

NATO UNCLASSIFIED

STANDARDIZATION
RECOMMENDATION

RECOMMANDATION
DE NORMALISATION

STANREC 4869

COUNTERING CLASS I UAS DATA
EXCHANGE FORMAT

CONTRE LES UAS DE CLASSE I
FORMAT D'ÉCHANGE DE
DONNÉES

EDITION/ÉDITION A VERSION 1

XX XXXX/XXXX 20XX (to be filled by NSO only)



NORTH ATLANTIC
TREATY ORGANIZATION

ORGANISATION DU TRAITÉ
DE L'ATLANTIQUE NORD

Published by
the NATO STANDARDIZATION OFFICE
(NSO)

Publiée par
le BUREAU OTAN DE NORMALISATION
(NSO)

© NATO/OTAN

NATO UNCLASSIFIED

NATO UNCLASSIFIED

XX XXXX/XXXX 20XX (to be filled by NSO only)

NSO REFERENCE/RÉFÉRENCE NSO

LETTER OF PROMULGATION

LETTRE DE PROMULGATION

STATEMENT

The enclosed NATO standardization recommendation (STANREC), which has been approved by member nations, is promulgated herewith.

ENACTMENT

This STANREC is effective upon receipt for use by the participating nations and NATO bodies.

ACTIONS BY NATIONS

Nations are invited to use the Allied standard(s) covered by the STANREC and to provide feedback to the NSO on the use of the covered Allied standard(s).

SECURITY CLASSIFICATION

This STANREC is a NATO UNCLASSIFIED document to be handled in accordance with C-M(2002)60.

RESTRICTION TO REPRODUCTION

This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (<https://nso.nato.int/nso/>) or through your national standardization authorities.

ADDITIONAL INFORMATION

None.

Thierry POULETTE
Major General, FRA (A)
Director, NATO Standardization Office

DÉCLARATION

La recommandation de normalisation OTAN (STANREC) ci-jointe, qui a été approuvée par les pays membres, est promulguée par la présente.

ENTRÉE EN VIGUEUR

Cette STANREC entre en vigueur dès réception aux fins d'application par les pays et les organismes OTAN participants.

MESURES À PRENDRE PAR LES PAYS

Les pays sont invités à appliquer la ou les normes interalliées couvertes par cette STANREC et à fournir des informations en retour au NSO quant à leur utilisation desdites normes.

CLASSIFICATION DE SÉCURITÉ

Cette STANREC est un document OTAN SANS CLASSIFICATION qui doit être traité conformément au C-M(2002)60.

RESTRICTION DE REPRODUCTION

Ce document de normalisation OTAN est produit par l'OTAN. Il peut être reproduit moyennant mention de la paternité de l'OTAN. L'OTAN n'exige aucune participation financière, à aucun stade, pour ses documents de normalisation, lesquels ne sont pas destinés à la vente. Ceux-ci sont disponibles dans la base de données des documents de normalisation OTAN (<https://nso.nato.int/nso/>) ou auprès de l'organisme national de normalisation.

INFORMATIONS SUPPLÉMENTAIRES

Aucune.

Thierry POULETTE
Général de division, FRA (A)
Directeur du Bureau OTAN
de normalisation

STANREC 4869 Edition/Édition A, Version 1

**COUNTERING CLASS I UAS
DATA EXCHANGE FORMAT**

**CONTRE LES UAS DE CLASSE I
FORMAT D'ÉCHANGE DE
DONNÉES**

AIM

The aim of this NATO standardization recommendation (STANREC) is to list recommended practices regarding:

Data messaging format in the C-UAS domain.

RECOMMENDATION

The following Allied and/or non-NATO standard is recommended:

STANDARD OR STANDARDS

British Standards Institute BSI Flex 335 v2.0:2024-03 (SAPIENT)

OTHER RELATED DOCUMENTS

None.

SUPERSEDED DOCUMENTS

This STANREC does not supersede any document.

USE

Member or partner nations and NATO bodies should provide feedback to the NSO on the use of Allied standards covered by a STANREC.

REVIEW

This STANREC is to be reviewed in accordance with AAP-03. The result of the review is to be recorded within the NATO Standardization Document Database (NSDD).

TASKING AUTHORITY

This STANREC is supervised under the authority of:

FEEDBACK

Any comments concerning this STANREC

BUT

La présente recommandation de normalisation OTAN (STANREC) a pour but de répertorier les pratiques recommandées concernant :

Format de messagerie de données dans le domaine C-UAS.

RECOMMANDATION

La norme interalliée ou non OTAN suivante est recommandée:

NORME OU NORMES

British Standards Institute BSI Flex 335 v2.0:2024-03 (SAPIENT)

AUTRES DOCUMENTS CONNEXES

Aucun.

DOCUMENTS ANNULÉS ET REMPLACÉS

La présente STANREC n'annule et ne remplace aucun document.

EMPLOI

Les pays membres ou partenaires et les organismes OTAN devraient fournir au NSO des informations en retour sur l'emploi des normes interalliées couvertes par les STANREC.

RÉEXAMEN

La présente STANREC doit être réexaminée conformément à l'AAP-03. Le résultat de ce réexamen doit être consigné dans la Base de données des documents de normalisation OTAN (NSDD).

AUTORITÉ DE TUTELLE

La présente STANREC est sous la responsabilité de :

C-UAS WG

INFORMATIONS EN RETOUR

Tous les commentaires concernant la

NATO UNCLASSIFIED

shall be addressed to:

présente STANREC doivent être adressés au :

NATO Standardization Office (NSO)

Bureau OTAN de normalisation (NSO)

**Boulevard Léopold III
1110 BRUXELLES - Belgique**

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

[illegible]

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[illegible]

INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1 FOREWORD	1
1.1. Conventions	1
1.2. Normative Versus Informative Language – RFC 2119 Compliance	1
1.3. Structured data serialization.....	1
1.4. Data Model.....	1
1.5. How to read this document?.....	1
1.6. References.....	2
CHAPTER 2 Introduction	3
2.1. AEDP AIM	3
2.2. AEDP Scope	4
2.3. Relation to BSI Flex 335	4
2.4. Synchronization with the base standard.....	5
2.5. Relation to other standards	5
CHAPTER 3 Terms, definitions and abbreviations	7
3.1. Terms and definitions	7
3.2. Abbreviations	8
CHAPTER 4 C-UAS Architecture	10
4.1. Information Exchange Requirements	10
4.2. Generic C-UAS Use Cases	11
4.3. Operational View.....	14
4.4. Technical Architecture View.....	15
4.5. Hierarchy of Fusion nodes	16
4.6. Systems Architecture View	16
4.7. Extensibility	18
4.8. Data Harmonization	18
CHAPTER 5 Interface description	19
5.1. Introduction	19
5.2. Message Structure	19
5.2.1. Message Wrapper.....	19
5.2.2. Inner Messages.....	20
5.3. Data Model.....	20
5.3.1. Data Units	20
5.3.2. UML Representation	21
5.3.3. Sapient Message	22
5.3.4. Registration Message	23
5.3.4.1. Node Definition.....	24
5.3.4.2. Capability	25
5.3.4.3. Status Definition	26
5.3.4.4. Mode Definition	27
5.3.4.5. Detection Definition	28
5.3.5. StatusReport Message.....	29
5.3.6. DetectionReport Message.....	29

5.3.7.	Task message	30
5.3.8.	Alert message	31
5.3.9.	Error message.....	32
CHAPTER 6	Implementation	34
6.1.	Transport Layer Mechanism.....	34
6.2.	Middleware extension	34
6.4.	Testing Support.....	35
6.5.	C-UAS System Generic Requirements	35
6.6.	Security Considerations for Message Exchange	37
6.6.1.	Security Classification of Messages	37
6.6.2.	External Security Aspects	37
6.6.3.	Security Accreditation and Penetration Testing.....	38
6.6.4.	Limitations of Cross-Domain Security Solutions Using Data Diodes...	38
6.6.5.	Implementation Guidance	39
6.7.	Legal by Design	39
CHAPTER 7	Life Cycle and Maintenance concept	41
7.1.	BSI Flex 335, Lifecycle / Maintenance concept.....	41
7.2.	AEDP 4869 Lifecycle / Maintenance concept	41
7.2.1.	Relation of BSI Flex 335 and AEDP	41
7.2.2.	Backward Compatibility	42
7.2.3.	Compliance testing.....	42
ANNEX A	Example Messages	A-1
A.1	Introduction	A-1
A.2	Registration Message	A-1
A.3	Status Report Example	A-6
A.4	Detection Report	A-7
A.5	StatusReport	A-9
ANNEX B	Compliance with Existing Standards.....	B-10
B.1	Introduction	B-10
B.2	Message Fields	B-10
B.3	Business Rules	B-11

LIST OF TABLES

Table 1: Terms and definitions used in this document	8
Table 2 : Message header encoding.....	Error! Bookmark not defined.

LIST OF FIGURES

Figure 1 Recommended reading order for the document set.	2
Figure 2: SAPIENT Concept and Architectural principles	4
Figure 3 Generic C-UAS use cases and actors.	12
Figure 4. OV1 for Coalition asset protection (blue cylinder represents C2/fusion node).....	14
Figure 5. OV1 for hierarchical fusion (blue cylinders represent C2/fusion nodes).	15
Figure 6 Generic SAPIENT architecture (one of two valid configurations) – derived from [BSI Flex 335 v2].....	15
Figure 7 Hierarchy of C2 nodes - from [BSI_Flex_335_v2].....	16
Figure 8 The use of SAPIENT data format in conjunction with Link16 and Asterix.....	17
Figure 9 An example of an integrated C-UAS capability with mixed standards.	18
Figure 10 High level representation of the Sapient Message and specialized content.	21
Figure 11 UML representation of the SapientMessage.	22
Figure 12 UML representation of the Registration message.	23
Figure 13 NodeDefinition and the NodeType values recommended in AEDP 4869.	25
Figure 14 Capability information under the registration message	26
Figure 15 Status Definition information under the registration message.	27
Figure 16 Mode Definition information elements under the Registration message.....	27
Figure 17 DetectionDefinition class inside of a Registration message.	28
Figure 18 StatusReport Message.	29
Figure 19 DetectionReport Message.	30
Figure 20 Task Message used by the C2 fusion node to control the sensor and effector edge nodes.	31
Figure 21 Alert message structure.....	32
Figure 22 Error message.....	33

INTENTIONALLY BLANK

CHAPTER 1 FOREWORD

1.1. Conventions

The AEDP-4869 is the technical standard document associated with the STANREC 4869. This AEDP document was developed as a wrapper around the UK SAPIENT standard BSI Flex 335. The use of “STANREC 4869” or just “4869” refers literally to the recommendation to the nations to use this data messaging format in the C-UAS domain.

1.2. Normative Versus Informative Language – RFC 2119 Compliance

1. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF, RFC 2119, 1997].
2. The key word "INFORMATIVE" is used to denote strictly informative content of the document.
3. BSI documents do not use the terms 'MUST' or 'MUST NOT' since these are considered external constraints (for example, legal constraints) that are not requirements for the document in question. For consistency with BSI Flex 335, on which this document is based, the terms 'SHALL' and 'SHALL NOT' are preferred.

1.3. Structured data serialization

The mechanism of implementing STANREC 4869 is through Google's Protocol Buffer (protobuf version 3) serialization protocol. In this context, the key information elements used in this document are messages, fields and types. These messages, fields and types are defined in BSI Flex 335 and will not be repeated in this document [BSI_Flex_335_v2].

1.4. Data Model

A UML model has been developed from the protobuf files and is used in the document to provide a graphical representation of messages and to support the understanding of complex types and relationships. The UML diagram is large and for presentation reasons it has been split into smaller diagrams. Maintaining an accurate view of the bigger picture is useful, therefore a complete printable copy of the main UML data model is provided in ANNEX A.

1.5. How to read this document?

The recommended reading order for the document set is depicted in Figure 1. An implementation guide is in development, the Implementation Guide may be consulted by component developers.

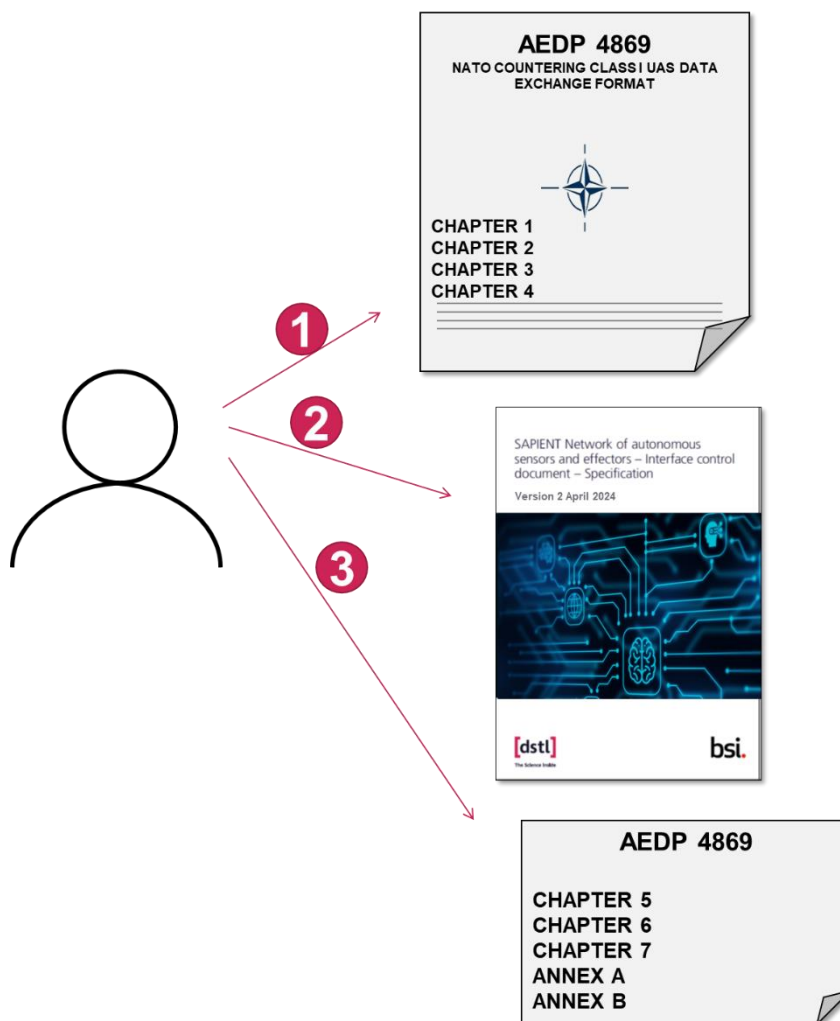


Figure 1 Recommended reading order for the document set.

1.6. References

[BSI Flex 335 v2]

British Standardization Institute, BSI Flex 335, version 2, available at <https://knowledge.bsigroup.com/products/bsi-flex-335-v2-0-2023-sapient-network-of-autonomous-sensors-and-effectors-interface-control-document-specification-specification?version=standard>

CHAPTER 2 <i>Introduction</i>

2.1. AEDP AIM

Many Defence and Security use cases require a networked sensing and effect capability, employing the advantages of multi-location, potentially multi-modality, layered approach. When this incorporates processing at-the-edge (i.e. within the sensor node), closely integrated with information fusion (correlation, association and tracking of targets) and dynamic sensor/effector management (dynamic tasking of the sensor/effector nodes in response to the unfolding scenario), strong performance benefits are shown (see Figure 2), but this creates a requirement for a suitable standard to define the communication mechanism.

SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) is a standard funded by the United Kingdom (UK) Ministry of Defence (MOD), and sponsored and written by the Defence, Science and Technology Laboratory (DSTL), which gives manufacturers and sensor network operators specifications for interfacing sensor edge nodes, effector edge nodes and fusion nodes. This describes a networked sensor and effector suite, based on autonomous sensors publishing low-bandwidth messages on an open architecture, to a fusion and sensor management system. The messages contain the output of the processing rather than the raw data collected by the sensor (i.e. information, not data) and therefore have sensor-agnostic content (i.e. the same information is reported whatever the sensor type). The SAPIENT concept has compelling benefits such as significantly lower cognitive burden for the user(s), operational flexibility, dual defence/security use and lower acquisition cost.

SAPIENT's concept specifically enables multi-sensor fusion and sensor management. Critically, SAPIENT explicitly builds-in support for autonomous fusion and autonomous tasking (of both sensors and effectors) which enables tight decision-action loops, essential in tactical environments. The SAPIENT concept shows its full benefits in highly dynamic scenarios where (for example) highly maneuverable targets are detected in real time by multiple sensors, the information from those sensors is autonomously fused to generate situational awareness, which in-turn generates real-time responses: either sensor taskings (i.e. tipping, cueing or target hand-off), effector responses, or both. All of the above occurs with minimal user involvement – i.e. 'human on-the-loop' (providing oversight and authorization) rather than in-the-loop (direct involvement in the decision-making).

Built on the SAPIENT concept is an open standard, embodying an Interface Control Document, which uses protobuf. This is BSI (British Standards Institution) Flex 335, and is a generic standard across all relevant use cases and domains.

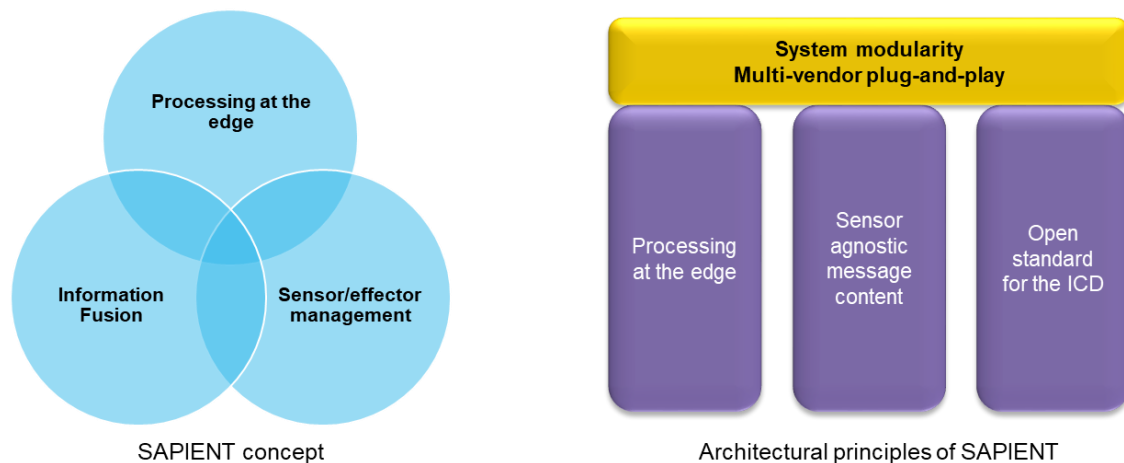


Figure 2: SAPIENT Concept and Architectural principles

Thus, the three architectural principles of SAPIENT, processing-at-the-edge, sensor agnostic message content and an open standard for the ICD, combine to create an architecture that strongly supports system modularity. I.e. a system can be built at deployment time from SAPIENT compatible nodes, which requires zero or minimal integration to work. This modularity provides a high degree of flexibility, both in acquisition (SAPIENT compatible components can be purchased from multiple suppliers to form an integrated system) and operationally (the suite of components can be changed during operational use – often live (“hot plug and play”)). The modular nature also supports easy swapping of sensors to adapt to different mission requirements or operational environments.

The architecture promotes vendor neutrality, which is key to avoiding vendor lock-in. By supporting a wide range of sensor types and fusion technologies, SAPIENT allows for a diverse ecosystem where users are not confined to products from a single vendor. This flexibility enhances innovation as users can choose the best-in-class sensors and technologies that meet their specific needs without compatibility concerns.

2.2. AEDP Scope

This document provides technical information required for the use of the BSI Flex 335 standard within NATO C-UAS domain.

The detailed data message specifications are fully provided in BSI Flex 335 and are only repeated in this document for the purpose of readability. The AEDP document refers to a specific version of BSI Flex 335 and a lifecycle management concept is included in CHAPTER 7.

2.3. Relation to BSI Flex 335

BSI Flex 335 forms the basis of this AEDP and is referenced extensively here. However, BSI Flex 335 is a generic standard covering multiple use cases and used by multiple communities. The purpose of this AEDP is to provide additional guidance on how to use the BSI standard in the NATO Counter Class-1 UAS domain.

It is recognized that other communities are also using or considering the use of SAPIENT. SAPIENT therefore offers opportunities to build systems that seamlessly cross traditional use-case boundaries. In future editions requirements from these communities could be included in AEDP 4869.

2.4. Synchronization with the base standard

Protobuf is a set of language-neutral, platform-neutral extensible mechanisms for serializing structured data. One of the properties of protobuf is its innate backwards- and forwards-compatibility. As long as developers follow some simple practices when updating .proto definitions, new code will read old messages and old code will read new messages without issues (ignoring any newly added fields). Therefore, BSI Flex 335 is, by its use of protobuf, naturally backwards- and forwards-compatible.

This AEDP references a specific version of BSI Flex 335, namely version 2.0 [BSI_Flex_335_v2]. The update frequency of BSI Flex 335 is greater than that of AEDP 4869, so in time, this document will reference an 'old' version of Flex 335; however, the forwards-compatible nature of protobuf mitigates any issues that might have arisen. Therefore, equipment that may be compatible with future versions of Flex 335 will still be compliant in an AEDP 4869 compatible system (just with the loss of whatever new features are introduced after the reference version of BSI Flex 335).

2.5. Relation to other standards

The SAPIENT format is adopted in the NATO C-UAS domain as a common data format to support the rapid transmission of detections, tracks and identification information from edge nodes (e.g. sensors) to fusion nodes (e.g. command and control) and commands from the fusion node to edge nodes (e.g. effectors). SAPIENT supports the automated processing of data, which will enhance the commander's decision process, through machine speed information and decision making between any sensor, any shooter, any C2 (autonomous sense-decide-effect). The format can also be used between fusion nodes to build an enhanced UAS recognized picture, which can be disseminated to specific customers using other data formats.

Some similarities can be noted between the SAPIENT format and other NATO standards. The Tactical Data Link (TDL) family of standards and the standards covered under the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA) are the closest to the purpose, scope and structure of SAPIENT format.

TDL standards such as Link 16 and the Joint Range Extension Application Protocol (JREAP) are focused on exchanging various tactical information like target tracks, sensor reports, and orders across NATO forces, between mobile platforms and ground stations and between ground control stations. SAPIENT on the other hand is used as a lightweight format to exchange sensor data and facilitate data fusion at the edge. The TDL transports mainly processed data and information whereas SAPIENT works with sensor data for the purpose of automatic data processing. The recognized

air picture (RAP) in military applications is often disseminated using Link 16 and the associated JREAP format. This TDL format is complex and could be used to build the C-UAS air picture. However, the cost (e.g. financial, personnel, time) for implementing this standard is a factor that limits its adoption in the C-UAS domain, where the cost efficiency is a relevant factor. Moreover, the recommended reporting frequency in Link 16 is about 12 seconds (can go down to 3 seconds in special cases), which is a limiting factor for C-UAS applications where more frequent reports are required due to highly dynamic air picture (common C-UAS update times are in order of 1 second). the C-UAS reaction time is required in highly dynamic threat environment when drones can move tens and hundreds of meters in 10s

Asterix is another popular protocol used to disseminate air surveillance information mainly in the civilian domain. Some Asterix extensions have been proposed to support the C-UAS domain. The challenge with these extensions is that they provide limited support to multisensor data fusion and tasking of the sensors and effectors. SAPIENT has the ability to work with a diverse category of sensors such as radar, electronic warfare, acoustics and EO/IR, and it complements existing standards in the multisensor data fusion task.

Typical C-UAS sensors include radar, radiofrequency (RF) direction finders (DF), acoustic, and electro-optical and infrared cameras (EO/IR). NIIA defines standards for transmitting these types of information between the ground control stations. For example STANAG 4607 is used to transmit the Ground Moving Target Indication (GMTI) data collected by ground surveillance radars, STANAG 4545 is used to transmit still EO/IR imagery, STANAG 4609 is used to transmit full motion imagery, STANAG 4676 is used as the ISR tracking standard and STANAG 4658 and STANAG 4633 are used in the Electronic Warfare (EW) domain. All these NIIA standards are highly specialized on particular sensing technologies. In the C-UAS domain, the cost of the systems has to be maintained low and one cannot afford to use multiple standards due to implementation costs and maintenance efforts. SAPIENT sits at the information level and not at the raw data level and therefore is not a replacement for NIIA standards.

CHAPTER 3	<i>Terms, definitions and abbreviations</i>
------------------	--

3.1. Terms and definitions

Term	Definition
unmanned aircraft (UA)	An aircraft that does not carry a human operator and is operated remotely using varying levels of automated functions. Note: NATO does not use or recognize the terms: unmanned aerial vehicle, unmanned aerial system, or drone. (NATOTerm)
unmanned aircraft system (UAS)	A system whose components include the unmanned aircraft, the supporting network and all equipment and personnel necessary to control the unmanned aircraft. (NATOTerm)
remotely piloted aircraft (RPA)	An unmanned aircraft that is controlled from a remote pilot station by a pilot who has been trained and certified to the same standards as a pilot of a manned aircraft. (NATOTerm)
remotely piloted aircraft system (RPAS)	A remotely piloted aircraft, its associated remote pilot station(s), the required command and control links and any other components as specified in the type design. (NATOTerm/ICAO)
lost link	The loss of command and control links between the control station and unmanned aircraft such that the aircraft cannot be controlled remotely. (NATOTerm)
remote split operation (RSO)	Unmanned aircraft system operation that involves the geographical separation of the launch and recovery site from the out-of-theatre mission control element. (NATOTerm)
counter-unmanned aircraft system operation (C-UAS)	A counter-air operation conducted to prevent mission accomplishment of an enemy unmanned aircraft system, which could include attacking the aircraft itself, its data links, or the control station. (NATOTerm)
automated unmanned aircraft	An unmanned aircraft that, in response to inputs, logically follows a predetermined set of rules to provide a predictable outcome. (NATOTerm)
autonomous unmanned aircraft	An unmanned aircraft capable of understanding higher-level intent and direction, sensing its environment, and, based on a set of rules and limitations, choosing from alternatives and taking actions to bring about an optimal but potentially unpredictable state without human input. (NATOTerm)
automated take-off and landing	Automated take-off is the ability of the [unmanned aircraft] to be launched with a single command once planning and pre-flight have been conducted and permission to launch has been granted. (NATOTerm)
automatic	Pertaining to a process or equipment that, under specified conditions, functions without human intervention. (NATOTerm)
autonomy	A system's ability to function, within parameters established by

	programming and without outside intervention, in accordance with desired goals, based on acquired knowledge and an evolving situational awareness. (NATOTerm)
autonomous operation	A mode of operation in which a sub-system functions independently of the operation of the remainder of the system to which it belongs. (NATOTerm)

Table 1: Terms and definitions used in this document

3.2. Abbreviations

AC	Aircraft
AD	Air Defence
ADA	Air Defence Artillery
AGL	Above Ground Level
AJP	Allied Joint Publication
AOI	Area of Operational Interest
AP	Air Policing
ATC	Air Traffic Control
C-IED	Counter-Improvised Explosive Device
C-UAS	Counter Unmanned Aircraft System
CBRN	Chemical Biological Radiological and Nuclear
CIS	Communications and Information Systems
COA	Course of Action
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
DI	Defence Investment
EA	Electronic Attack
ECCM	Electronic Counter Counter Measures
ECM	Electronic Counter Measures
EO	Electro-Optic
ES	Electronic Surveillance
ESCD	Emerging Security Challenges Division (within NHQ)
ESM	Electronic Security Measures
EW	Electronic Warfare
FP	Flightplan
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HN	Host Nation
IAMD	Integrated Air Missile Defence
ID	Identification
IFF	Identification Friend or Foe
IPB	Intelligence Preparation of the Battlefield
IPE	Intelligence Preparation of the Environment
IPOE	Intelligence Preparation of the Operating Environment
IR	Infrared
IS	International Staff

ISO	International Organization for Standardization
JIPOE	Joint Intelligence Preparation of the Operating Environment
LIDAR	Light Detection and Ranging
LOS	Line of Sight
LSS	Low, Slow, Small
NAI	Named Area of Interest
NATO	North Atlantic Treaty Organisation
NIAG	NATO Industrial Advisory Group
PET	Passive Emitter Tracking
PNT	Position, Navigation, Timing
RAM	Rocket, Artillery, and Mortar
RF	Radio Frequency
RTO	Research and Technology Organisation
SA	Situational Awareness
SATCOM	Satellite Communications
SOF	Special Operation Forces
STANAG	Standard NATO Agreement
sUAS	small Unmanned Aerial System
TAI	Target Area of Interest
TAIS	Tactical Airspace Integration System
TDOA	Time Difference Of Arrival
TEWA	Threat Evaluation and Weapons Assignment
TV	Television
UAS	Unmanned Aerial System
USA	United States of America
USAF	United States Air Force
VIP	Very Important Person
WG	Working Group

CHAPTER 4 C-UAS Architecture
--

4.1. Information Exchange Requirements

This document outlines key information exchange requirements necessary to support interoperability, maintain data integrity, and enhance security. By defining clear messages and business rules, we aim to facilitate efficient data communication across diverse platforms and systems, enabling the end user to harness the full potential of their capabilities while adhering to regulatory compliances. This standard serves as the foundation for building reliable and scalable data exchange C-UAS architectures that are crucial for operational success in a data-driven environment.

The information exchange requirements can be grouped by the following categories:

1. *Detection and Tracking Information*

- Sensor Data Fusion: Information from radar, Radio Frequency Direction Finding (DF), Electro-Optical/Infrared (EO/IR), acoustic and other sensors needs to be fused to improve detection accuracy and tracking. This involves exchanging data on detected objects' speed, altitude, direction, accuracy and other attributes.
- Real-time Data Sharing: Ensure real-time or near-real-time sharing of sensor data among the C2 system, effectors and relevant stakeholders for quick decision-making.
- Sensor Specifications: Prior information about sensors is highly relevant in any data and information fusion architecture. For example, information regarding sensor coverage areas and potential overlaps for redundancy and improved accuracy. This can be supported through proper registration messages as well and through sensor management functions and messages.

2. *Identification and Classification*

- UAS Signature Database: Sharing information from a database of known UAS signatures (acoustic, RF, visual, etc.) with sensors for accurate identification.
- Machine Learning/Artificial Intelligence (AI) Algorithms: Exchange of model information, pattern recognition and behavioural analysis data to distinguish between friendly, hostile, or neutral UAS.

3. *Engagement and Neutralization*

- Effector Coordination: Information on the location, engagement capabilities (range, field of view, effective altitude), and status (ready, engaged, reloading) of kinetic and non-kinetic effectors (e.g., jammers) to select the most suitable response.
- Engagement Rules: Transmission of clear, pre-defined rules of engagement (ROE) that dictate when, how, and which drones can be engaged, including legal and safety considerations.

4. *Command and Control (C2) Systems*

- Situation Awareness: Comprehensive battlefield and airspace situation awareness, including the status of all sensors, effectors, and identified UAS threats.
- Decision Support: Results of algorithms and data analytics to support human decision-making, suggesting optimal engagement strategies based on current threats and assets status.
- Communication Networks: Information regarding secure, reliable, and resilient communication networks for the exchange of command and control messages, sensor data, and engagement orders. This includes redundancy to ensure network availability in the face of jamming or other electronic warfare tactics.

5. *Interoperability with Existing Standards and Capabilities*

- Data Standards: Harmonization of common concepts, data formats and protocols to ensure interoperability existing NATO STANAGs or other relevant standards.
- Interface Protocols: Well-defined interface protocols for integration between new and existing systems, ensuring that future upgrades or additions can be seamlessly integrated.

6. *Security and Encryption*

- Cybersecurity Measures: Protection of C-UAS systems from cyber threats, including data encryption and secure authentication mechanisms to prevent unauthorized access or data manipulation.
- Electronic Counter-Countermeasures (ECCM): Strategies to protect against electronic warfare tactics aimed at disrupting sensor data or C2 communications.

7. *Legal and Ethical Considerations*

- Compliance Information: Ensuring all engagements comply with local, national, and international laws, including information on ROE, engagement authorization processes, and accountability measures.
- Privacy Concerns: Addressing privacy issues related to surveillance and data collection, especially when operating in or near civilian areas.

4.2. Generic C-UAS Use Cases

A Counter-Unmanned Aircraft System (C-UAS) system is designed to detect, track, identify, and neutralize unmanned aircraft systems (UAS) that pose a threat to safety, security, or privacy. There are numerous implementations of these C-UAS systems and their architecture and concept of employment is equally diverse. In the development of this document common architecture elements have been considered in order to focus the standardization recommendations. The architecture integrates a variety of technologies and systems to create a comprehensive defense against

unauthorized UAS. A brief overview of use cases the key actors and involved in a typical C-UAS architecture is outlined in this section.

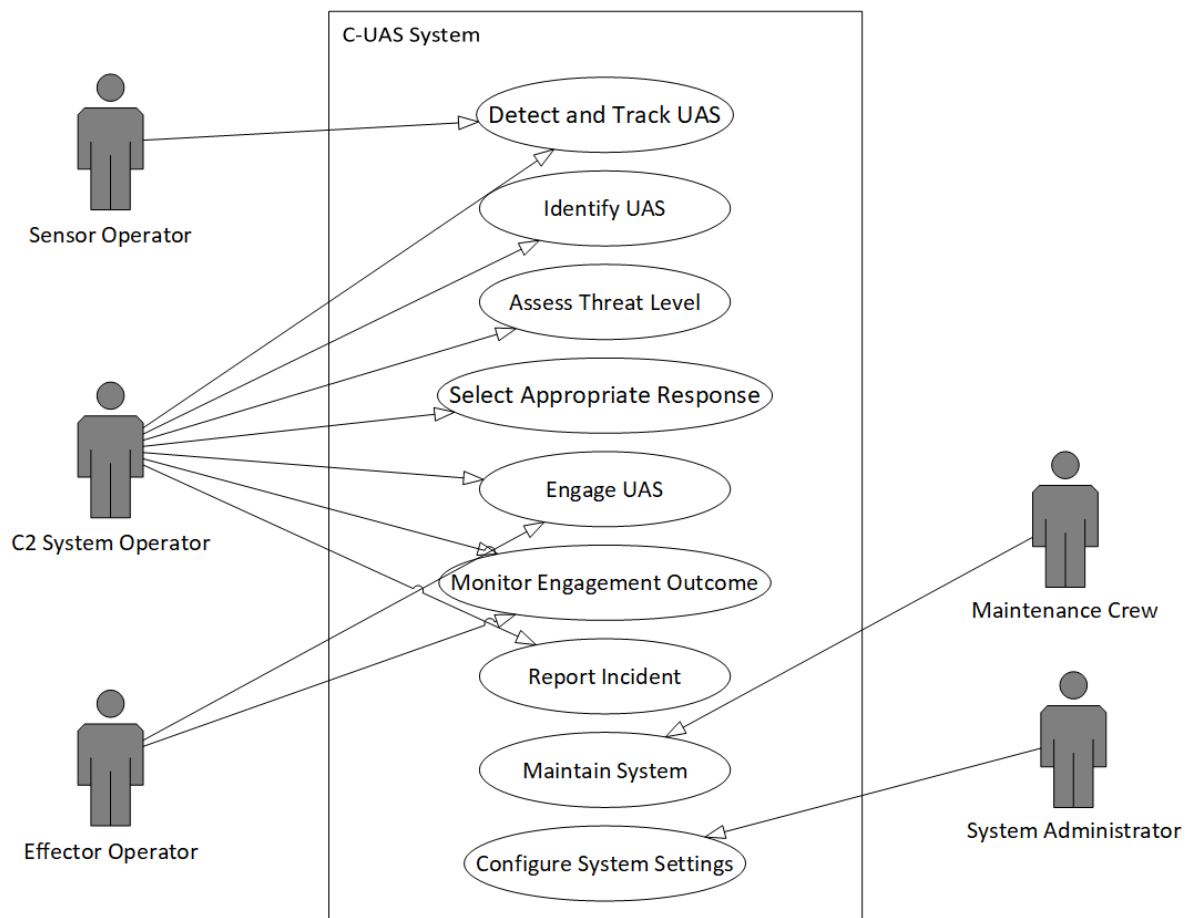


Figure 3 Generic C-UAS use cases and actors.

The main use cases illustrated in Figure 3 are:

1. Detect and Track UAS: Utilizing radar, RF direction finders, EO/IR, and acoustic sensors to detect unidentified aerial systems and track their movements.
2. Identify UAS: Analysing sensor data to identify the UAS type, whether it's a known commercial model, a potential threat, or an unidentified object. This use case covers mainly non-cooperative identification. Unmanned Traffic Management (UTM), which deals with cooperative identification, is covered by other standards, but UTM information can be added to AEDP 4869 messages.
3. Assess Threat Level: Based on the UAS's trajectory, payload, and behaviour, the system evaluates the potential threat it poses.

4. Select Appropriate Response: Deciding on the most suitable countermeasure based on the threat assessment, whether it involves electronic jamming, kinetic engagement, or other tactics.
5. Engage UAS: Activating the chosen effector to neutralize or mitigate the threat posed by the UAS.
6. Monitor Engagement Outcome: Assessing the effectiveness of the engagement and deciding on further actions if necessary.
7. Report Incident: Documenting the encounter and the response for future analysis, training, and legal purposes.
8. Configure System Settings: Adjusting parameters, updating software, and customizing the system to adapt to evolving threats and operational requirements. This includes changes in the system configurations, which can be transmitted through edge node registration messages.
9. Maintain System: Regular maintenance and repair of sensors, effectors, and C2 systems to ensure operational readiness.

A set of actors are used in Figure 3 to indicate the human interaction with the main use cases considered in this document:

1. Sensor Operators: Personnel responsible for operating and monitoring detection systems like radar, DF, EO/IR, and acoustic sensors.
2. C2 System Operators: Individuals who oversee the command and control system, making decisions based on the information gathered from sensors and effectors.
3. Effector Operators: Operators in charge of deploying countermeasures, whether kinetic (e.g., nets, projectiles) or non-kinetic (e.g., RF jammers).
4. System Administrator: Individuals responsible for the configuration, security, and overall management of the counter-drone system's network and software components.
5. Maintenance Crew: Technicians responsible for the upkeep and repair of sensors, effectors, and C2 systems.

The efficiency gained by using SAPIENT may allow for some of the roles listed above to be combined (e.g. sensor operator, effector operator could be merged into the C2 Systems operator role). The data exchange formats defined in BSI Flex 335 and in this document should support the communications between use cases and actors defined in Figure 3.

4.3. Operational View

The main operational concepts assumed in the development of this standards are graphically depicted in Figure 4 and Figure 5. The protection of a coalition asset, showing four Edge Nodes connecting to a C-UAS C2 (Fusion Node) is illustrated in Figure 4. Here, threats are detected by the sensor edge nodes, passed to the fusion node, which tasks other Edge Nodes to confirm or engage.

A hierarchical fusion case is depicted in Figure 5. This shows three local tactical C-UAS C2 systems (blue cylinders) feeding into a higher echelon coalition C2 node. At each of the local C2 nodes the so-called Single Local Air Picture (SLAP) will be produced, which filters out the false alarms and consolidate the UAS air picture. This consolidated UAS air picture is sent up the higher echelon where it gets integrated in the Recognized Air Picture (RAP). The frequency of the updates between SLAP and RAP can also differ in accordance with operational requirements.

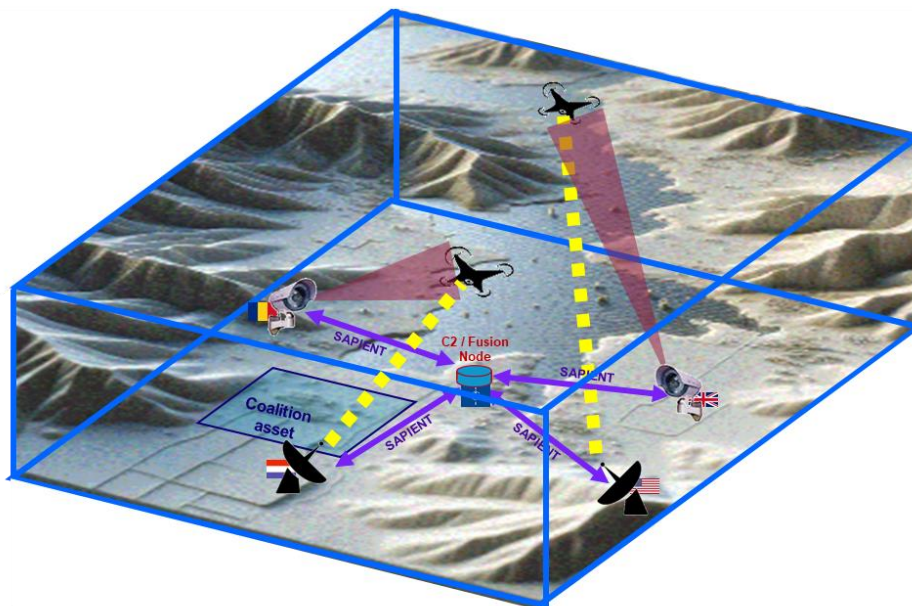


Figure 4. OV1 for Coalition asset protection (blue cylinder represents C2/fusion node).

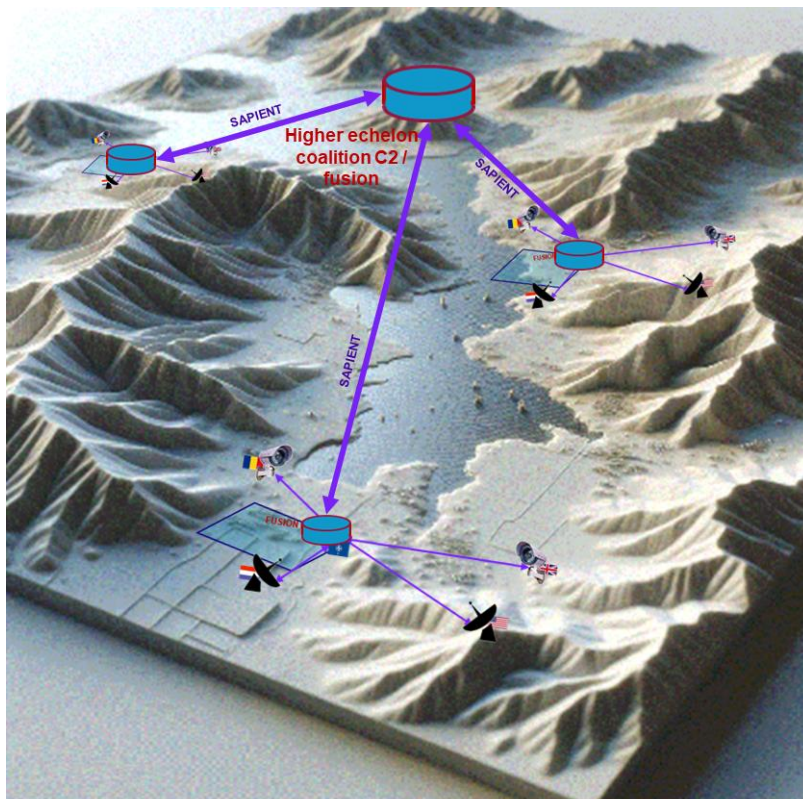


Figure 5. OV1 for hierarchical fusion (blue cylinders represent C2/fusion nodes).

4.4. Technical Architecture View

The generic SAPIENT architecture is shown in Figure 6 (reproduced with permission from [BSI Flex 335 V2]), consisting of multiple edge nodes connected to a fusion node.

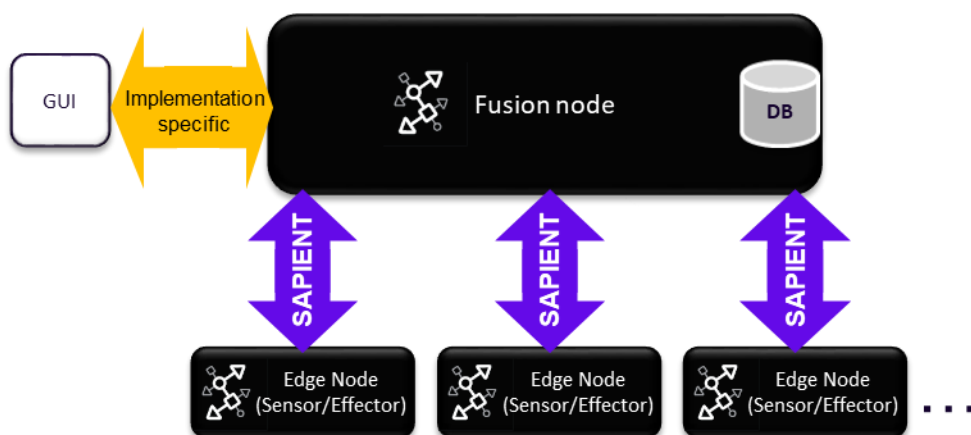


Figure 6 Generic SAPIENT architecture (one of two valid configurations) – derived from [BSI Flex 335 v2].

The term Fusion node describes a component that performs a spectrum of functions from geospatial aggregation through to correlation, confirmation, de-confliction and task optimization. Edge Nodes can be Sensor Edge Nodes or Effector Edge Nodes (or both). This AEDP uses the term C2 (Command and Control) node as a synonym for Fusion Node, and it uses the term Sensor and Effector as specific types of Edge Node.

4.5. Hierarchy of Fusion nodes

BSI Flex 335 V2 allows for a hierarchy of Fusion nodes, see Figure 7. This could be used (for example) to enable fusion nodes that cover local regions to be aggregated by higher-level fusion nodes that cover larger areas.

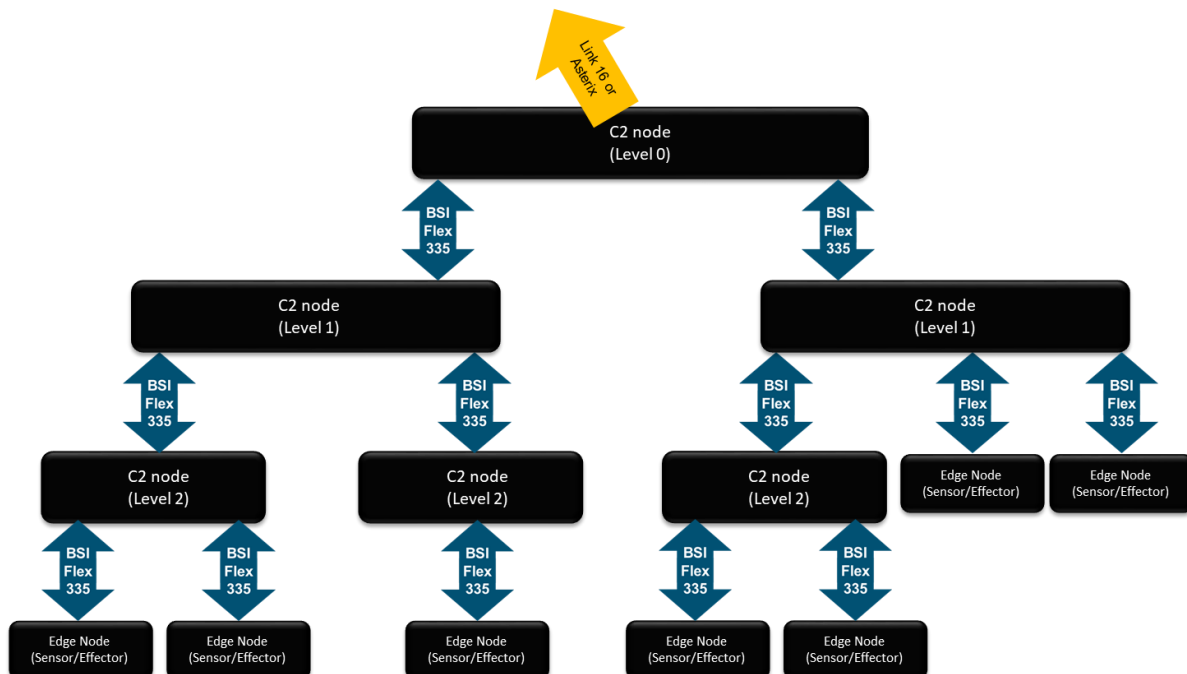


Figure 7 Hierarchy of C2 nodes - from [BSI_Flex_335_v2].

4.6. Systems Architecture View

The system architecture depicted in Figure 8 illustrates how SAPIENT can be used in connection with other NATO and civilian standards to address the internal and external information exchange requirements. By incorporating these standards, we ensure that the C-UAS systems will meet rigorous quality, security, and compatibility requirements. The main benefits of using SAPIENT are discussed in CHAPTER 2. Existing standards will facilitate our integration with broader community already

exposing these interfaces, while our internal standards focus on optimizing specific C-UAS workflows and processes.

Other standards may be used inside of C-UAS systems but these may make the components less interoperable with NATO capabilities. This is due to inevitable loss of information when translating between standards (e.g. different information concepts, different business rules etc.).

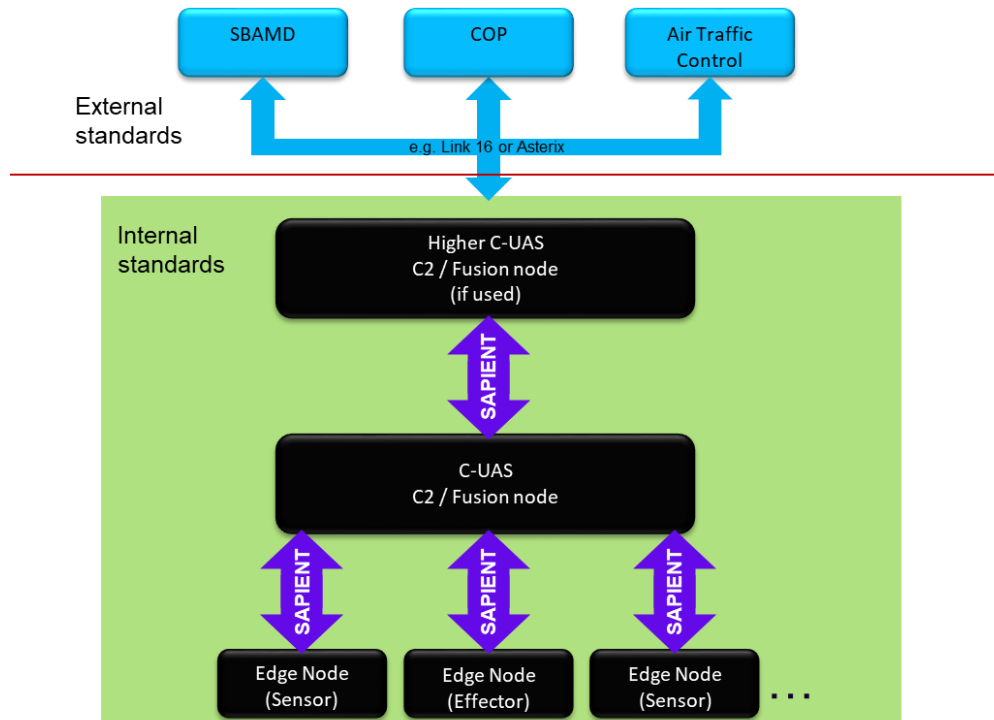


Figure 8 The use of SAPIENT data format in conjunction with Link16 and Asterix.

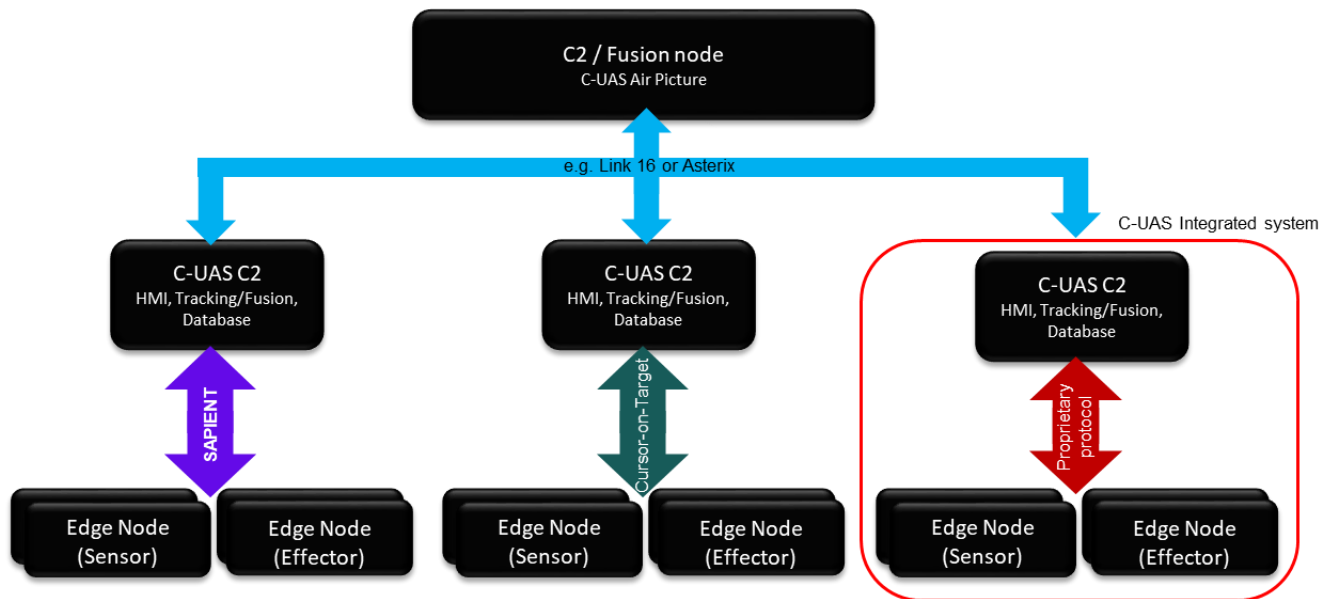


Figure 9 An example of an integrated C-UAS capability with mixed standards.

An example of a possible architecture where standards other than SAPIENT are used is depicted in Figure 9. This approach is feasible, but will restrict the technical interoperability levels.

4.7. Extensibility

In the C-UAS domain, many sensor edge nodes have native capability to detect and distinguish air targets and air vehicle behavior that go beyond the BSI Flex 335 V2 core taxonomy. Fortunately, BSI Flex 335 V2 includes an approach to dynamically extend the taxonomy. C-UAS edge nodes with additional detection capabilities can declare the taxonomy extensions they will use at registration time and then use them at detection time.

For example, this may allow classes from external taxonomies (e.g. ADAT-P3, AAP-6, MIP, NATO JC3IEDM, etc.) to be dynamically declared by Edge Nodes that wish to use those class structures.

4.8. Data Harmonization

This section addresses the need of data harmonization between L16, Asterix, and SAPIENT standards. A compatibility matrix is included in ANNEX B.

CHAPTER 5 <i>Interface description</i>
--

5.1. Introduction

This section describes the high-level SAPIENT message structure and provide guidance on how to use the BSI Flex 335 specifications to support C-UAS systems interoperability.

5.2. Message Structure

The overall structure of SAPIENT message consists of a common wrapper message and multiple inner messages. The inner messages are common across various use cases such as detection reports or tasking messages.

5.2.1. Message Wrapper

All SAPIENT messages are contained in a message wrapper, shown in Table 1 of the BSI Standard [BSI_Flex_335_v2]. This consists of three **Mandatory** fields, one **Conditional** field and one **Discretionary** field. Please see Clause 3 of the BSI document for a description of these terms.

The Mandatory fields are **timestamp**, **node_id**, and **Content**. **Content** is one of a list of all the possible message types, *Registration*, *RegistrationAck*, *StatusReport*, *DetectionReport*, *Task*, *TaskAck*, *Alert*, *AlertAck* and *Error*.

The **Conditional** field is the **destination_id** field. This is **Conditional** because the id of the destination node is not always known, for example, when a node sends the initial registration message it doesn't know the destination id. However, when a Task message is generated by a fusion node, it shall be sent to the specified node and this field would be mandated.

The **Discretionary** field is called **additional_information**. This string field SHALL be used in the context of this AEDP to contain the Confidentiality marking as defined in STANAG 4774.

An example Confidentiality marking from STANAG 4774 is:

“NATO UNCLASSIFIED Releasable to Japan, KFOR”,

which can be contained in a text field. An example of how the confidentiality marking can be implemented using discretionary field is provided in ANNEX A

Note: *this AEDP does not mandate any further action to be taken in the handling of a SAPIENT message due to the contents of this field.*

5.2.2. Inner Messages

Common Messages are defined messages which can be called, set and used by the unique sapient message. The BSI standard [BSI Flex 335 v2] in Clause 5 defined a set of five inner messages. These could also be described as Common message types, which means that these messages contain information that is common across other message types.

These messages are:

1. Location
2. Range Bearing
3. Velocity
4. Associated Detections
5. Associated File

Location contains the necessary data types to define where a node is located and allows for UTM or Lat/Long coordinate system and altitude, together with margins of error and datum information where appropriate. There is also a data structure that allows for lists of locations.

Range Bearing contains the necessary data structures to define a Range and Bearing or a Range and Bearing Cone reading from an edge node. For all Range bearing messages the extent or field of view is defined symmetrically around the center point.

Velocity contains the necessary data structure to define a Velocity reading obtained from an edge node. Only East, North, Up frame of reference is permitted.

Associated Detections contains the necessary data structure to define a list of IDs of detection reports with different object IDs

Associated File contains the necessary data structure to define a type and URL of a file which is required in the context of a higher-level message.

5.3. Data Model

5.3.1. Data Units

Many variables in SAPIENT can be provided in multiple units (e.g. deg/rad, km/m etc.) and these are specified in separate fields in the registration message or data message. Ultimately, in a complex multi-component system, unit conversions shall happen somewhere. The general principle in SAPIENT is to allow the edge nodes the most flexibility to report/consume data in their native format, while performing all the conversions in the C2/fusion node.

5.3.2. UML Representation

At the implementation level, the SAPIENT message is described by a series of Google protocol buffers files. In addition to the definition provided in the BSI Flex Version 2 and the protocol buffers files, the AEDP defines these protocol buffers as a UML diagram. UML diagrams are a general-purpose visual modelling language that is intended to provide a standard way to visualize the design of a system.

The structure of the UML diagram is divided for each message identified in the SapientMessage. SapientMessage is above Registration, RegistrationAck, StatusReport, DetectionReport, Task, TaskAck, Alert, AlertAck, and Error messages. Ack messages are acknowledgement responses, which can be positive or negative. In the protocol buffers definition, the top messages can be Message or Enum. Another field worthy of mention is the Oneof field, in which at most one of the fields can be set and serialized at a time.

The UML diagrams included in this document use the following colour codes for the 3 main topics: Blue for Message, Orange for Enum, and Pink for Oneof.

Some proto files are not displayed in the UML diagrams included in this document: AssociatedDetection, AssociatedFile, Follow, Location, ProtoOptions, RangeBearing, Velocity messages. These messages depend on the structure of the SapientMessage and specific information which needs to be sent.

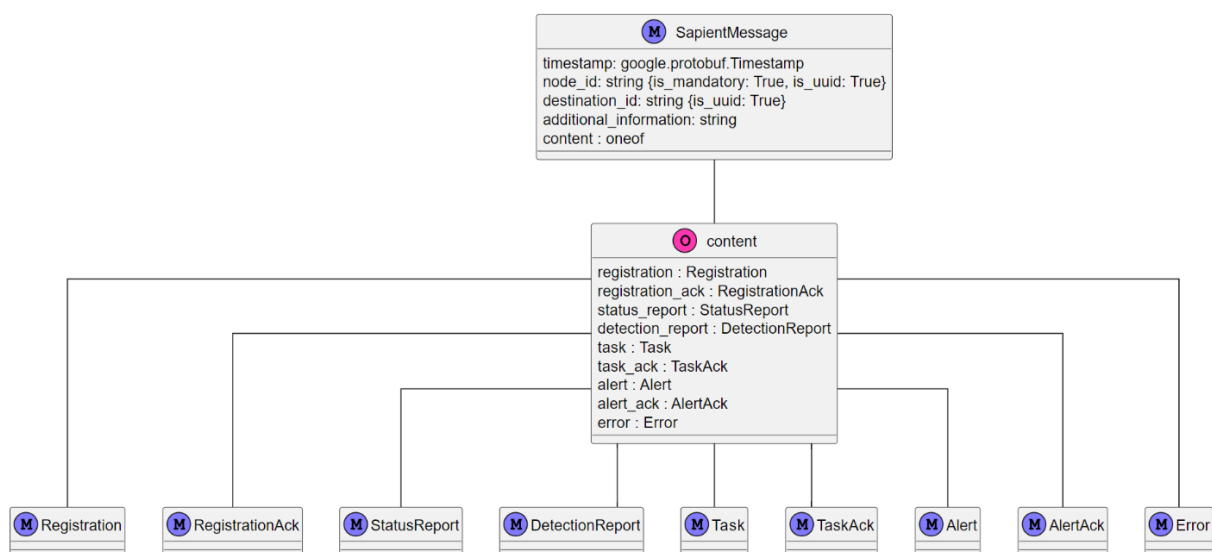


Figure 10 High level representation of the Sapient Message and specialized content.

Figure 10 depicts a Sapient message as a root element, which can be specialised using different content:

- The Registration message represents the core capability of the Edge Node (C-UAS Sensor or Effector). A Registration message is mandatory before other

messages such as StatusReport, DetectionReport or Task can be exchanged between sensors, effectors and C2 systems.

- The RegistrationAck message is sent by the C2 to the sensor / effector which sent the registration confirming unique connection. Transmission and receipt of the RegistrationAck is a mandatory condition to be able to receive and accept other messages from the node.
- The StatusReport provides status information from the C-UAS Sensor or Effector.
- The DetectionReport provides information about the detection from the Sensor to the C2. The DetectionReport provides information about the detected drone.

5.3.3. Sapient Message

The Sapient Message is the higher-level message which will be set and sent through the network. The information elements included in this message are presented in Figure 11

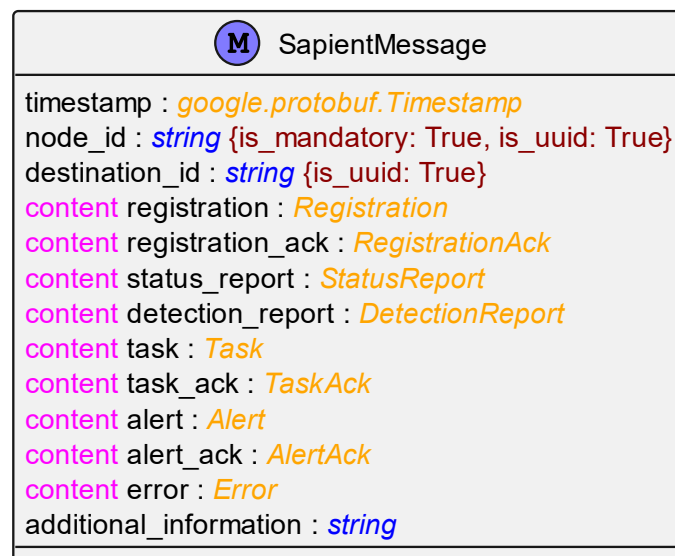


Figure 11 UML representation of the SapientMessage.

The timestamp, node_id, and destination_id are defined in the BSI standard [BSI Flex 335 v2]. The node_id and destination_id are the identification between the sender and receiver of the SapientMessage. It should be noted that the timestamp field should be populated with the time applicable to the message content (i.e. The timestamp of the detection message should reflect the time of the observation rather than the time of the generation of the message).

The oneof “content” field defines the lower-level message, of which only one needs to be set and sent. In the context of AEDP 4869, each message is described below with a C-UAS specific context.

Additional_information is used to define the NATO classification of the message in the context of AEDP 4869. The field additional_information SHALL contain the following information:

Field details	Field description
Additional Information	NATO Classification of the SAPIENT message

Table 2: Additional_information field

5.3.4. Registration Message

The Registration message is one of the most complex messages that can be encapsulated in a SapientMessage (see Figure 12).

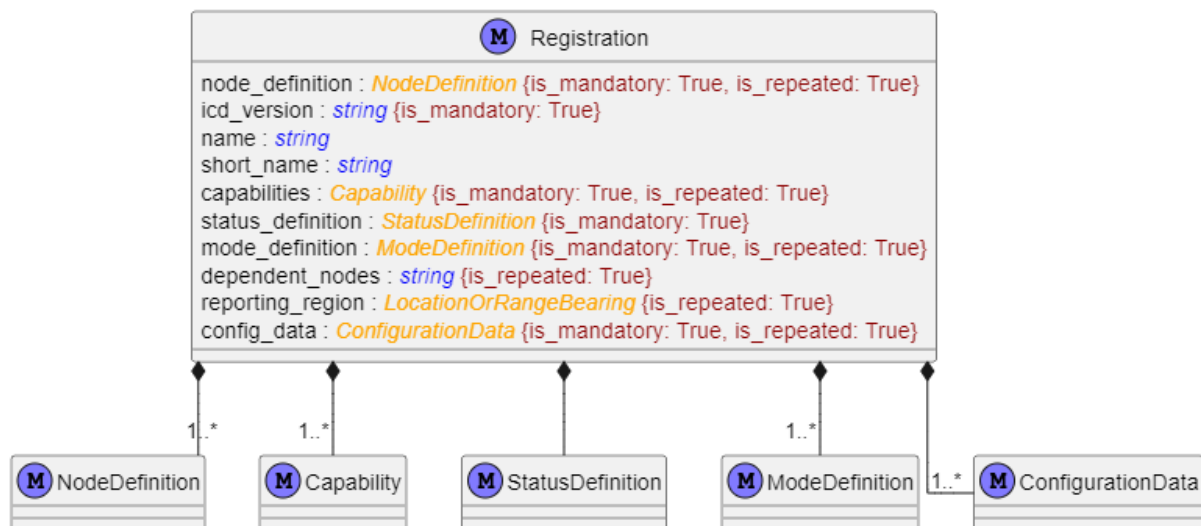


Figure 12 UML representation of the Registration message.

The top level of this message is presented in Figure 12. The first field is the *node_definition* which can be repeated multiple times.

The *ICD_version* field (see Figure 12) SHALL be populated with the current STANREC 4869 version,

"BSI Flex 335 V2.0 / NATO STANREC 4869 Ed A V1.0"

rather than only the BSI version. Sending the current STANREC version ensures proper interpretation of the messages by the fusion node.

The fields: name, short_name, capability and status definition (see Figure 12) follow the BSI Flex 335 definition. The mode_definition field has some specific population

rules in the AEDP 4869 implementation. The ModeType, ScanType, TrackingType and DetectionDefinition's location_type fields are to be used as described in the BSI Flex 335, however it is recommended to use the WGS84_E system with the LAT_LNG_DEG_M coordinate system for C-UAS applications.

5.3.4.1. Node Definition

The *node_definition* field contains the platform field, which aligns with the BSI Flex 335 definition. Besides that, the Node type field is present, which in the scope of AEDP 4869 can have the following values;

- Other
- RADAR
- LIDAR
- CAMERA
- ACOUSTIC
- PASSIVE_RF
- KINETIC
- JAMMER
- CYBER
- LDEW
- RFDEW
- MOBILE_NODE
- POINTABLE_NODE
- FUSION_NODE

Where the CAMERA type is used for both EO and IR sensors.

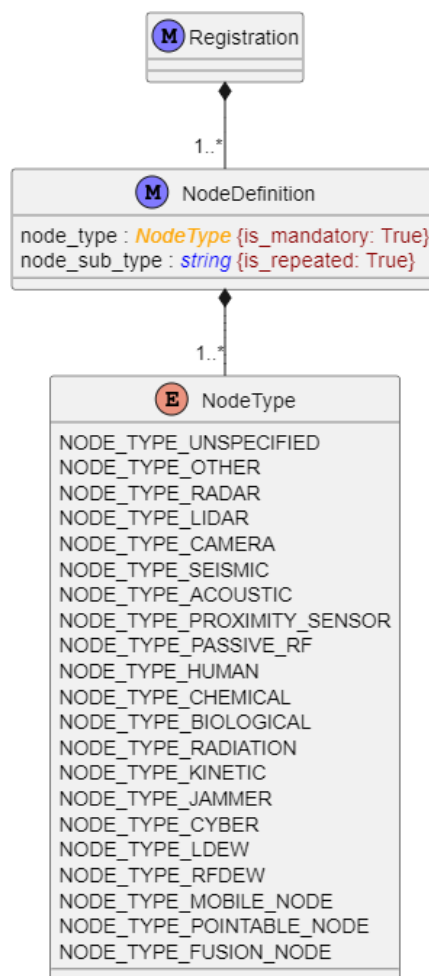


Figure 13 NodeDefinition and the NodeType values recommended in AEDP 4869.

5.3.4.2. Capability

The Capability element, which is mandatory under the registration message is depicted in Figure 14.

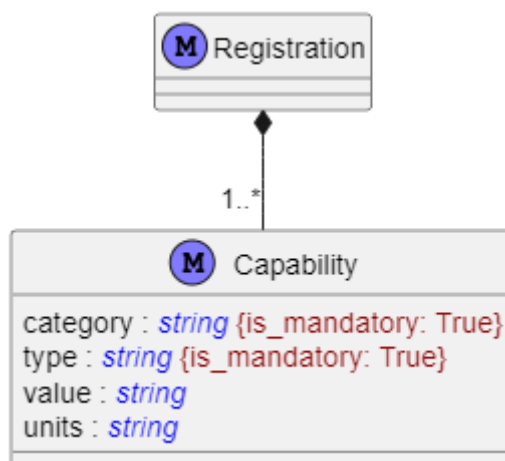


Figure 14 Capability information under the registration message

In the Capability message information relevant to the NODE_TYPE SHALL be provided. For example, in case of a NODE_TYPE_RADAR one could use the following categories:

- category: FMCW, type: Bandwidth, value: 10, unit: MHz;

The units SHALL be restricted to SI values and derivatives of these (e.g. K (kilo), M (mega), G (giga)).

GNSS jamming can be another category, GNSS spoofing another category.

5.3.4.3. Status Definition

The Status Definition Message is the component of the registration message that defines what status messages the node will send. It defines which fields are to be present in status report messages generated by the node and what format and units the fields are to use. The information elements included in this message are presented in Figure 15 Status Definition information under the registration message. Figure 15.

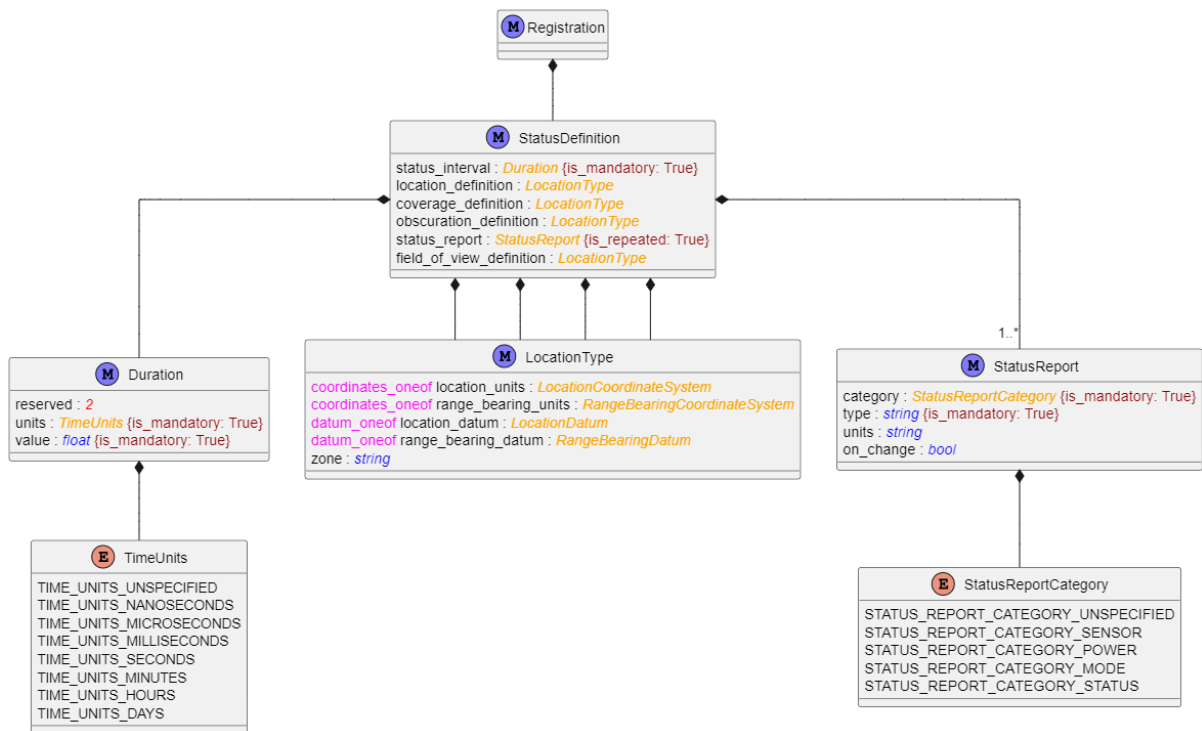


Figure 15 Status Definition information under the registration message.

5.3.4.4. Mode Definition

The Mode Definition Message is the component of the registration message that defines the modes the node can adopt. The information elements included in this message are presented in Figure 16.

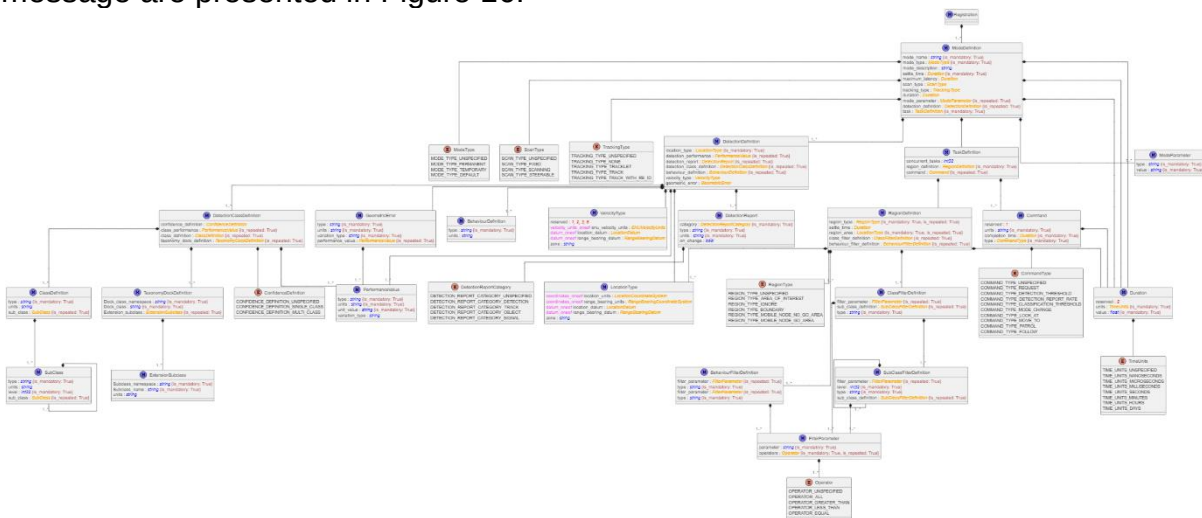


Figure 16 Mode Definition information elements under the Registration message.

For example in the radar case the sensor node can be in the Tracking mode or Surveillance mode. These are basically the modes a C2 can task the sensor node to use.

5.3.4.5. Detection Definition

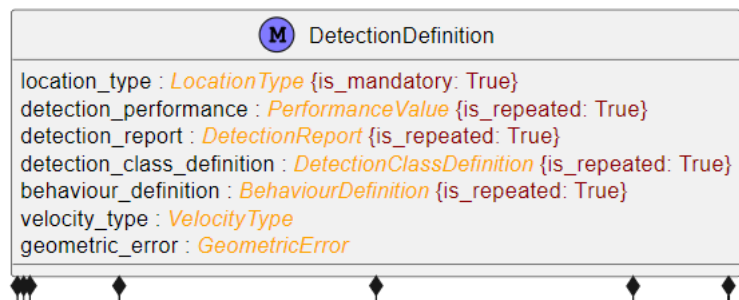


Figure 17 DetectionDefinition class inside of a Registration message.

The `detection_performance` and `detection_report` fields (see Figure 17) remain unchanged with respect to the BSI Flex 355 ICD. In the `detection_class_definition` the class definition should be populated with values originating from the table “*Full list of class names in the SAPIENT object classification taxonomy*” with the remark that the UAV transmitter in the EM transmitter class should be considered to comprise of the UA/UAS/UAV transmitter, as specified in the lexicon. In the Air Vehicle class the subclasses “UAV rotary wing” and “UAV fixed wing” can also be used to indicate the presence of an UAV.

If the sensor edge node is capable of discriminating further subclasses of air vehicle beyond the SAPIENT object classification taxonomy then the edge node should use the taxonomy extension fields in 7.3 of the BSI Flex 355 ICD. This SHALL be declared in the registration message, docking the taxonomy extension into subclass 3 field under the subclass 2 field “other”. If the sensor detects an UAV but is not capable of classifying it as fixed or rotary wing, it SHALL send a detection for both, setting each to a probability of 0.5. If the edge node is capable of decoding the telemetry between the UAV and controller it shall use the EM transmitter with subclasses, UAV transmitter and UAS control station to disseminate the detections for the UAV location and the controller location. If the home location can be disseminated the Edge node shall use the taxonomy extension mechanism to include it under EM Transmitter, Other, Home Location.

For the `behaviour_definition` the Active option SHALL be used in the cases of “piloted” or “autonomous” UAVs. For UAVs in the “dark” state, the Passive option SHALL be used.

The `task_definition` SHALL be populated in line with the BSI Flex 335 ICD where the `location_type` has the same recommended values as the `location_type` in `DetectionDefinition`.

5.3.5. StatusReport Message

The StatusReport message is used by a node to report its state and behaviour (see Figure 18). The StatusReport message can be decomposed in different views:

- The System Management status can be represented by the Power and the Status,
- How the node is currently working can be represented by System and Info, and its current mode (as defined in the Registration Message),
- In certain definition cases (as defined in BSI Flex 335), the node location and information associated with the location can be represented.

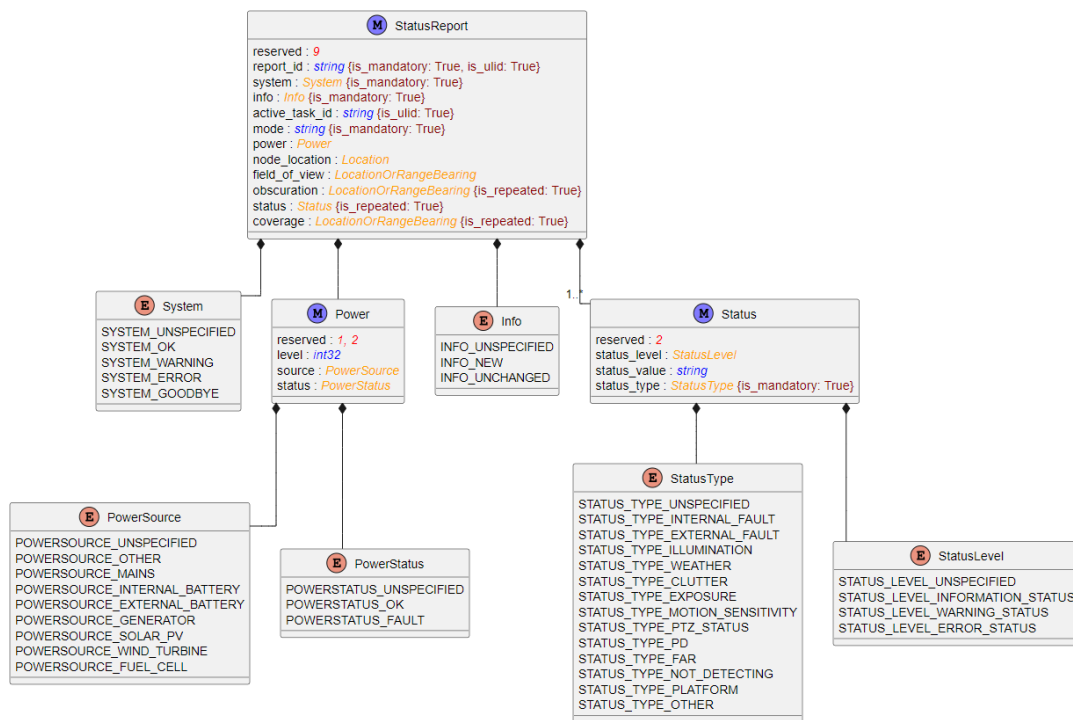


Figure 18 StatusReport Message.

5.3.6. DetectionReport Message

The DetectionReport Message is used to report a detection that a sensor node has made. This detection report is used to detect, track, and inform the C2 system about a UAV flying (see Figure 19). The timestamp of the Sapient message containing the detection report should reflect the time of the detection.

The DetectionReport, similar to StatusReport, can be divided in different sub categories.

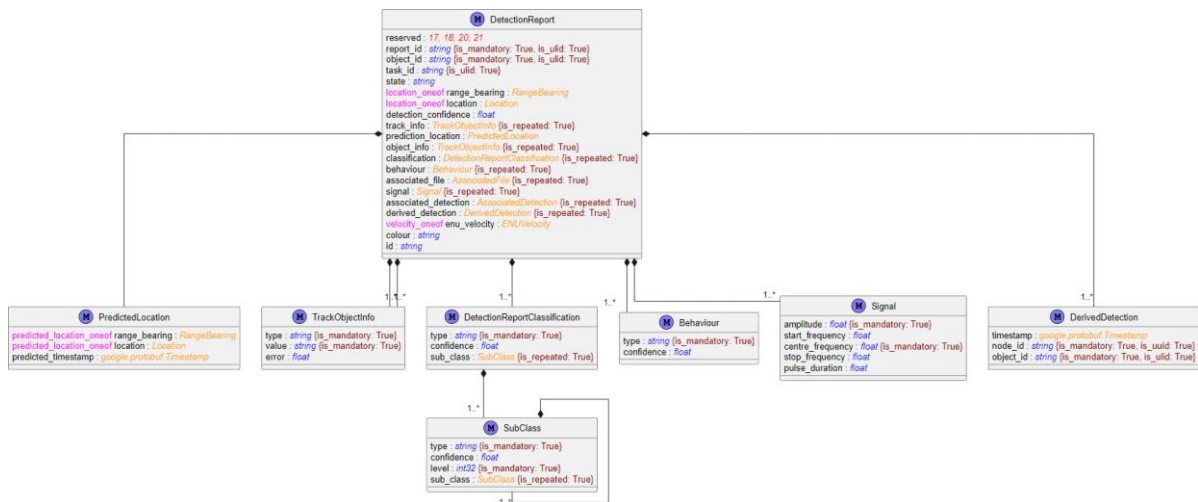


Figure 19 DetectionReport Message.

The Detection Report message is aligned with the definition from BSI Flex 335 Version 2, with the following additional considerations for some fields:

- For the behavior_definition the Active option SHALL be used in the cases of “piloted” or “autonomous” UAVs. For UAVs in the “dark” state, the Passive option SHALL be used.
- If the sensor edge node detects a signal or emission it SHOULD be communicated via the signal field. If additional information is available for example a SigMF file, it SHOULD be disseminated via the associated_file field.

Detections without location information like RF detectors should use the sensor location for detections with a range bearing cone set to 360° uncertainty for the direction and the maximum detection range for the range error.

5.3.7. Task message

The Task message (see Figure 20) is used to direct or request actions from an edge node, either sensor or effector. It specifies what needs to be done, where, when, and possibly how, providing essential information for the execution of tasks. This message is critical for coordinating and managing operations, enabling precise and efficient responses by autonomous systems in a variety of scenarios.

Default tasks can be of explicit or implicit nature. The preference is to use explicit tasks and avoid ambiguity in the default task.

In the AEDP the user can specify that there are no default tasks, to avoid automated engagement of effectors without human approval. Effectively the default task should remain empty to achieve this.

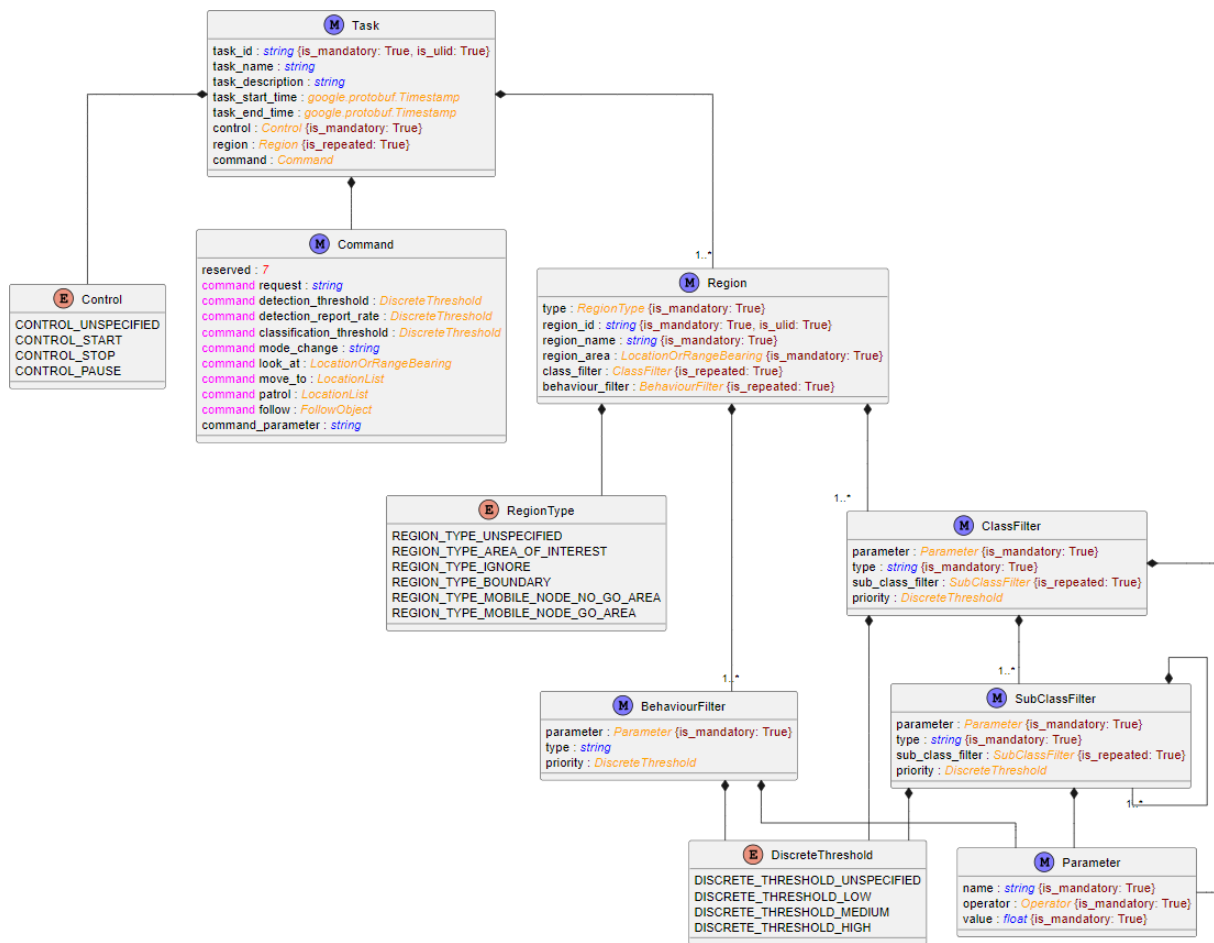


Figure 20 Task Message used by the C2 fusion node to control the sensor and effector edge nodes.

5.3.8. Alert message

The Alert message, as depicted in Figure 21, serves as a critical notification mechanism within the SAPIENT architecture. It is designed to communicate urgent or important information in two use cases:

- a) a node transmitting information to the GUI; and
- b) a node transmitting information to the fusion node that is not covered in a status or detection report.

Examples are significant changes in operational environment, potential threats to a node, or specific events that require immediate attention. Note: alert messages SHALL NOT be used to report UAS detections, these SHOULD be reported in Detection messages. However, they can be used to provide additional information on detections or events for display in a GUI.

The Alert message is structured to ensure clarity and promptness in response, enabling systems and operators to quickly assess and act on the information provided. This message enhances situational awareness and facilitates a rapid and coordinated response across different systems and stakeholders involved in the operations.

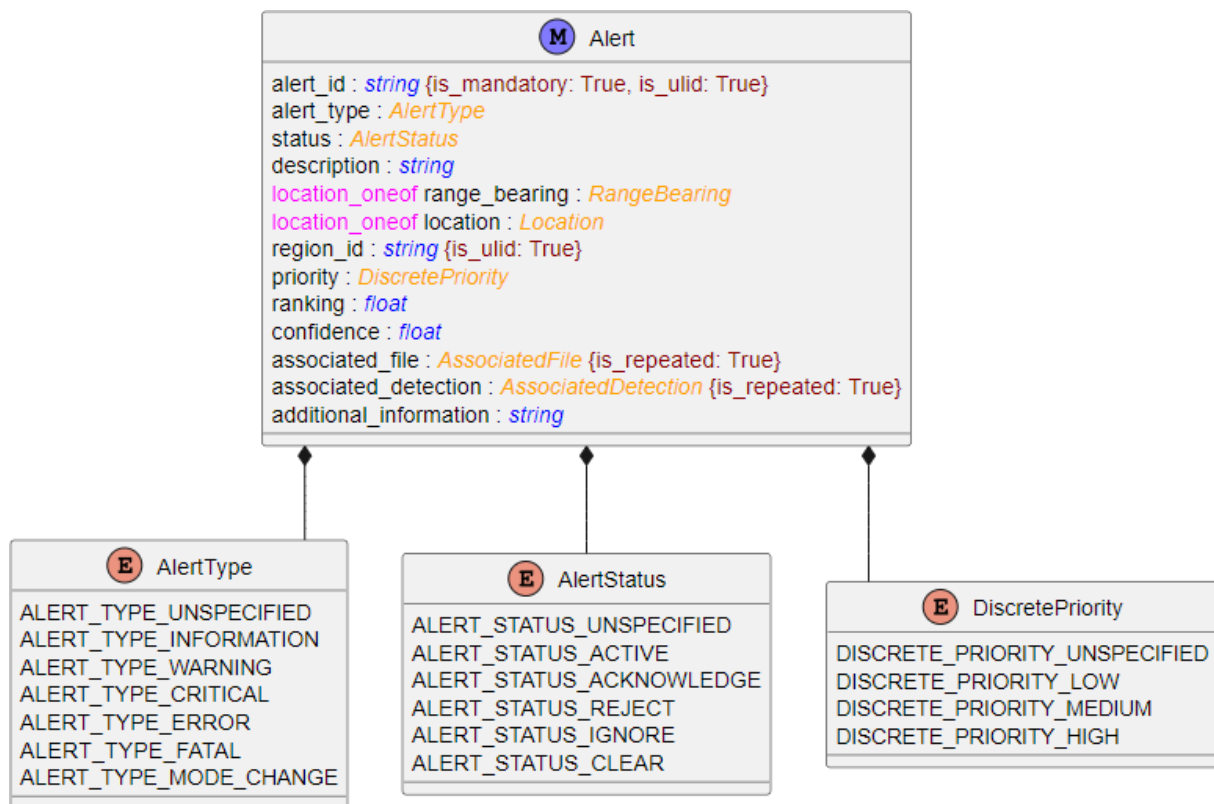


Figure 21 Alert message structure.

See BSI Flex 335 for additional information on Alert messages.

5.3.9. Error message

The Error message, as depicted in Figure 22, is designed to report issues or malfunctions within autonomous systems or sensors. It communicates specific details about errors encountered during operation, including the nature of the error, affected components, and any relevant diagnostic information. This message is essential for troubleshooting and corrective actions, allowing system operators and maintenance teams to quickly identify, analyze, and resolve issues. By standardizing the format and content of Error messages, the SAPIENT standard ensures consistent error reporting and enhances the overall reliability and efficiency of system operations.

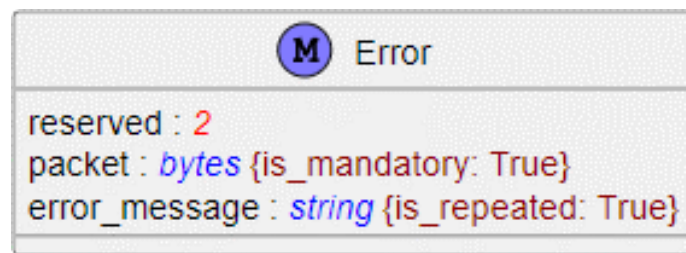


Figure 22 Error message.

CHAPTER 6 *Implementation*

6.1. Transport Layer Mechanism

As described in Clause 4 of the BSI standard [BSI_Flex_335_v2] the minimum requirement is that any SAPIENT implementation SHALL support the TCP/IP network transmission protocol.

This means, for example, that the use of UDP *instead of* TCP is not permitted, however it is permitted to implement a dual (or multiple) configuration system that offers both TCP/IP and UDP (with a software or hardware switch to change configuration). Thus, by local arrangement, all compliant nodes could be configured as UDP and a UDP network established. Any transport protocol on top of TCP/IP is permitted, for example message queuing software, publish/subscribe software or operation over Web services. Some of these solutions may provide benefit but, at the time of writing, none of these options have been implemented or tested.

A proposal was made at NATO Technical Interoperability Exercise (TIE) in 2023 to use broadcast or multicast to support use cases when messages have multiple recipients. This approach however does not support the requirement for single command authority since in the broadcast or multicast architecture sensors and effectors could be connected to multiple C2 systems. SAPIENT in operational use SHALL follow the hierarchical structure in Figure 7, therefore each edge node SHALL connect to one, and only one, C2 system.

6.2. Middleware extension

It is possible, though not mandatory, to run a SAPIENT system with a message handling application, often referred to as a 'Middleware'. The Middleware is completely transparent to the SAPIENT system, as is necessary for a non-mandatory component. An example SAPIENT Middleware is available from the UK Defence Science and Technology Laboratory (DSTL) [Github](#) site under an Open Source software licence – though other SAPIENT Middleware applications, with differing features may be available from other suppliers. Although a middleware is not a compulsory component of a SAPIENT system, there are situations where it may be useful to run a middleware, for example, integration with external systems, or pattern-of-life use cases requiring storage of SAPIENT messages in the middleware database.

6.3. Serialization - Sapiient Header

The BSI Flex document [BSI_Flex_335_v2] (section 4.2 Message framing/structure) introduces the message length header which SHALL be added after the serialization and before sending it through the transport protocol (TCP/IP).

The length of the serialized message without the header should be found and encoded in 4 bytes which is inserted at the front of the message in a 'little endian' format. For example if the message length was 10 bytes the header is equal to 00 00 00 10.

However, 10 bytes is small, a more realistic example is if the message length is 1251, the header is equal to 00 00 E3 04.

6.4. Testing Support

A SAPIENT Test Harness software package has been made available by the UK Defence Science and Technology Laboratory (DSTL) on its [Github](#) site under an Open Source software licence. The Test Harness software enables testing the compliance of SAPIENT components to BSI Flex 335 V2 of the SAPIENT standard. Although STANREC 4869 is based on BSI Flex 335 v2, it makes additional recommendations that the Test Harness will be unable to check. For example, the STANREC may recommend that a field that is Optional in BSI Flex 335 v2 shall always be populated in STANREC compliant systems, but the (BSI Flex 335 v2) Test Harness would not flag a non-compliance if this Optional field was absent. Thus STANREC Users/Developers using the BSI Flex 335 v2 Test Harness will need manually check compliance where the STANREC differs from BSI Flex 335, or develop their own additional testing facilities or procedures for these edge cases.

6.5. C-UAS System Generic Requirements

STANREC 4869 imposes additional requirements on the implementations of the Fusion node when used as C2 system. In particular the Fusion node is required to understand and implement features of edge nodes that register with the Fusion Node. Since these features may be undeclared until the Edge Node registers on the system, they shall be dynamically determined from the registration message.

Some Fusion nodes may support fully autonomous tasking of the registered edge nodes. In this case this tasking logic shall be dynamically configured when the Edge Node registers. In other cases the Fusion Node will support manual tasking (or manual task authorization) via a user interface. In that case, when a fusion node C2 system receives a registration message, the fusion node shall make the specified tasks executable from the interface.

The fusion node shall be able to send the appropriate basic task message to the edge node for all advertised tasks.

For a RADAR system connecting to a fusion node the minimum list of features to be accessible by the end user of the C2 system are:

- Frequency/ bandwidth
- PRI/sleep rate

- TX power
- Area of interest /Active sector
- Ignore detections from a region/Silent sector
- List of available Modes (if the Node supports more than one Mode)

When the RADAR system edge node indicates in the registration message that these can be set via SAPIENT messages, the fusion node shall make these available via the user interface.

For an RF Direction finder these features are:

- Frequency band(s) of interest
- Area of interest
- Ignore detections from a region

For optical systems the following SAPIENT Commands are mandatory in the interface of the C2 system:

- Look_at
- Follow
- List of available Modes (if the Node supports more than one Mode)

For effectors (jammers) connecting to a Fusion Node the minimum list of features to be accessible by the end user of the C2 system are:

- Frequency / bandwidth
- TX power
- Area of interest / Active sector
- List of available Modes (if the Node supports more than one Mode)
- Mode Description field to be populated (if the Node supports more than one Mode)

For jammer effectors the following SAPIENT Commands, as a minimum, shall be supported by the Edge Node and Fusion Node:

- Request: Arm
- Request: Start
- Request: Stop
- Mode_Change (where Edge Node supports more than one Mode)

In case of hierarchical fusion nodes it is recommended that the lower level fusion nodes propagate the registered edge node features to the higher level fusion nodes in their original or aggregated form.

Usage of the Alert message is not mandatory in the implementation of STANREC 4869. The alert message should only be used to disseminate information about the sensor or effector to the fusion node operator, information about detections or status SHALL be communicated using the designated messages.

The Counter UAS Use Case demands low latencies and good time synchronization of all SAPIENT nodes to ensure effective operation.

6.6. Security Considerations for Message Exchange

To ensure the secure handling of information, the standard incorporates specific provisions for managing the security classification of messages, while deferring additional security mechanisms such as encryption or tunneling to the underlying transport network or communication layer.

6.6.1. Security Classification of Messages

To address security within the message exchange framework, the standard mandates the inclusion of information fields in the message structure (see Sapiient Message section) to indicate the security classification level of each message. These fields allow nodes to identify and handle messages according to their sensitivity, ensuring that only authorized nodes process or access the information. The NATO STANAG 4774 is used as reference for security classification information elements, which are concatenated as a string into the “additional_information” field as follows:

- **Policy Identifier:** A mandatory field specifying the Security Policy Authority, which in turn defines the value domain for the other elements within the Confidentiality Information (e.g. NATO, KFOR, GBR).
- **Classification Level:** A mandatory field specifying the sensitivity of the message content (e.g. Unclassified). This ensures that receiving nodes can apply appropriate access controls and handling procedures.
- **Handling Instructions:** An optional field providing additional guidance on how the message should be processed, stored, or disseminated based on its classification (e.g. RELEASABLE TO).

These fields SHALL be embedded within the message format, as specified above, and are designed to support compliance with organizational and regulatory security requirements without imposing specific implementation constraints. By including these metadata fields, the standard ensures that security classification is an integral part of the message exchange protocol, enabling secure and context-aware communication across the SAPIENT network.

In addition, Originator Information is provided in the message identifying the source of the message, enabling verification of the message's authenticity (to some extent) and ensuring compliance with security policies. This information is confirmed during the registration process, which includes an acknowledgement step.

6.6.2. External Security Aspects

The AEDP 4869 standard intentionally excludes prescriptive requirements for cryptographic mechanisms, such as encryption, or network-level security measures, such as tunneling through Virtual Private Network (VPN) channels. These aspects are considered the responsibility of the underlying transport network or communication layer. This approach provides flexibility for implementers to select security solutions that align with their specific operational and environmental requirements.

By deferring these mechanisms to the transport layer, the standard maintains its focus on defining interoperable interfaces while allowing for the integration of robust security practices tailored to the deployment context. Implementers are encouraged to consult relevant standards, to ensure compliance with best practices for secure data transmission.

When implementing the AEDP 4869 standard within API web services, authentication mechanisms are managed as part of the API specification, which is separate from the AEDP 4869 standard itself. A common approach for securing API-based implementations is the use of JSON Web Tokens (JWT) for authentication and authorization. JWTs provide a standardized method for verifying the identity of nodes and ensuring that only authorized entities can access or process AEDP 4869 messages. The configuration and validation of JWTs, including token issuance, verification, and expiration policies, are defined within the API specification and are not prescribed by the AEDP 4869 standard. Implementers should ensure that JWT-based authentication aligns with best practices, such as those outlined in RFC 7519, to maintain secure and interoperable API deployments.

6.6.3. Security Accreditation and Penetration Testing

To authorize the deployment of systems implementing the AEDP 4869 standard in operations, often security accreditation processes are required. These processes typically involve rigorous evaluation, including penetration testing, to identify and mitigate vulnerabilities in the system. Penetration testing should assess both the AEDP 4869 message exchange implementation and the underlying transport layer mechanisms (e.g. authentication, VPN configurations). The results of these tests may have implications for the standard implementation, particularly if vulnerabilities are identified in how security classification metadata is handled or processed by nodes.

6.6.4. Limitations of Cross-Domain Security Solutions Using Data Diodes

The AEDP 4869 standard relies on bidirectional communication to ensure reliable message exchange, particularly through the use of acknowledgement (ACK) messages to confirm receipt and processing of data between nodes. This requirement poses limitations when deploying AEDP 4869 standard in cross-domain security solutions that utilize data diodes, which enforce unidirectional data flow to prevent information leakage between security domains (e.g., from a low-security to a high-security domain). Data diodes inherently block the return path needed for ACK messages, which are a key component of the SAPIENT protocol for ensuring reliable communication.

A potential workaround involves a relaxed implementation where ACK messages are omitted, allowing SAPIENT messages to be transmitted unidirectionally through the data diode. However, this approach is not supported in the current version of the BSI Flex 335 standard (v2.0:2024-03), as it deviates from the protocol's requirement for bidirectional confirmation. Such a relaxation could introduce risks, such as undetected message loss or processing errors, and may require additional error-

handling mechanisms at the application layer. Implementers considering this approach should conduct thorough risk assessments and seek approval from relevant security accreditation bodies. Future revisions of the SAPIENT standard may address this limitation by defining optional configurations for unidirectional deployments, but no such provisions exist in the current specification.

The AEDP 4869 standard security approach is lightweight and flexible, suitable for diverse, interoperable systems, but it delegates critical security functions to the transport layer and external specifications.

6.6.5. Implementation Guidance

Developers and system integrators implementing the SAPIENT standard should:

1. Ensure that all messages include the required security classification fields to facilitate proper handling by receiving nodes.
2. Verify that the transport network implements appropriate security measures, such as VPN, to protect message confidentiality and integrity during transmission.
3. For API-based implementations, integrate robust authentication mechanisms like JWT, as defined in the API specification, to secure access to SAPIENT messages.
4. Conduct security accreditation processes, including penetration testing, to validate the implementation and identify potential vulnerabilities that may require updates to the SAPIENT standard or its deployment.
5. When deploying in cross-domain environments with data diodes, evaluate the impact of omitting ACK messages and implement compensatory measures to ensure reliability, pending future standard updates.
6. Regularly review and update security configurations in accordance with the latest recommendations from standards bodies, to address evolving threats.
7. This approach ensures that the SAPIENT standard remains flexible and adaptable while prioritizing secure message exchange within autonomous sensor and effector networks.

6.7. Legal Protection by Design

When considering the integration of AI applications into C-UAS through the SAPIENT messaging standard, it is important to consider embedding considerations retrieved from the Rule of Law from the outset – this is termed ‘Legal Protection by Design’¹. Trust in AI should be institutionalized through interdisciplinary requirements that combine law, technology, and operational needs. SAPIENT, as a leading example,

¹ Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar and Hildebrandt, M. (2018), *Preregistration of Machine Learning Research Design. Against P-Hacking*. In: E. Bayamlioglu, I. Baraliuc, L. Janssens, M. and Hildebrandt, M. (Eds.), *Being Profiled. Cogitas Ergo Sum*. Amsterdam: Amsterdam University Press.

offers operational flexibility and reduced cognitive burden for commanders, but this also raises questions about accountability and alignment with mission intent. To address these concerns, it is important to perform early legal scoping and scenario-based approaches to identify and mitigate risks, ensuring that AI deployment aligns with the Rule of Law².

Important considerations for implementation of SAPIENT systems include shaping new technical requirements during the acquisition and design phases. These technical requirements should be implemented in the review process of Article 36 Additional Protocol I to the Geneva Conventions. Art. 36 AP I mandates a review of new means and/or methods of warfare. Legal experts, who actively seek for a consolidated understanding with other disciplines - like engineering and mathematics - should be involved early. Using a scenario-based approach encourages collaboration across fields and helps prevent “black box” designs that can undermine accountability after deployment. Verification and validation processes - such as operational testing, serious gaming, and digital twins - are essential to ensure compliance and trustworthiness. These mechanisms should be embedded into the ‘concept’ and the ‘assessment’ phases of the acquisition process, to support responsible use and legal oversight throughout the lifecycle of AI-enabled C-UAS³.

By adopting a scenario-based approach, implementers can guide the responsible deployment of AI in military operations. The approach includes four key steps: capability gap analysis, scenario design, requirement identification, and validating, verifying and implementing requirements⁴. These steps help clarify the legal and operational implications of AI use, ensuring that stakeholders - from developers to policymakers - can make informed decisions. By adopting these measures into the implementation life cycle, SAPIENT compatible equipment suppliers can uphold NATO’s principles of responsible use of AI, including Lawfulness, Responsibility and Accountability, Explainability and Traceability, Reliability, Governability, and Bias Mitigation. The scenario-based approach assists in reinforcing the Rule of Law in technologically advanced warfare contexts. More information is available via the works placed in the references and the research conducted for NATO HQ in the project ‘The Design of AI Applications in C-UAS and the Rule of Law’⁵ for the C-UAS working group (JCGCUAS) wherein a requirements analysis for C-UAS with AI is presented via the scenario-based approach.

² Janssens, L.A.W. in Belli and Gaspar eds. (2023 & 2025). The Quest for AI Sovereignty, Transparency and Accountability, chapter: Clarifying Military Advantages and Risks of AI Applications via a Scenario, pp. 197-213, Springer Nature 2025, pre-published in 2023, *book version available in 2025*.

³ Janssens, L. A. W. & Huijgen, H. (2021). The Juridical Landscape of Countering Unmanned Aircraft Systems in A Comprehensive Approach to Countering Unmanned Aircraft Systems. The Joint Air Power Competence Centre, pp. 394-413.

⁴ L. A. W., Lucassen, O., Middeldorp, L., Lobbezoo, L. & Schoenmakers, O. (2024). Responsible AI: The Rule of Law, Janssens, TNO.

⁵ Liisa Janssens LLM MA, Okke Lucassen MA, Laura Middeldorp MSc, Larissa Lobbezoo MSc (17th April 2024). NATO HQ Report ‘The Design of AI Applications in C-UAS and the Rule of Law’.

CHAPTER 7 <i>Life Cycle and Maintenance concept</i>

7.1. BSI Flex 335, Lifecycle / Maintenance concept

SAPIENT has been developed over several years from a DSTL research programme investigating sensor autonomy, edge processing and fusion.

From July 2023, DSTL has sponsored the British Standards Institute (BSI) to publish the SAPIENT ICD as a BSI Flex Standard. The first BSI published version of SAPIENT (BSI Flex 335 v1) was released in July 2023 on the BSI website. The lifecycle/maintenance process for SAPIENT is now owned and run by BSI and consists of an Advisory Group (AG) that scrutinizes a candidate release drafted by the Technical Author. This draft is circulated to AG members for final, minor, corrections, before being published on the BSI website. Once published, BSI open a public consultation for a set period of time, however, any comments made during the public consultation are held over to the release of the next version of the standard.

Additionally a sub-committee of the AG, the SAPIENT Standardization Sub-Committee (S3C) is run by DSTL as a group of subject matter experts providing technical input into new features in the ICD.

Following the release of BSI Flex 335 v2 in March 2024, it is hoped that future releases of BSI Flex 335 will be on approximately an annual basis. Comments on the current version of BSI Flex 335, or requests for features in future versions can be submitted to Dstl for discussion at S3C meetings by emailing SAPIENT@dstl.gov.uk . Whilst the ICD document is published by BSI, SAPIENT Protobuf files, essential for maintaining interoperability between component providers are published on DSTL's public Github site: <https://github.com/dstl> .

7.2. AEDP 4869 Lifecycle / Maintenance concept

Any standards containing interface control documents or software representations of that standard should maintain a robust lifecycle and process for maintenance of the standard. This enables reliance of the user community (e.g. government, commercial or research organization) on the standard and ensures that investments that rely on the standard can be made with confidence.

7.2.1. Relation of BSI Flex 335 and AEDP

The BSI Flex 335 standard sets the framework for the communication of information in a logical way between edge nodes and fusion nodes, whereas the AEDP 4869 provides more details on how to use SAPIENT in the Counter-UAS area.

The versioning strategy of the two standards, AEDP 4869 and BSI Flex 335, is a critical component in the lifecycle maintenance concept of AEDP 4869. Specifically,

version 1 of AEDP 4869 is linked to version 2 of BSI Flex 335. Given the differing update frequencies (e.g. BSI Flex 335 being revised on an annual basis and AEDP 4869 on a five-year cycle) the need for a coherent versioning and compatibility strategy becomes apparent. This discrepancy in revision timelines necessitates a structured approach to version control and compatibility to ensure that updates to the BSI Flex 335 do not inadvertently render it incompatible with the current version of AEDP 4869.

The frequent updates of BSI Flex 335 allow it to incorporate the latest technological innovations and regulatory changes more swiftly than AEDP 4869. This responsiveness is beneficial but also introduces potential challenges in maintaining alignment with AEDP 4869, which evolves at a slower pace. Therefore, ensuring that each new release of BSI Flex 335 remains functional and relevant with the existing references in AEDP 4869 is crucial.

7.2.2. Backward Compatibility

Backward compatibility is a key strategy in managing these challenges. By ensuring that new versions of BSI Flex 335 are compatible with earlier versions referenced by AEDP 4869, disruptions are minimized, and both standards can continue to function effectively in a synchronized manner. This compatibility supports the integrity of systems that rely on these standards, reduces the need for frequent system upgrades, and helps maintain stakeholder confidence by providing a stable and reliable framework that accommodates both current needs and future developments.

In essence, the versioning approach and backward compatibility measures are fundamental to sustaining the operational effectiveness of AEDP 4869 in conjunction with the more frequently updated BSI Flex 335. These practices ensure that the standards not only coexist but also support and enhance each other, aligning with both current operational demands and future technological advancements.

7.2.3. Compliance testing

Compliance testing is a critical process designed to ensure that systems, products, or services conform to established regulatory, technical, and operational requirements. This testing involves a series of assessments, where the functionality and performance of the item being tested are rigorously evaluated against the specific criteria outlined in the AEDP 4869.

The two important aspects of compliance testing are the verification of:
Compliance of the AEDP 4869 version to the corresponding BSI Flex 335 version,
and Backwards compatibility of the current BSI Flex 335 Version to a specified older BSI Flex 335 Version referred to by the AEDP 4869.

The test is that the candidate AEDP 4869 compliant node populates the messages in the BSI Flex 335 Versions and stay within the prescribed mandatory fields. If this condition is fulfilled, AEDP 4869 will be defined as compliant to the corresponding BSI Flex 335 Version. To ensure that this is feasible a formal validation should be

performed by the SAPIENT Test Harness based on the protocol buffer definitions. With this, first the compliance of BSI Flex 335 Version with generic content, which is in the definitions of the interface control document (such as data types, message length and content) needs to be satisfied.

The check against BSI specifications is necessary but not sufficient, in addition one will need to verify the AEDP 4869 compliance. The content SHALL be specifically populated according to AEDP 4869 and the SAPIENT test harness uses these test values.

INTENTIONALLY BLANK

ANNEX A <i>Example Messages</i>

A.1 Introduction

This section contains examples of messages generated by a typical C-UAS sensor. Alert, Task, Error messages and the acknowledgement messages are assumed to be very similar to the message examples shown in BSI Flex 335 v2 so these are not replicated here.

A.2 Registration Message

A.2.1 Registration message for a sensor edge node

```
timestamp {
  seconds: 1694780145
  nanos: 300463337
}
node_id: "aa399163-0498-407b-ac0b-ed5e31665ec8"
registration {
  node_definition {
    node_type: NODE_TYPE_RADAR
  }
  icd_version: "BSI Flex 335 V2.0 / NATO STANREC 4869 Ed A V1.0"
  name: "long_name_node"
  short_name: "short_name_node"
  status_definition {
    status_interval {
      units: TIME_UNITS_SECONDS
      value: 10
    }
    location_definition {
      location_units: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
      location_datum: LOCATION_DATUM_WGS84_E
    }
  }
}
mode_definition {
  mode_name: "Default"
  mode_type: MODE_TYPE_PERMANENT
  mode_description: "default mode"
  settle_time {
    units: TIME_UNITS_SECONDS
    value: 5
  }
}
scan_type: SCAN_TYPE_FIXED
tracking_type: TRACKING_TYPE_TRACK
detection_definition {
  location_type {
    location_units: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
    location_datum: LOCATION_DATUM_WGS84_E
  }
}
```

```

}
detection_report {
  category: DETECTION_REPORT_CATEGORY_DETECTION
  type: "confidence"
  units: "probability"
}
detection_class_definition {
  class_definition {
    type: "Air Vehicle"
    units: "probability"
    sub_class {
      type: "UAV Fixed Wing"
      units: "probability"
      level: 1
    }
    sub_class {
      type: "Manned Fixed Wing"
      units: "probability"
      level: 1
    }
  }
  class_definition {
    type: "Unknown"
    units: "probability"
  }
}
velocity_type {
  shp_velocity_units {
    angular_units: ANGULAR_UNITS_RADIANS
    speed_units: SPEED_UNITS_MS
  }
  location_datum: LOCATION_DATUM_WGS84_E
}
}
task {
  region_definition {
    region_type: REGION_TYPE_IGNORE
    settle_time {
      units: TIME_UNITS_SECONDS
      value: 1
    }
  }
  region_area {
    location_units: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
    location_datum: LOCATION_DATUM_WGS84_E
  }
}
}
command {
  name: "Start"
  units: "Start"
  completion_time {
    units: TIME_UNITS_SECONDS
    value: 1
  }
}

```

```

    }
    type: COMMAND_TYPE_REQUEST
  }
  type: "REQUEST"
}
task {
  region_definition {
    region_type: REGION_TYPE_IGNORE
    settle_time {
      units: TIME_UNITS_SECONDS
      value: 1
    }
    region_area {
      location_units: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
      location_datum: LOCATION_DATUM_WGS84_E
    }
  }
  command {
    name: "Stop"
    units: "Stop"
    completion_time {
      units: TIME_UNITS_SECONDS
      value: 1
    }
    type: COMMAND_TYPE_REQUEST
  }
  type: "REQUEST"
}
}
}

```

A.2.2 Registration message for an effector edge node (Jammer)

```

{
  "timestamp": "2025-06-03T13:29:23.589253Z",
  "node_id": "e052c885-e30f-405a-8a64-9ed23f96a246",
  "registration": {
    "node_definition": [
      {
        "node_type": "NODE_TYPE_JAMMER"
      }
    ],
    "icd_version": " BSI Flex 335 V2.0 / NATO STANREC 4869 Ed A V1.0",
    "name": "long_name_node",
    "capabilities": [
      {
        "category": "Jammer",
        "type": "Power",
        "value": "10",
        "units": "W"
      }
    ]
  }
},

```

```

"status_definition": {
  "status_interval": {
    "units": "TIME_UNITS_SECONDS",
    "value": 0.5
  },
  "location_definition": {
    "location_units": "LOCATION_COORDINATE_SYSTEM_LAT_LNG_DEG_M",
    "location_datum": "LOCATION_DATUM_WGS84_E"
  },
  "status_report": [
    {
      "category": "STATUS_REPORT_CATEGORY_SENSOR",
      "type": "location",
      "on_change": false
    },
    {
      "category": "STATUS_REPORT_CATEGORY_POWER",
      "type": "status",
      "units": "OK, Fault",
      "on_change": false
    },
    {
      "category": "STATUS_REPORT_CATEGORY_MODE",
      "type": "mode",
      "units": "Default,Jamming",
      "on_change": false
    },
    {
      "category": "STATUS_REPORT_CATEGORY_STATUS",
      "type": "SelectedFunctions",
      "units": "300mhz is selected,600mhz is selected,gps is
selected,2.4ghz is selected,5.2ghz is selected,5.8ghz is selected,500mhz is
selected,900mhz is selected,all is selected,None",
      "on_change": false
    },
    {
      "category": "STATUS_REPORT_CATEGORY_STATUS",
      "type": "JammerActive",
      "units": "true,false",
      "on_change": false
    }
  ],
  "field_of_view_definition": {
    "range_bearing_units": "RANGE_BEARING_COORDINATE_SYSTEM_DEGREES_M",
    "range_bearing_datum": "RANGE_BEARING_DATUM_TRUE"
  }
},
"mode_definition": [
  {
    "mode_name": "Default",
    "mode_type": "MODE_TYPE_DEFAULT",
    "mode_description": "System is on standby",

```

```

"settle_time": {
  "units": "TIME_UNITS_SECONDS",
  "value": 1.0
},
"task": {
  "concurrent_tasks": 1,
  "region_definition": {
    "region_type": [
      "REGION_TYPE_IGNORE"
    ],
    "region_area": [
      {
        "location_units": "LOCATION_COORDINATE_SYSTEM_LAT_LNG_DEG_M",
        "location_datum": "LOCATION_DATUM_WGS84_E"
      }
    ]
  },
  "command": [
    {
      "units": "Jamming",
      "completion_time": {
        "units": "TIME_UNITS_SECONDS",
        "value": 1.0
      },
      "type": "COMMAND_TYPE_MODE_CHANGE"
    },
    {
      "units": "Registration,Reset,Status",
      "completion_time": {
        "units": "TIME_UNITS_SECONDS",
        "value": 1.0
      },
      "type": "COMMAND_TYPE_REQUEST"
    }
  ]
},
{
  "mode_name": "Jamming",
  "mode_type": "MODE_TYPE_PERMANENT",
  "mode_description": "Jammer is active",
  "settle_time": {
    "units": "TIME_UNITS_SECONDS",
    "value": 1.0
  },
  "task": {
    "concurrent_tasks": 1,
    "region_definition": {
      "region_type": [
        "REGION_TYPE_IGNORE"
      ],
      "region_area": [

```

```

        {
            "location_units": "LOCATION_COORDINATE_SYSTEM_LAT_LNG_DEG_M",
            "location_datum": "LOCATION_DATUM_WGS84_E"
        }
    ],
},
"command": [
    {
        "units": "Default",
        "completion_time": {
            "units": "TIME_UNITS_SECONDS",
            "value": 1.0
        },
        "type": "COMMAND_TYPE_MODE_CHANGE"
    },
    {
        "units":
"300mhz,600mhz,gps,2.4ghz,5.2ghz,5.8ghz,500mhz,900mhz,all",
        "completion_time": {
            "units": "TIME_UNITS_SECONDS",
            "value": 1.0
        },
        "type": "COMMAND_TYPE_REQUEST"
    },
    {
        "units": "Registration,Reset,Status",
        "completion_time": {
            "units": "TIME_UNITS_SECONDS",
            "value": 1.0
        },
        "type": "COMMAND_TYPE_REQUEST"
    }
]
}
},
"config_data": [
    {
        "manufacturer": "manufacturer name",
        "model": "model name"
    }
]
}
}
}

```

A.3 Status Report Example

```

timestamp {
    seconds: 1694780151
    nanos: 403052356
}

```

```
node_id: "aa399163-0498-407b-ac0b-ed5e31665ec8"
status_report {
  report_id: "01HACC9NKAX1W37WFMNBK17SHA"
  system: SYSTEM_OK
  info: INFO_NEW
  active_task_id: "01HACAZVJP9M3BVQ20A7CKDSM0"
  mode: "Default"
  sensor_location {
    x: 0.10245314715824172
    y: 0.89923266299633742
    z: 65.0434034729004
    coordinate_system: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
    datum: LOCATION_DATUM_WGS84_E
  }
}
```

A.4 Detection Report

```
timestamp {
  seconds: 1694780158
  nanos: 29387895
}
node_id: "aa399163-0498-407b-ac0b-ed5e31665ec8"
detection_report {
  report_id: "01HACC9W2D9R4245EMD9T5B2MN"
  object_id: "000000011NNC7WHW4T53YBH746"
  task_id: "01HACAZVJP9M3BVQ20A7CKDSM0"
  location {
    x: 0.10838393666669571
    y: 0.89595896709357792
    z: 11429.214961894788
    coordinate_system: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M
    datum: LOCATION_DATUM_WGS84_E
  }
  detection_confidence: 1
  object_info {
    type: "covariance_xx"
    value: "5115.60"
  }
  object_info {
    type: "covariance_yy"
    value: "3540.44"
  }
  object_info {
    type: "covariance_zz"
    value: "6926.19"
  }
  object_info {
    type: "covariance_xy"
    value: "-4107.89"
  }
}
```

```
}
object_info {
  type: "covariance_xz"
  value: "-313.87"
}
object_info {
  type: "covariance_yx"
  value: "-4107.89"
}
object_info {
  type: "covariance_yz"
  value: "1356.90"
}
object_info {
  type: "covariance_zx"
  value: "-313.87"
}
object_info {
  type: "covariance_zy"
  value: "1356.90"
}
object_info {
  type: "rcs"
  value: "1.000000"
}
object_info {
  type: "speed"
  value: "228.33"
}
object_info {
  type: "az"
  value: "120.05"
}
classification {
  type: "Air Vehicle"
  sub_class {
    type: "Manned Fixed Wing"
    confidence: 0.9
    level: 1
  }
}
shp_velocity {
  speed: 228.32715636274492
  heading: 2.0952803150648176
  pitch: -0.0055269354688765827
}
}
```

A.5 StatusReport

```
timestamp {  
  seconds: 1694780151  
  nanos: 403052356  
}  
node_id: "aa399163-0498-407b-ac0b-ed5e31665ec8"  
status_report {  
  report_id: "01HACC9NKAX1W37WFMNBK17SHA"  
  system: SYSTEM_OK  
  info: INFO_NEW  
  active_task_id: "01HACAZVJP9M3BVQ20A7CKDSM0"  
  mode: "Default"  
  sensor_location {  
    x: 0.10245314715824172  
    y: 0.89923266299633742  
    z: 65.0434034729004  
    coordinate_system: LOCATION_COORDINATE_SYSTEM_LAT_LNG_RAD_M  
    datum: LOCATION_DATUM_WGS84_E  
  }  
}
```

ANNEX B	<i>Compliance with Existing Standards</i>
---------	--

B.1 Introduction**B.2 Message Fields**

B.2.1 Mapping table of Sapient to Asterix Detection report fields

	timestamp	reportID	objectID	taskID	State	location	rangeBearing	detectionConfidence	trackInfo	predictedLocation	objectInfo	colour	id	class	Behaviour	associatedFile	signal	location	rangeBearing	associationDetection	derivedDetection
I015/000					D																
I015/010																					
I015/015																					
I015/020																					
I015/030																					
I015/050																					
I015/145																					
I015/161																					
I015/170																					
I015/270																					
I015/300																					
I015/400																					
I015/580																					
I015/600																					
I015/601																					
I015/602																					
I015/603																					
I015/604																					
I015/605																					
I015/625																					
I015/626																					
I015/627																					
I015/628																					
I015/629																					
I015/630																					
I015/631																					
I015/SP																					

B.2.2 Status Report

	timestamp	nodeID	reportID	system	info	activeTaskID	mode	power	sensorLocation	fieldOfView	coverage	obscuratio n	statusRegi on	status
I016/000														
I016/010														
I016/015														
I016/140														
I016/200														
I016/300														
I016/400									P					
I016/405									A					
I016/410														
I016/420														

Jean would like to check this with Pavel. Category 62 table needed?

D= Autofilled to measurement plot and periodic report value. P = Position. A = Altitude.

Include a table with SAPIENT fields and the equivalent L16 fields.

B.3 Business Rules

Describe some of the core business rules such as update rate, reporting responsibility etc.

INTENTIONALLY BLANK

AEDP-4869 (A)