E is defined in the Enterprise Technical View (TV1). By implementing the Tactical DDIL IP Technical View specified herein on one "side" and the Enterprise Technical View on the other "side", an ISA Bridge can enable the exchange of data between the two domains. This section identifies the specifications for integrating ISA environments with the SIF DI2E capabilities.

The Tactical DDIL IP Technical View capabilities to provide the required bridge are defined in enterprise mappings and incorporated in the SWE Bridge conformance class. Compliance with the SWE Bridge conformance class is conditionally required when interconnecting beyond the specified communications environment to exchange information in the enterprise communication environment.

9.1 Mapping Common Data Types

Applicable Specifications:

- ISA Data Model Specification
- SIF-SP Ontology
- SIF-SP Ontology ISA to SWE Data Element Mapping

All ISA data entities are described in the ISA Data Model Specification. The ISA Data Model has been mapped into SWE Common by the ISA to SWE Data Element Mapping Specification. However, SWE Common only defines syntax. It is also necessary to map the ISA semantics. The SIF-SP Ontology addresses that issue by defining common data concepts for use by all SIF-SP Technical Views, including the concepts defined in the ISA Data Model. Therefore, ISA data can be converted into SWE data by transforming the syntax using the ISA-to-SWE mapping, then referencing the appropriate concept in the SIF-SP Ontology from the SWE Common definition element.

9.2 Mapping Descriptions

Applicable Specifications:

- SIF-SP Ontology ISA to SWE Data Element Mapping
- SIF-SP Ontology SensorML to DDMS 2 Data Element Mapping

Due to the limitations of the DDIL networks in which ISA was designed to operate, ISA components initially reporting their full status and thereafter only report changes to their status. This is incompatible with the SIF view of a single, up-to-date representation. The SWE Bridge is the ISA capabilities for bridging this gap. A SWE Bridge is responsible for gathering up ISA description metadata reporting it up to the Enterprise. This capability is supported by two data element mappings:

- The ISA to SWE Data Element Mapping specification includes a mapping of elements from ISA Config and Status messages into a a SensorML 2.0 document..
- The SensorML to DDMS mapping describes how to generate a DDMS 2.0 document from a SensorML 2.0 document.

9.3 Mapping Observables, Observations, and Measurements

Applicable Specifications:

- ISA Data Model Specification
- SIF-SP Ontology
- SIF-SP Ontology ISA to SWE Data Mapping Specification

Most ISA observables implement Reporting Data Types that are defined in Section 8.0 of the ISA Data Model Specification. Reporting Data Types are subdivided into Reporting Enumerations, Reporting Unions, and Reporting Composite Data Types:

- Enumeration – a list of valid values.
- Union – a choice of data types of which only one can be used at a time.
- Composite – a data type composed of multiple elements. Each element has a type and cardinality. The types are drawn from the Base Data Types (Section 4).

All ISA observables, Reporting Data Types, and Base Data Types are described in the SIF-SP Ontology. The SIF-SP Ontology also preserves the whole-part relationships which make up Union and Composite types. The ISA to SWE Data Mapping Specification describes the encoding of these entities using SWE Common. The ISA to OGC Observations and Measurements Mapping Specification describes how SWE Observations should be constructed using ISA data.

9.4 Mapping Spatial-Temporal Concepts

Applicable Specifications:

- SIF-SP Ontology ISA to SWE Data Element Mapping

A mapping between the tactical DDIL IP and Enterprise representation of Spatial-Temporal concepts is provided in the ISA to SWE Data Element Mapping Specification. This mapping is summarized in **Error! Reference source not found.**.

SIF-SP Ontology	ISA Data Elements	SWE Common	Comments
GeographicArc	GeographicArc	Gml:Arc	An Arc is an arc string with only one arc unit, i.e. three control points including the start and end point.
GeographicEllipse	GeographicEllipse	gml:AbstractCurveSegment	Implemented per the example in section E.2.4.7 of OGC 07-036.
GeographicPolygon	GeographicPolygon	Gml:Polygon	A Polygon is a special surface that is defined by a single surface patch (see D.3.6). The boundary of this patch is coplanar and the polygon uses planar interpolation in its interior. The elements exterior and interior describe the surface boundary of the polygon.
GeographicPolyline	GeographicPolyline	Gml:LineString	A LineString is a special curve that consists of a single segment with linear interpolation. It is defined by two or more coordinate tuples, with linear interpolation between them.
GeographicPosition	GeographicPosition	Gml:Point	Defined by a single coordinate tuple.
TemporalInstance	UTC	gml:TimeInstant	A zero-dimensional geometric primitive that represents an identifiable position in time.
TemporalPeriod	none	gml:TimePeriod	A one-dimensional geometric primitive that represents an identifiable extent in time. The location in of a gml:TimePeriod is described by the temporal positions of the instants at which it begins and ends.

Table 22: Mapping Between ISA and SWE for Space and Time

9.5 Mapping the Computational View

Applicable Specification:

- OGC Sensor Observation Service 2.0
- ISA Interface Control Document
- DDF documentation at http://www.codice.org/ddf/

An ISA Bridge serves as a mediator between the ISA interface used for the Tactical DDIL IP Technical View and the OGC SWE and DDF interfaces used for the Enterprise Technical View. Its primary function is to accumulate data reported through ISA messages until there is sufficient information to generate either a SensorML or O&M Observation document. Once sufficient information has been gathered, the Bridge will generate the document and post it to the corresponding Enterprise level Sensor Observation Service. In addition, it will generate a DDMS document from that same information and post it to the DDF component associated with the SOS.

At this time no support is required for information flowing from the Enterprise to the Tactical environment. This capability will be addressed in a future version of the SIF-SP.

Annex A Abstract Test Suite

Table 23 provides a Requirement Trace Matrix which maps SIF-SP TV-3 requirements to the abstract tests which validate compliance with each requirement. The tests are identified by their Annex A paragraph number.

Requirements
Requirement 1: A Component that claims to be conformant to the SIF-SP TV-3 Basic Conformance Class shall demonstrate conformance to the requirements specified in the ISA Component Requirements specification cited in the Normative Specifications Section of this document.
Tests: A.1.1
Requirement 2: A Component that claims to be conformant to the SIF-SP TV-3 Basic Conformance Class and implements the ISA Controller capabilities shall demonstrate conformant to the requirements specified in the ISA Controller Requirements specification cited in the Normative Specifications Section of this document.
Tests: A.1.2
Requirement 3: A Component that claims to be conformant to the SIF-SP TV-3 Basic Conformance Class shall demonstrate conformance to the requirements specified in the ISA Data Model specification cited in the Normative Specifications Section of this document.
Tests: A.1.3
Requirement 4: A Component that claims to be conformant to the SIF-SP TV-3 Basic Conformance Class shall demonstrate conformance to the requirements specified in the ISA Interface Control Document cited in the Normative Specifications Section of this document.
Tests: A.1.4
Requirement 5: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate the ability to receive ISA Config and Status messages from other ISA Components and to generate valid and complete SensorML documents from those messages.
Tests: A.2.1
Requirement 6: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate the ability to receive ISA Config and Status messages from other ISA Components and to generate valid and complete DDMS 2.0 documents from those messages.
Tests: A.2.2
Requirement 7: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate the ability to receive ISA Event messages from other ISA Components and to generate valid and complete OGC O&M Observation documents from those messages.
Tests: A.2.3
Requirement 8: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate the ability to receive ISA Event messages from other ISA Components and to generate valid and complete DDMS 2.0 documents from those messages.
Test: A.2.4
Requirement 9: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate conformance to the client-side requirements of the OGC Sensor Observation Service (SOS) Transaction Extension requirements class.

Requirements
Test: A.2.5
Requirement 10: A Component that claims to be conformant with the SIF-SP TV-3 SWE Bridge Conformance Class shall demonstrate conformance to the client-side requirements of one or more of the DDF publication interfaces.
Test: A.2.6
Requirement 11: A Component that delivers Interactive Steaming measures shall use one or more of the Interactive Stream protocols identified in Table 9.
Test: A.2.7
Requirement 12: A Component that delivers Coverage measures shall use one or more of the coverage formats identified in Table 10
Test: A.2.8
Requirement 13: A Component that delivers Measurement Streams shall use one or more of the Measurement Stream protocols identified in Table 9
Test: A.2.9

Table 23 : Requirement Test Matrix

A.1. SIF-SP TV-3 Basic Conformance Class Module

A.1.1 ISA Component

a) Test Purpose: Verify that the service implements the requirements from the ISA Component Requirements specification.

b) Test Method: See Appendix A of the ISA Component Requirements specification

c) References: ISA Component Requirements Release 6.0

d) Test Type: Capability

A.1.2 ISA Controller

a) Test Purpose: Verify that the service implements the requirements from the ISA Controller Requirements specification.

b) Test Method: See Appendix A of the ISA Component Requirements specification

c) References: ISA Controller Requirements Release 6.0

d) Test Type: Capability

A.1.3 ISA Data Model

a) Test Purpose: Verify that the service implements the requirements from the ISA Data Model specification

b) Test Method: Random testing of the data produced by the component complies with the ISA Data Model

c) References: ISA Data Model Specification Version 6.0

d) Test Type: Capability

A.1.4 ISA Interface Control Document

a) Test Purpose: Verify that the service implements the requirements from the ISA Interface Control Document.

b) Test Method: Testing can take place at three phases of the development process:

   a. Code inspection during development

   b. Wire protocol inspection during Unit Testing

   c. Integration testing during Factory Acceptance Test and Site Acceptance Test

c) References: ISA Interface Control Document Version 6.0

d) Test Type: Capability

A.2. SIF-SP TV-3 SWE Bridge Conformance Class Module

A.2.1 SWE Bridge SensorML Generation

a) Test Purpose: Verify that a component that implements the SWE Bridge can generate valid and complete SensorML documents from received Config and Status messages.

b) Test Method: Post config and status messages with known content to the ISA enterprise:

   a. Verify that a SensorML document was produced

   b. Validate the SensorML document against the SensorML 2.0 XML Schema and schematron rules

   c. Validate that all information that could be populated in the SensorML document has been populated using the ISA to SWE Data Element Mapping specification as a guide.

c) References:

   a. OGC SensorML Model and XML Encoding Standard version 2.0

   b. Data Element Mapping Between the Integrated Sensor Architecture (ISA) and OGC Sensor Web (SWE) version 1.0

d) Test Type: Capability

A.2.2 SWE Bridge DDMS Generation for Sensors

a) Test Purpose: Verify that a component that implements the SWE Bridge can generate valid and complete DDMS 2.0 documents from received Config and Status messages.

b) Test Method: Post config and status messages with known content to the ISA enterprise:

   a. Verify that a DDMS 2.0 document was produced

   b. Validate the DDMS 2.0 document against the DDMS 2.0 XML Schema and schematron rules

c. Validate that all information that could be populated in the DDMS document has been populated.

c) References: Department of Defense Discovery Metadata Specification 2.0

d) Test Type: Capability

A.2.3 SWE Bridge O&M Observation Generation

a) Test Purpose: Verify that a component that implements the SWE Bridge can generate valid and complete O&M Observations from received Event messages.

b) Test Method: Post Event messages with known content to the ISA enterprise:

a. Verify that a Observation document was produced

b. Validate the Observation document against the O&M Observation 2.0 XML Schema and schematron rules

c. Validate that all information that could be populated in the Observation has been populated using the ISA to SWE Data Element Mapping specification as a guide:

c) References:

a. OGC Observations and Measurements XML Implementation standard version 2.0

b. Data Element Mapping Between the Integrated Sensor Architecture (ISA) and OGC Sensor Web (SWE) version 1.

d) Test Type: Capability

A.2.4 SWE Bridge DDMS Generation for Observations

a) Test Purpose: Verify that a component that implements the SWE Bridge can generate valid and complete DDMS 2.0 documents from received Event messages.

b) Test Method: Post Event messages with known content to the ISA enterprise:

a. Verify that a DDMS 2.0 document was produced

b. Validate the DDMS 2.0 document against the DDMS 2.0 XML Schema and schematron rules

c. Validate that all information that could be populated in the DDMS document has been populated.

c) References: Department of Defense Discovery Metadata Specification 2.0

d) Test Type: Capability

A.2.5 Sensor Observation Service - Transactional

a) Test Purpose: Verify that a component that implements the SWE Bridge can successfully interoperate with a service that is compliant with the Sensor Observation Service Transaction standard.

b) Test Method: The Sensor Observation Service standard does not include client-side requirements. Therefore, this requirement shall be validated by successful completion of all of the SOS

Transactional Extension Tests defined in Section 14.3 of the SoS standard. These tests shall be executed against an OGC recognized reference implementation of the SoS service.

c) References: OGC Sensor Observation Service Interface Standard version 2.0

d) Test Type: Capability

A.2.6 DDF Publication

a) Test Purpose: Verify that a component that implements the SWE Bridge can successfully publish DDMS 2.0 documents to the DDF.

b) Test Method: Publish the DDMS documents generated through tests A.2.2 and A.2.4 to an instance of the DDF. Query the DDF using a standard client and verify that the DDMS documents can be discovered.

c) References: DDF documentation at http://www.codice.org/ddf/

d) Test Type: Capability

A.2.7 Interactive Streaming

a) Test Purpose: Verify that Interactive Streaming measures comply with the protocol standards identified in Table 9.

b) Test Method: For each Component which delivers Interactive Streaming measures, validate sample measures against the compliance criteria for the specified protocols.

c) References: See citation for JPIP in the Normative Specifications section.

d) Test Type: Capability

A.2.8 Coverages

a) Test Purpose: Verify that coverage measures comply with the standards identified in Table 10.

b) Test Method: For each Component which delivers coverage measures, validate sample measures against the compliance criteria for the specified format standards.

c) References: See citations for JPEG 2000, Exif, PNG, NITF, GeoTIFF and LAS in the Normative Specifications section.

d) Test Type: Capability

A.2.9 Measurement Streams

a) Test Purpose: Verify that Measurement Streams comply with the standards identified in Table 9

b) Test Method: For each Component which delivers Measurement Streams, validate sample measures against the compliance criteria for the specified protocol standards.

c) References: See citations for MISP in the Normative Specifications section.

d) Test Type: Capability

Annex B Terms and Definitions

Abstract Test Case

A generalized test for a particular requirement. [ISO 19105]

Abstract Test Method

A method for testing an implementation that is independent of any particular test procedure. [ISO 19105]

Abstract Test Module

A set of related abstract test cases. Abstract test modules may be nested in a hierarchical way. [ISO 19105]

Abstract Test Suite (ATS)

A set of abstract test modules and associated abstract test cases that collectively specify all the requirements to be satisfied for conformance. [digest from ISO 19105]

Basic Test

An initial capability test intended to identify clear cases of non-conformance. [ISO 19105]

Capability Test

A test designed to determine whether an IUT conforms to a particular characteristic of a standard as described in the test purpose. [ISO 19105]

Compliance

Adherence to policy, directives, instructions, guidance, etc. Often used to define or mean the same as conformance. E.g. an implementation exhibits conformance when it complies with the conformance requirements of the applicable information standards.

Component Capability Description (CCD)

The set of declarations of the ISA capabilities supported by an ISA component.

Conformance

The fulfilment of specified requirements. [ISO 19105]

Conformance Class

Conformance classes may be used to group, define, and label different kinds of conformance requirements pertinent to implementation of the standard. [digest from ISO 19105]

Conformance Level

A conformance level is a special kind of conformance class in which the conformance requirements of a higher level contain all the requirements of the lower levels. [digest from ISO 19105]

Executable Test Suite (ETS)

A set of executable test cases. [ISO 19105]

An executable test suite (ETS) is an instantiation of an ATS, in which all implementation- dependent parameters are assigned specific values. An executable test case is derived from an abstract test case and is in a form that allows it to be run on the IUT. Executable test cases result from the instantiation of specific values for parameters in abstract test cases. Executable test cases may be unique to each IUT. [digest from ISO 19105]

Implementation Conformance Statement (ICS)

A statement made by the supplier of an implementation or system claimed to conform to a given standard (or set of standards/specifications), asserting which capabilities have been conformingly implemented. [digest from ISO 19105]

Implementation Under Test (IUT)

The realization of a specification that is the focus of test. [digest from ISO 19105]

ISA capability

A property, observable, or command declared by an ISA component.

ISA Command

A task that an ISA component can perform upon request.

ISA component

A component that complies with the ISA interface and supports the required ISA behaviors.

ISA message

An application message exchanged over the ISA interface.

ISA network

A set of interconnected ISA components.

ISA Observable

Information that a component can publish about observations that it makes.

ISA Property

Information that a component can report about its current status.

Performer

ISA component that is performing a task upon request.

Reference Implementation (RI)

A conformant, trusted, or well-known exemplar implementation of one or more standards used to support standards conformance and interoperability testing. In some instances, the RI is suitable for reuse by developers in their own instantiations of the standardized function or service.

Requester

ISA component that is requesting the performance of a task.

Standards Conformance Testing

Testing performed to determine the extent to which a system or subsystem adheres to or implements a standard. It involves testing the capabilities of an implementation against both the conformance requirements in the relevant standard(s) and the statement of the implementation's capabilities. [NSGM 3202]

Subscriber

ISA component that has created a subscription that specifies subsequently available ISA messages that are of interest.

System Under Test (SUT)

The computer hardware, software and communication network required to support an IUT. [ISO 19105]

Annex C **Abbreviations**

In this document the following abbreviations and acronyms are used or introduced:

ATS	Abstract Test Suite
CCD	Component Capability Description
DDIL	Denied Disconnected Intermittent and Limited
DDMS	DoD Discovery Metadata Specification
DI2E	Defense Intelligence Information Enterprise
DMS	Data Model Specification
DoD	Department of Defense
ETS	Executable Test Suite
GWG	Geospatial-Intelligence Standards Working Group
IC	Intelligence Community
ICS	Implementation Conformance Statement
IP	Internet Protocol
ISA	Integrated Sensor Architecture
ISO	International Organization for Standardization
IUT	Implementation Under Test
JESC	Joint Enterprise Standards Committee
JPIP	JPEG 2000 Interactive Protocol
LIDAR	Light Detection and Ranging
MISB	Motion Imagery Standards Board
MISP	Motion Imagery Standards Profile
NGA	National Geospatial-Intelligence Agency
NSG	National System for Geospatial Intelligence
OGC	Open Geospatial Consortium
PKI	Public Key Infrastructure
RI	Reference Implementation
SensorML	Sensor Model Language
SIF	Sensor Integration Framework
SIF-SP	Sensor Integration Framework Standards Profile
SIGINT	Signals Intelligence

SUT	System Under Test
SWE	Sensor Web Enablement
UCI	Unique Component Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
USMS	US MASINT System

Annex D **Implementation Conformance Statement (ICS)**

An ICS is a statement made by the supplier of an implementation or system claimed to conform to a given standard (or set of standards/specifications), asserting which capabilities have been conformingly implemented. An ICS provides a uniform means for the implementer to declare the mandatory, conditional, and optional provisions of the standard that were actually implemented.

The following ICS may be used by the supplier or sponsor of an implementation as a framework to document the standards conforming capabilities of the implementation of this standard

SIF-SP TV-3 - Implementation Conformance Statement (ICS)

B=Baseline KML P=Profile Obligation I=Implemented P/F=Pass/Fail

M=Mandatory O=Optional C=Conditional

Implementation Under Test: **Conformance Level (1, 2 or 3):**
Test Point: **Profile Identifier:**
Date of Initial ICS Completion: **Test Sponsor:**
Date of Test Completion: **Test Organization:**

Basic Conformance Level – component meets the requirements to participate in an ISA federation	Component complies with the ISA Component Requriements specifcation	M			
	Component complies with the ISA data model	M			
	Component complies with the ISA Interface Control Document	M			
SWE Bridge Extension – component can serve as an intermediary between the Tactical DDIL and Enterprise environments.	Component can generate valid SensorML documents from ISA Config and Status messages	M			
	Component can generate valid DDMS 2.0 documents from ISA Config and Status messages	M			
	Component can generate valid O&M Observation documents from ISA event messages	M			
	Component can generate valid DDMS 2.0 documents describing the O&M Observation documents generated from ISA event messages	M			
	Component can properly and successfully publish DDMS 2.0 documents to an Enterprise DDF instance using one of the standard DDF publication interfaces.	M			
	Component delivers interactive streaming content in conformance to one of the specified standards.	C			
	Component delivers coverage content in conformance to one of the specified standards.	C			
	Component delivers measurement streaming content in conformance to one of the specified standards.	C			