GOSSRA

Generic Open Soldier System Reference Architecture

Collaborative Project

PADR_FPSS_A_2017_800783

GOSSRA Architecture for Standardisation - Vol. 5

System View (NSV)

This project has received funding from the European Union's Preparatory Action on Defence Research under grant agreement No 800783 GOSSRA. This document reflects the view of the author(s) and the GOSSRA Consortium, EDA and the Commission are not responsible for any use that may be made of the information it contains.

EUROPEAN DEFENCE AGENCY

Identification:	BL8464A037 REP
Document Date:	31 July 2020
Version:	v1.1
Status:	Final

Dissemination Level: PU: Public

Metadata

Work Package	WP8: Technical Validation
Deliverable Number	D8.5
Due Date:	30 April 2020
Submission Date:	30 April 2020
Lead Partner	GMV
Author(s):	See Section 1.2
Reviewer(s):	All GOSSRA Consortium
Delivery Type:	R: Report
Dissemination Level:	PU: Public

Version History

Version	Date	Author	Organisation	Description
0.1	2019-12-05	Norbert Härle	RME	Initial Release
1.0	2020-04-30	Iñigo Barredo	GMV	Submitted Release
1.1	2020-07-31	Daniel Riggers	RME	Included Stakeholder feedback in Section 2.4.1.1.1.2.3 Final Release

Table of Contents

Table of Figures

Use or disclosure of data contained on this sheet is subject to restriction on the title page of this document

Table of Tables

1 Overview and Summary Information

The Generic Open Soldier System Reference Architecture (GOSSRA) is described in this set of documents and represents the proposal of the GOSSRA Consortium for subsequent standardisation.

The standardisation itself lies outside the scope of this project. However, the consortium plans to propose the architecture to the “C4I and System Architecture” Working Group of the NATO “Land Capability Group Dismounted Soldier System” (LCG DSS) which has been following the work through GOSSRA Presentations and discussions during the course of the project.

The architecture consists of a set of documents with seven volumes /1/, /2/, /3/, /4/, /5/, /6/, and /7/ which contain the different architectural views according to the NATO Architecture Framework v3.1, with the addition of a Security View (see Figure 1-1). It is accompanied by a formal architecture represented by a set of computer files, compiled by using the SparxSystems Enterprise Architect (version 13) /8/.

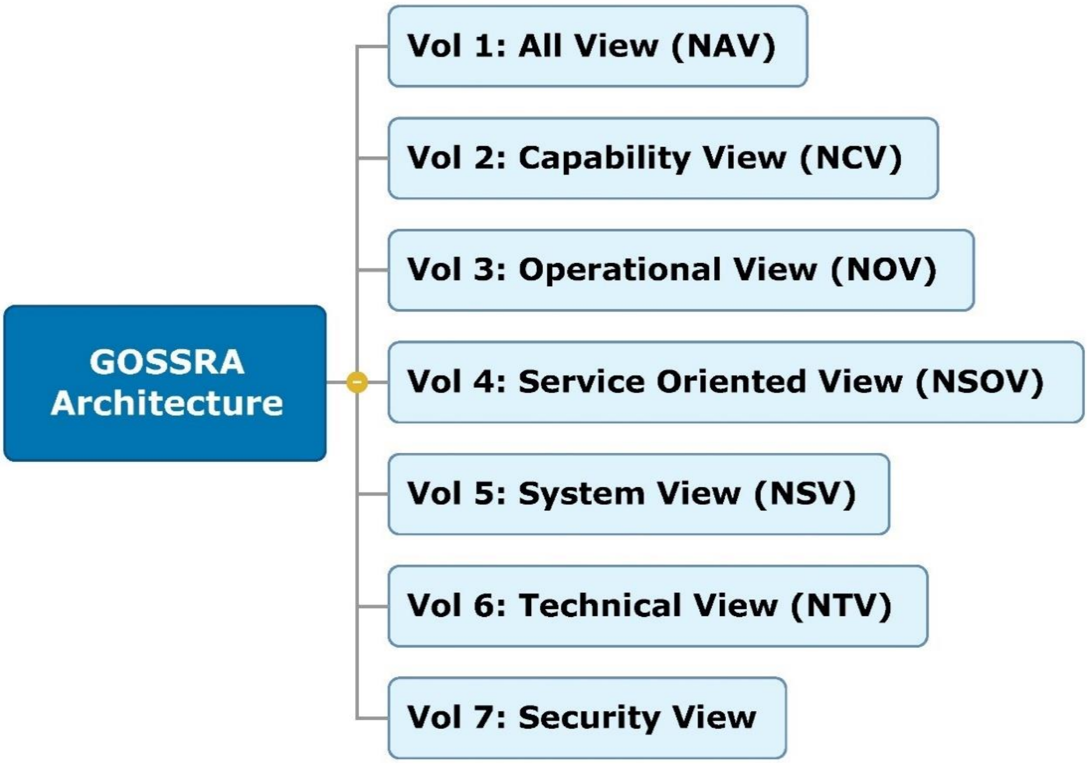

GOSSRA Architecture
Vol 1: All View (NAV)
Vol 2: Capability View (NCV)
Vol 3: Operational View (NOV)
Vol 4: Service Oriented View (NSOV)
Vol 5: System View (NSV)
Vol 6: Technical View (NTV)
Vol 7: Security View

Figure 1-1 – GOSSRA Document Structure

This for Soldier Systems was developed based on following assumptions:

- **This is a reference architecture**. It consists of common best practices and does not depict any one nation's solution. When nations define, specify or develop their specific dismounted soldier system, they may elect to use this architecture as a reference.
- As a reference architecture, it is **not intended to dictate acquisition or procurement decisions**. Rather, it is meant to be used as a template for developing solutions.
- Nations are responsible for **using this reference to create target architectures (solutions)** depicting their implementation including specific equipment for specific roles.
- The reference architecture **standardizes specific aspects where innovation is expected to be slow**, but **leave options open where innovation is fast and competition is desired**.
- **Nations are also responsible for using this reference** when creating system-of-system architectures that include soldier systems.
- This architecture models **a squad as well as a single soldier**. We recognize soldiers do not operate on their own, are networked, and share equipment (especially vehicle platforms). A squad also consists of soldiers performing different roles, e.g. as commander, machine gunner, sniper, scout, medic, or other mission specific role and thus, needing different equipment.
- This architecture focuses on the **electrical and electronic equipment** a soldier wears, carries, and consumes as well as on **software and data communication**.
- This architecture embraces concepts of **interoperability, interchangeability, and commonality**.
- This reference architecture does not strictly and blindly comply with the process and views in the NATO Architectural Framework but rather takes the underlying concepts and uses them to efficiently develop **views which** are thought to be **useful for the purpose and the community**.

1.1 Architecture Scope

The purpose of the Generic Open Soldier System Reference Architecture (GOSSRA) is to serve as a common reference architecture on EU-/NATO-Level for deriving a Target Architecture at country-level.

This Reference Architecture comprehensively focuses on:

- software
- electronics
- voice and data communication
- sensors
- effectors
- human interface devices
- C4I

This Reference Architecture for Soldier Systems is ready for standardization to become openly available and not implying any protected intellectual property. The architecture, to be applied during at least the next 10 years, shall consider trends and potentials with respect to capabilities, operations and technologies.

The architecture represents “best practice”, “future trends and developments” and suggests standard interfaces. It shall be used as a reference to derive the “Target Architecture” which is the architecture for a specific Soldier System to be procured.

By referring to this reference architecture, the “Target Architecture” then:

- is easier to develop,
- includes all major aspects, and
- uses specific common standards enabling interoperability.

1.2 Identification

This set of documents represent the “GOSSRA Architecture for Standardisation” which is the deliverable D8.5 of the GOSSRA project.

The architecture had been developed between the 6th May 2019 and the 30st April 2020 by the GOSSRA Consortium. Led by Rheinmetall Electronics GmbH (Germany), GOSSRA’s consortium encompasses 9 participants from 7 countries: GMV (Spain), iTTi (Poland), Tekever-ASDS (Portugal), Larimart (Italy), Leonardo (Italy), SAAB (Sweden), Indra (Spain) and TNO (the Netherlands) and received an EU grant of roughly €1.5 million over 23 months (1st July 2018 to 30st April 2020).

The companies include major European Soldier System companies which developed and already delivered Soldier Systems in large numbers. Further, participants are smaller companies which provided subsystems or components and contributed their specific and valuable expertise to the project. Finally, a research institute provided knowledge about newest developments and technologies.

Following are the GOSSRA project team members:

- Rheinmetall Electronics GmbH (DEU, prime contractor)
    - Dr. Norbert Härle (Contract Manager)
    - Erik Wimmer (Deputy Contract Manager)
    - Daniel Riggers (Technical Coordinator)
    - Dr. Deepak Das (Technical Expert)
- GMV Aerospace and Defence (ESP)
    - Jose Luis Delgado (Project Manager and Technical Expert)
    - Ricardo Sáenz Amandi (Technical Expert)
    - Vicente Javier de Ayala Parets (Technical Expert)
    - Iñigo Barredo (Technical Expert)
    - Gustavo Alberto García García (Technical Expert)
- ITTI Sp. z o.o. (POL),
    - Piotr Gmitrowicz (Project Manager and Technical Expert)
    - Łukasz Szklarski (Technical Expert)
    - Patryk Maik (Technical Expert)
    - Mateusz Oles (Technical Expert)
- Tekever ASDS Lda. (PRT),
    - António Monteiro (Project Manager)
    - Duarte Belo (Technical Expert)
    - Aleksandra Nadziejko (Technical Expert)
    - Filipe Rodrigues (former Project Manager & Technical Expert)
    - André Oliveira (former Project Manager & Technical Expert)
- Larimart SpA (ITA),
    - Marco Stella (Technical Expert),
    - Fabrizio Parmeggiani (Project Manager and Technical Expert)
    - Luigi Esposito (Technical Expert)
- Leonardo SpA (ITA)
    - Francesco Fedi, LDO (Principal Editor)
    - Rosa Ana Lopez Mazuelas (Technical Expert)
    - Fabio Casalino (Technical Expert)
    - Francesco Cazzato (Project Manager)
    - Antonio DiRocco (Technical Expert)
    - Mazzulli Vanessa (Technical Expert)
    - Zamburru Lorenzo (Technical Expert)

- SAAB AB (SWE)
    - Dennies Olesen (Technicas l Expert)
    - Pär-Åke Anderkrans (Project Manager and Technical Expert)
- Indra (ESP)
    - Pablo Martínez Mena (Project Manager)
    - Ángel Pérez Martín-Nieto (Technical Expert)
- TNO (NLD)
    - Marcel van der Lee (Technical Expert)
    - Angela Kwaijtaal (Project Manager)
    - RonaldRonald in 't Velt (Technical Expert)
    - Eelco Cramer (Technical Expert)

Additional to the consortium, the GOSSRA project established a Stake Holder Advisory Board with representatives from following European Governments:

- NLD
    - Luc de Beer (Mindef, DMO, DP&V, Ressort Projecten, Soldier System Procurement)
    - Major Koen van Veen (Defence Centre of Expertise for Soldier and Equipment)
    - Jasper Groenewegen (DNV GL)
- DEU
    - Dr. Karl-Heinz Rippert (Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support, Soldier System Procurement)
- ITA
    - Magg. Ing. Mattia Bevilacqua (Ministero della Difesa, IV Reparto “Coordinamento dei programmi di armamento”, Direzione di Programma “Forza NEC”)
    - Ten. Col. Vincenzo Bello (Ministero della Difesa, IV Reparto “Coordinamento dei programmi di armamento”, Direzione di Programma “Forza NEC”)
    - Col. Mauro Fanzani (Ministero della Difesa, IV Reparto “Coordinamento dei programmi di armamento”, Direzione di Programma “Forza NEC”)
- ESP
    - Col. Antonio Varo Gutiérrez (ET MDE)
    - Col. (ET) Moisés Serrano Martínez (ET MDE)
- PRT
    -
    - Lt. Col. Luís Paz Lopes (Portugese Army)
    - LTCol Simão Sousa (Portugese Army)

Special thanks for their feedback and contributions.

2 System View

The System View describes the related systems and subsystems that provide support to the required functions and associates the system resources to the Operational View and to the Service Oriented View. The system resources support the operational activities and facilitate the exchange of information among operational nodes. The architecture is applicable to current and future systems and shall provide interfaces that comply with publicly available open standards which are already established or are under preparation.

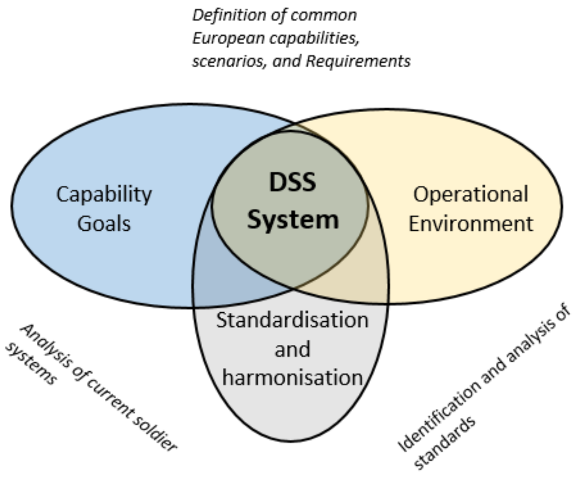

Definition of common European capabilities, scenarios, and Requirements
Capability Goals
DSS System
Operational Environment
Standardisation and harmonisation
Analysis of current soldier systems
Identification and analysis of standards

Figure 2-1 – System architecture context diagram

It considers international operations, interoperability and interchangeability. Special emphasis is given to the definition of interfaces with all necessary layers based on existing or upcoming standards.

The system view illustrates the required systems and devices to support power distribution and data information exchange needs of the DSS with external and internal elements - via wireless communication, radio or cabling transmission.

The DSS architecture is designed to support an open standard System architecture, simple, low cost and highly integrated with the current military systems.

The Standard Architecture for Soldier Systems shall represent a comprehensive reference open architecture for dismounted soldiers performing typical European operations in a squad or similar formation as part of a platoon conducting major combat, counterinsurgency, peace support or peacetime military engagement. Although the architecture focuses on a soldier system for a single soldier with different roles and system configurations, it also considers the squad context, especially regarding the equipment shared at the squad level.

C2 systems are currently essential for providing commanding officers with all the necessary information, and processing capacity to improve their decision taking capability and allow them to act in a proper and informed way.

The system view scope is chosen to be the squad instead of the individual soldier because some devices and power sources are shared between soldiers within their squad. Additionally, depending on the weight that each soldier carries, spare batteries are distributed over the soldiers within a squad.

2.1 System Domains

A set of domains has been identified each addressing a given context where a soldier can operate either as a standalone unit of by interacting with other units of the system.

For each domain, the System View specifies the set of resource and interactions which aims at satisfying the soldier needs for the related context.

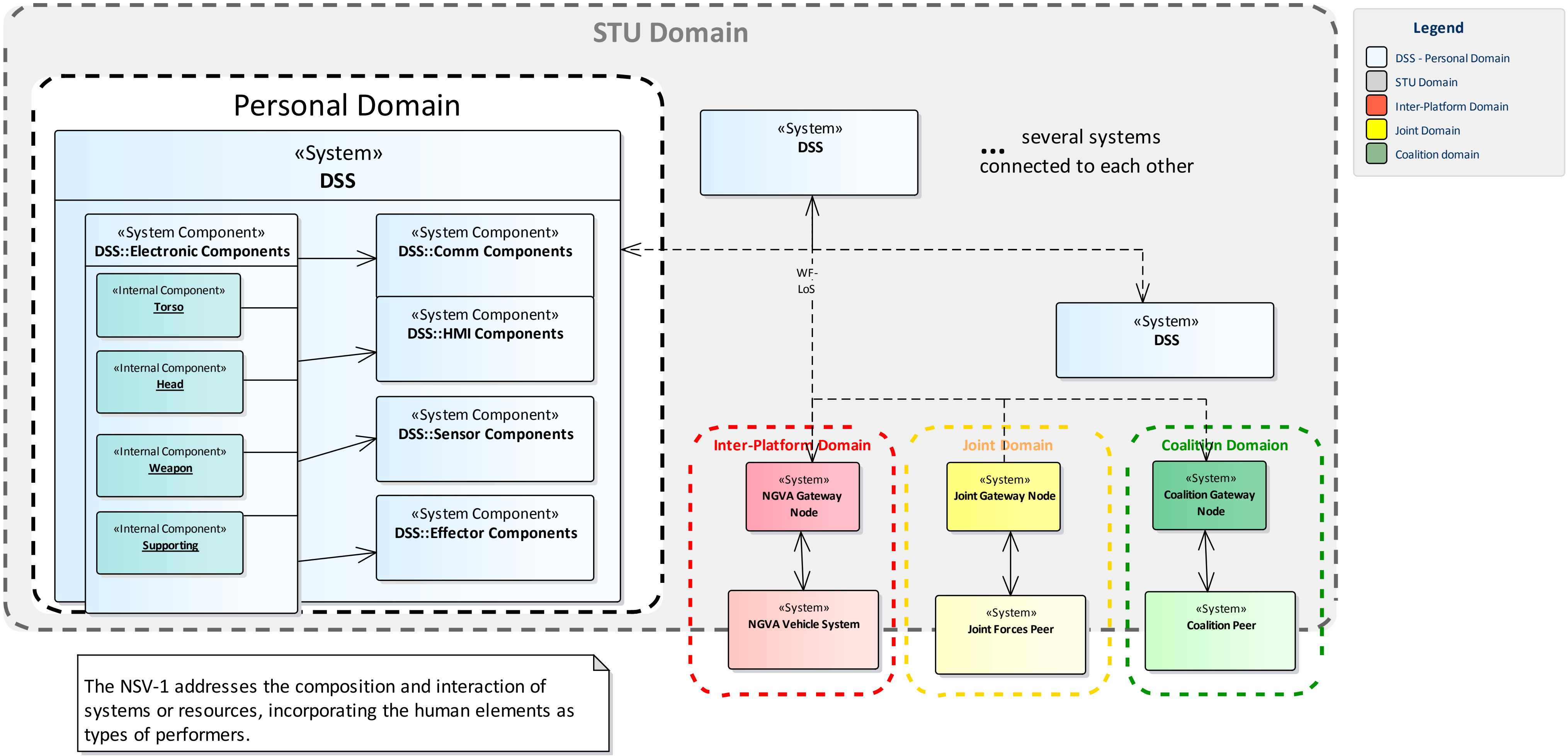
The following domains have been identified:

- **Soldier Personal Domain**, which addresses the needs of a Dismounted Soldier as a stand-alone unit
- **Small Tactical Unit Domain**, which addresses the needs of a Dismounted Soldier as a node of a Squad or Team;
- **Inter-Platform Domain**, which addresses the needs of a soldier as a node that interacts with another platform, e.g. a vehicle. This domain also includes the Mounted Soldier in an Vehicle;
- **Joint Domain**, which addresses the needs of a Dismounted Soldier as a node which interacts with units of different forces;
- **Coalition Domain**, which addresses the needs of a Dismounted Soldier as a node that interacts with units belonging to allied forces.

Figure 2-1 shows the relation between the domains and the relations between the domains.

The domains contain tables with requirements. These requirements can be of three different types.

- Compulsory Requirement (CR)
- Operational Enhancement (OE)
- Required if operational enhancement is available (RE)



The NSV-1 addresses the composition and interaction of systems or resources, incorporating the human elements as types of performers.

Figure 2-2 – System Domains and their relations

2.2 Compliance and Scoring

Throughout the System View, requirements are formulated in Requirements Tables. Although the architecture is meant as reference and the target architecture developer may choose which aspect to use in her/his Target Architecture, there are aspects to which she/he shall comply, e.g. in order to achieve interoperability or interchangeability of devices. This issue is reflected by stating the **"Compulsory Requirements" (CR)**.

Other requirements may be fulfilled in order to enhance the target architecture with additional features. These requirements are labelled as **"Operational Enhancement" (OE)**.

If such OE requirements are desired to be fulfilled, there are further associated requirements which need to be fulfilled in order to support these OEs. They are labelled with **"Required if operational enhancement is available" (RE)**. E.g. if the indicated wireless interface is chosen to be implemented, it will be necessary, that the GOSSRA data infrastructure will be also implemented.

The following states a method for assessing the compliance with the System View or Technical View of this Soldier System Reference Architecture and a scoring system is described for measuring such a compliance. Thus, this scoring system gives some guidance of how much of Reference Architecture is implemented in the Target Architecture. It also encourages the introduction of technical useful features to the target architecture leading to technological better Soldier Systems and a more future proof Target Architecture.

To be compliant, the target architecture needs to **fulfil all CRs**. Thus, it is ensured, that the target architecture follows the most important guidelines of the Reference Architecture. 50 points out of 100 are then given. If not all CRs are fulfilled, the target architecture is considered as "Not Compliant" and the total score is zero.

The remaining 50 points are derived by counting the fulfilled OEs but only if all associated REs are fulfilled. Each fulfilled OE adds 1.28206 points1. The sum of OE points is then rounded off and results in the overall total score:

$$\mathrm{Total}_{\mathrm{Score}} = 50 + \mathrm{Round\_Down}(1{,}28206 * \#\mathrm{of\_fulfilled\_OEs})$$

Example 1:

A target architecture is GOSSRA-compliant (all CRs are fulfilled) and fulfils 20 OEs (with its REs).

$$75 = 50 + \mathrm{Round\_Down}(1{,}28206 * 20)$$

Example 2:

A target architecture is GOSSRA-compliant (all CRs are fulfilled) and uses Bluetooth. To be GOSSRA-Compliant in the first place it will need to fulfil REQ-27, REQ-28, REQ-29 as these Requirements are REs and are bound to the Bluetooth interface. As it now fulfils one OE-Requirement the score will be 51.

$$51 = 50 + Round\_Down(1{,}28206 * 1)$$

[1] 1,28206 = 50 Points divided by total number of Operational Enhancements (OE)

2.3 Soldier System Devices and Configurations

In this section common soldier system configuration are shown. It considers not only the individual soldier but also the squad, as some devices and power sources are shared between soldiers within their small tactical unit (STU). Additionally, depending on the weight that each soldier carries, spare batteries and other types of equipment are distributed among the soldiers within an STU.

2.3.1 Dismounted Soldier System Configurations

As outlined in the analysis of the current DSS systems, there are lots of components and devices available to accommodate almost every conceivable mission. However, every new service added comes at a cost, be it in terms of size, weight or power consumption. Hence, the overall impact on agility[2] should always be taken into account, to ensure that the possible benefits are not overwhelmed by drawbacks.

Taking this into account and the three generic roles identified in the Organizational Relationship Chart (see NOV-4 in the relevant section) and to achieve and facilitate modularity in a soldier system, three configurations have been recommended in the current architecture, however, each nation is responsible for defining what elements are available in each one:

- Minimum Configuration “Basic”
- Minimum Configuration “Commander”
- Minimum Configuration “Role Specific”

These configurations are made up of the minimum set of functionalities/devices for a basic DSS architecture. The final implementation of these configurations depends on the needs of every nation, that is, the target architecture developed for a particular nation might include more functionalities/devices in the *Basic* minimum Configuration than the ones specified in this reference architecture as a minimum set of devices.

[2] Agility is the capability to successfully effect, cope with and/or exploit changes in circumstances, NATO C2 Agility /68/

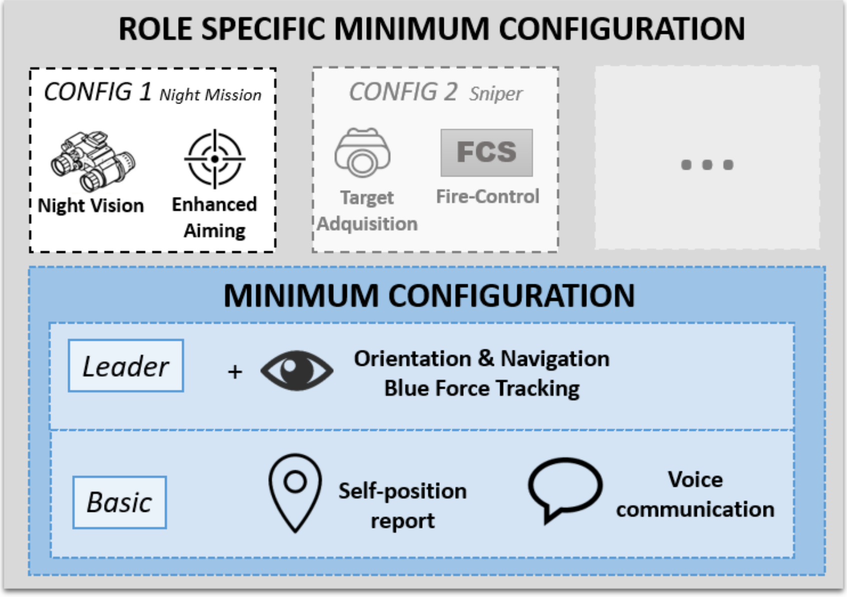


Figure 2-3 – Recommended DSS Configurations based on the functionalities provided

Figure 2-3 shows the services/functionalities provided by the different DSS minimum configurations. The *basic* minimum configuration provides core functionalities: voice and position exchange. These are guaranteed to every soldier in the squad. This *basic* minimum configuration allows the user to communicate not only at squad level with other soldiers and the squad's vehicle but also to communicate with upper levels (platoon) via the squad Commander. Moreover, it allows improving the situational awareness disseminating the squad member's positions inside the group and to upper echelons also via the squad Commander. These two elementary capabilities imply a fundamental improvement for the infantry soldier from an operational perspective. Being able to instantly communicate with any squad member and knowing at all times their locations, allowing for example to reduce the risk of friendly fire. On one hand, the historical evolution of the DSS concept, considering the path followed by the nations that have invested in soldier systems, invite to consider that the best way to build a DSS is to follow a *bottom-up* approach. On the other hand, it is inevitably necessary to consider the command role that a soldier needs to perform in the squad to decide which devices are required. Therefore, it is convenient to distinguish between a regular soldier (*basic* minimum configuration), and a squad Commander (*Commander* minimum configuration), who needs to add devices to ensure the fulfilment of the proposed capabilities.

The benefits obtained distinguishing the *basic* minimum configuration for regular soldiers and a squad *Commander* minimum configuration, considering that the basic minimum configuration is potentially the most numerous deployed configuration, are a reduction of:

- energy consumption, the power supply is still a very restrictive issue in the field,
- costs, lowering the number of devices of the *basic* minimum configuration (the most frequent configuration) allows decreasing procurement expenditures,
- logistic needs, and
- training requirements: the *basic* configuration requires minimum training to be deployed.

The Role Specific Configuration is a composition of the *basic* minimum configuration plus added devices that enable more functionalities. In fact, it is a bundle of different device configurations. To achieve this, specific devices are included such as a long-range radio, a mini UAV, a laser pointer, a thermal optical device, etc. This can be devices allocated to a specific soldier in the squad or shared devices that can be used by several squad members.

The following figure shows the main characteristics of each configuration.

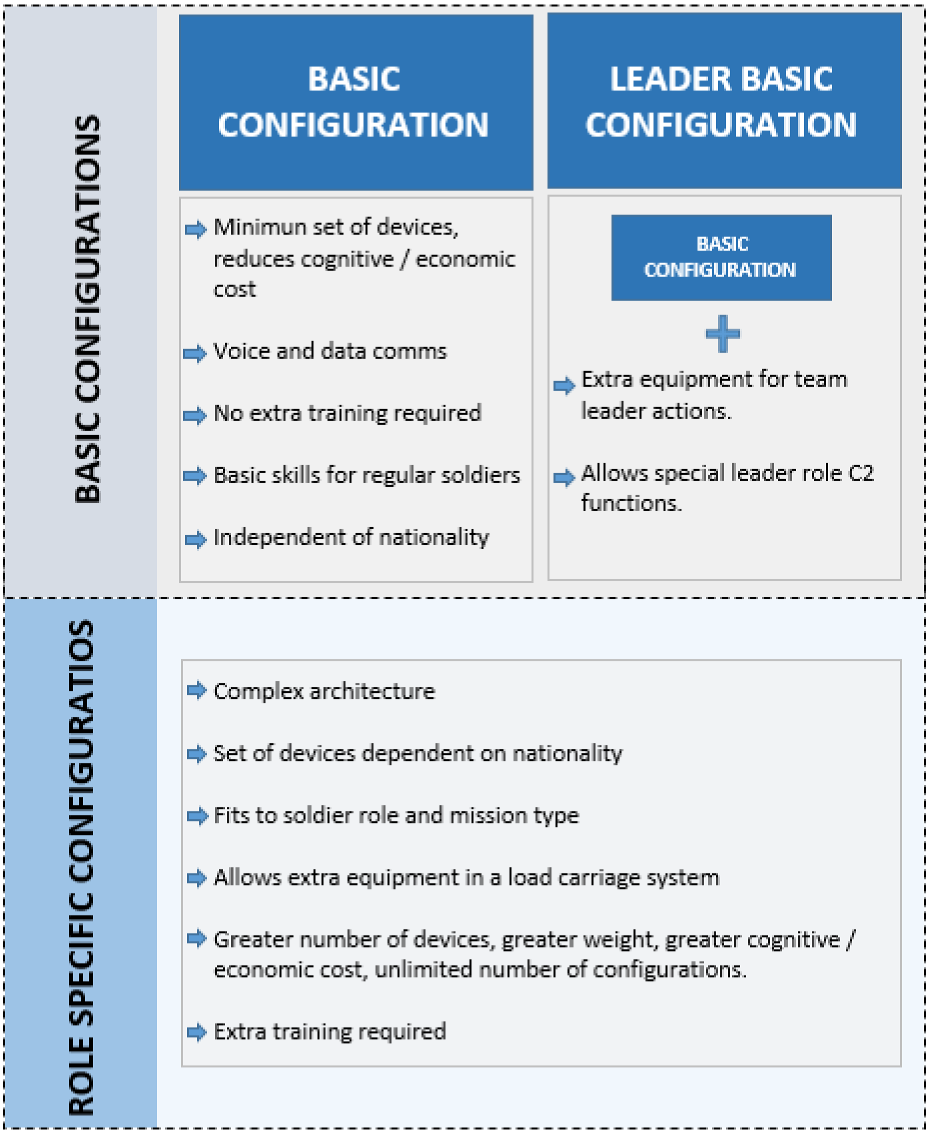
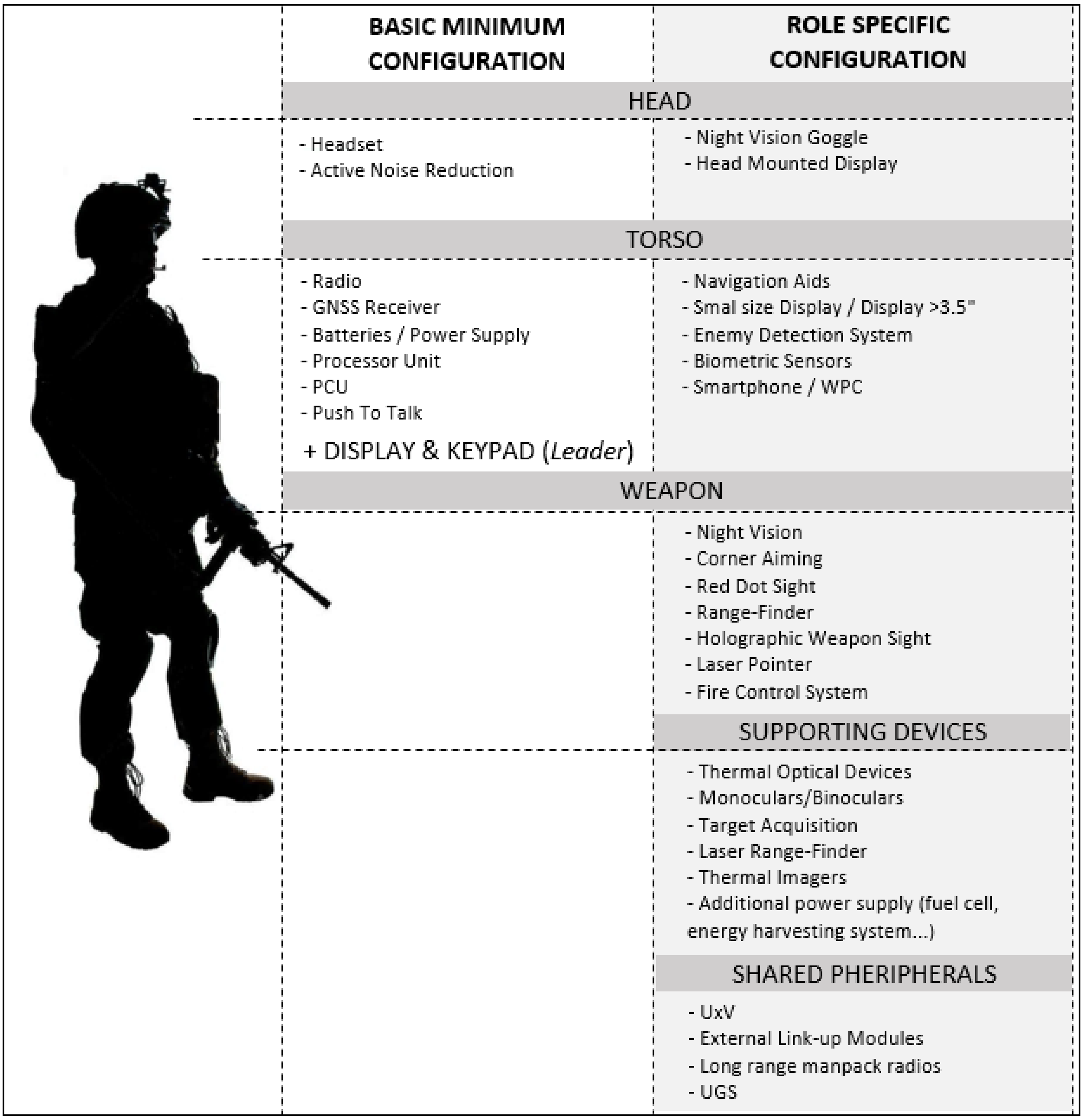

BASIC CONFIGURATIONS
BASIC CONFIGURATION
LEADER BASIC CONFIGURATION
Minimun set of devices, reduces cognitive / economic cost
Voice and data comms
No extra training required
Basic skills for regular soldiers
Independent of nationality
BASIC CONFIGURATION
+
Extra equipment for team leader actions.
Allows special leader role C2 functions.
ROLE SPECIFIC CONFIGURATIOS
Complex architecture
Set of devices dependent on nationality
Fits to soldier role and mission type
Allows extra equipment in a load carriage system
Greater number of devices, greater weight, greater cognitive / economic cost, unlimited number of configurations.
Extra training required

Figure 2-4 – Characteristics of the DSS configurations

This modularity approach, along with the use of standard interfaces, allows easy innovation, facilitating the upgrade of subsystems and the inclusion of new devices which otherwise would require a costly integration development or a completely new system development.



	BASIC MINIMUM CONFIGURATION	ROLE SPECIFIC CONFIGURATION
HEAD		
	- Headset - Active Noise Reduction	- Night Vision Goggle - Head Mounted Display
TORSO		
	- Radio - GNSS Receiver - Batteries / Power Supply - Processor Unit - PCU - Push To Talk + DISPLAY & KEYPAD (*Leader*)	- Navigation Aids - Smal size Display / Display >3.5" - Enemy Detection System - Biometric Sensors - Smartphone / WPC
WEAPON		
		- Night Vision - Corner Aiming - Red Dot Sight - Range-Finder - Holographic Weapon Sight - Laser Pointer - Fire Control System
		SUPPORTING DEVICES
		- Thermal Optical Devices - Monoculars/Binoculars - Target Acquisition - Laser Range-Finder - Thermal Imagers - Additional power supply (fuel cell, energy harvesting system...)
		SHARED PHERIPHERALS
		- UxV - External Link-up Modules - Long range manpack radios - UGS

Figure 2-5 – Considered Equipment needed for all Different Roles

The devices included in a *Role Specific* Configuration of a DSS depend on the functional role to be played and this usually varies between nations.

For devices with low/medium power demand, a power hub shall also be present. However, high power consumers shall include their own battery.

Considering the division into four main categories, head, torso, supporting devices and weapon, the generic device connections are data transport (state, control, data information) and power from the SDCI (see section 2.2), a central power and data hub, or specific device power supply – when additional energy storage is required.

2.3.1.1 Minimum Configuration "*Basic*"

The rationale followed to define this configuration is that the essential services the DSS is expected to provide are those fulfilling the basic needs of the soldier that still allow the DSS itself to be called a system, i.e. a set of connected components forming a complex whole. Therefore, the systems that provide functionality that does not interact with other systems, such as a Red Dot Sight, a Laser Pointer, etc. are considered to be part of the Role Specific Configuration.

The *basic* configuration with a minimum set of functionalities provides essential capabilities for the squad soldier on the battlefield, and is composed of:

- **communications** that allow voice and data communication,
- **voice interaction with active noise reduction** that offers noise cancellation and voice functions,
- **positioning** (usually included in the radio or other devices), situational awareness capability,
- **data processing** that provides the basic computing necessary for exchanging positions,
- **power supply**,
- **HMI** that allows the user interaction, and
- **automatic position reporting,**

The architecture from non-electronic components perspective such as clothing, protection, carrying systems, etc. is out of the scope of this document and should be complemented in a subsequent study.

The *basic* minimum configuration recommended for a regular soldier provides advanced communications, continuous self-positioning and load carriage support customized to the soldier's mission profile.

To provide basic situation awareness, this configuration needs to include a piece of software that performs automatic position reporting. This system can be a simple piece of SW that only exchanges positions. Typically, a state-of-the-art radio includes this functionality. In a Role Specific Configuration this SW system could be included in a complex fully functional C4I system, which in essence performs this position exchange among many other functions.

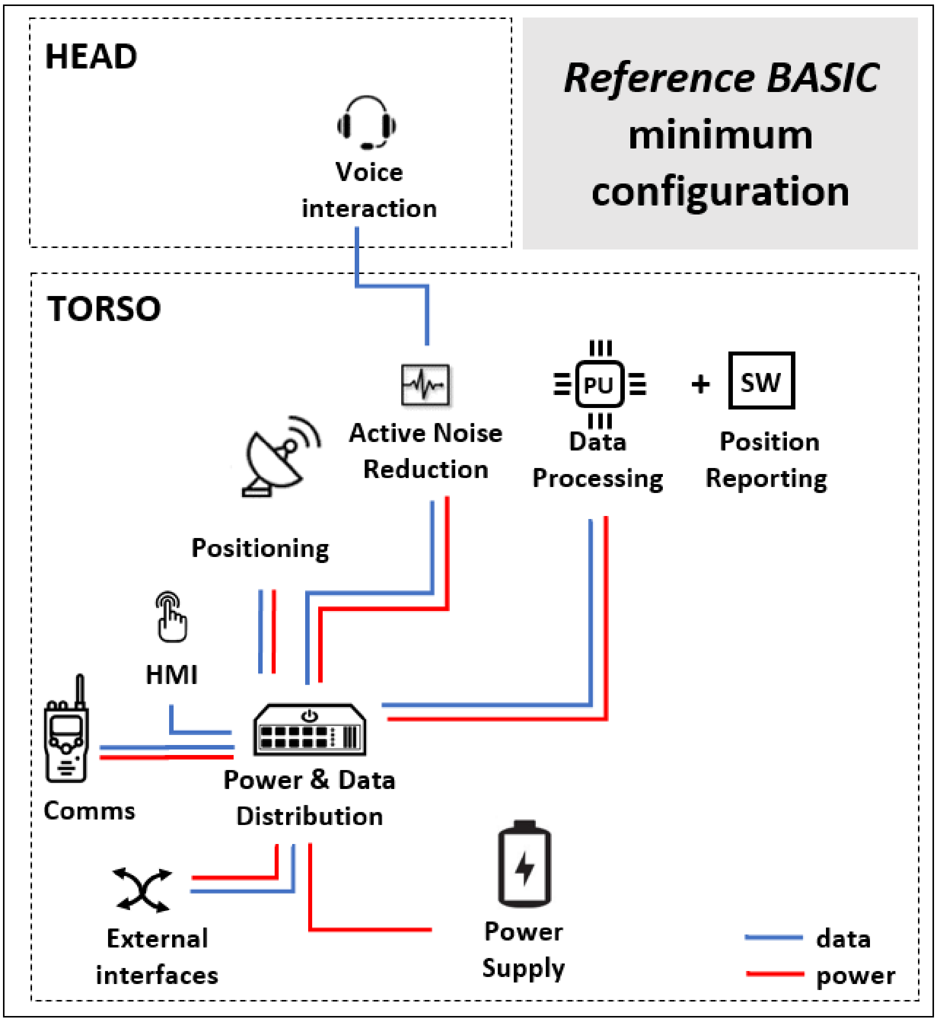


Figure 2-6 – Systems' *Basic* Minimum Configuration for a regular soldier

As we can see in the previous figures, the *Basic* Configuration is the minimum set of devices necessary to satisfy the essential functionalities from an architectural point of view. Note that, the listed components are not necessarily discrete components. For instance, the radio may integrate the GNSS receiver, PU and PTT for example, depending on its complexity. A wearable computing device, customized or COTS, may exchange and show BFT data and partially or completely integrate power and data distribution. Likewise, the Data Hub and PCU could be integrated in a single device.

The integration of several functionalities in a single device is recommended, as long as the affordability and modularity features of the system are not significantly diminished. The advantages provided are that it reduces the weight, cabling, and cognitive burden of the system. In addition, by reducing the number of devices, it reduces energy consumption, which minimizes the need for rechargeable batteries by increasing the operation time between recharges.

As a consequence, the whole life cost of ownership is reduced, and the maintenance of the DSS is simplified. A simple system reduces the training needs for the regular soldier and eases standardization by minimizing the interfaces.

The following figure shows an example of a commercial device that integrates several functionalities.

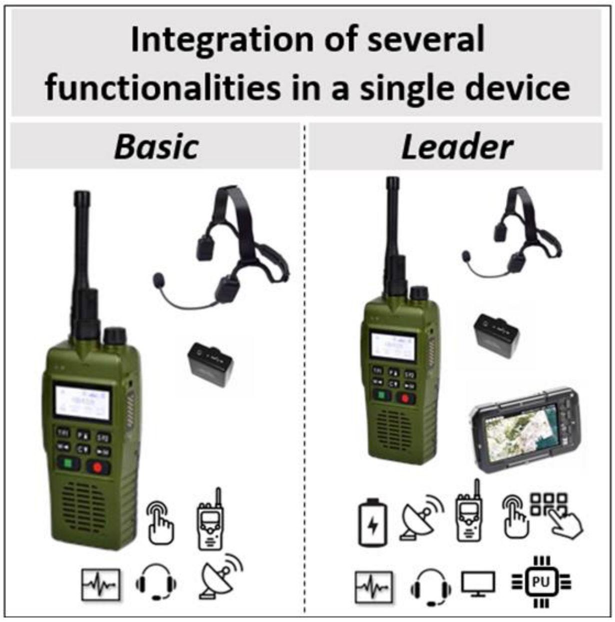


Figure 2-7 – Target Architecture example - Integration of several functionalities in a single device

2.3.1.1.1 *Basic* Minimum Configuration Components

The communication, data processing, and display components enable the squad Commander to send and receive information in real-time, visualize the common operational picture built by other members and upper echelon systems and access to multimedia and data from off-board/on-board sensors. The data source could be the images and video from the helmet or weapon camera of another DSS with a Role Specific Configuration (section 2.3.1.3), from external systems like platforms and UAV or tactical information received from other comrades. These data can be transmitted, along with position and other metadata, to other squad members or to the command post.

In this section, a minimum set of components has been defined for the *basic* and *Commander* Configurations. This set of components could be reviewed in several years and some new elements can be considered since technological development allows the integration of new components with less energy consumption and smaller size. Biometric sensors are likely to be considered as part of the basic configurations if the current privacy issues are solved.

The set of devices to ensure the basic needs of the DSS is detailed next.

Radio

The personal radio is a core device of a DSS, which must include simultaneous voice and data communications, to guarantee intra-squad voice and positions exchange. It is desirable that this radio allows not only intra-squad communication but also inter-squad voice and data communication at the platoon level. Some personal radio systems with advanced capabilities allow the exchange of tactical data (self-position for BFT) not needing an additional processing unit hosted in a WPC or similar. Usually, a state of the art personal radio includes a GNSS receiver and a dedicated battery.

For modularity purposes and to ease the integration it is advisable to use radio models that allow cabling connections using USB or Ethernet.

Data transfer rate requirements for a DSS should enable at least BFT and basic tactical information exchange (tactical objects, orders, requests, etc.). For this aim, assuming the use of the most important message types defined in the STANAG 4677, it is possible to calculate an estimation of the required minimum bandwidth. The white paper “NATO Information Exchange Mechanism for Dismounted Soldier Systems” /11/ offers an estimation of the latency, frequency and average size of the messages, Table 2-1. Considering this information, a more refined analysis considering the specific needs of every nation can be performed to calculate whether a radio fulfils the requirements or not.

Message Type	Frequency of Occurrence	Required Latency	Average size at demonstration	
			XML-Size	compressed with Efficient XML (with schema)
Identification (PRESENCE)	only when entering the network the first time	· < update rate	· 10858 bytes	· 657 bytes
Presence Report (PRESENCE UPDATE)	fast rate (10-300sec)· large number (max.: 4 squads * 10 soldiers)	· < update rate	· 1517 bytes	· 137 bytes
Casualty Evacuation Request (CASEVACREQ)	occasionally	· <60sec	· 4275 bytes	· 626 bytes
Overlay Message (GENINFOMSG)	occasionally	· <300sec	· 2325 bytes	· 617 bytes
Own Land Forces Situation Report (OWNSITREP)	occasionally	· <300sec	·	·
Nuclear Biological Chemical -1 Report (NBC-1)	occasionally	· <60sec	· 477 bytes	· 477 bytes
Contact/ Sighting Report (CONTACT/ SIGHTINGREP)	occasionally but more often than others	· <300sec	· 2261 bytes	· 286 bytes
Text Message with a graphics Object for Overlay transfer	occasionally	· <60sec	· 3507 bytes	· 408 bytes

Table 2-1 – Details of typical transmission-related data for different message types (adapted to the current messages defined in the STANAG 4677 from /11/ p.20)

GNSS receiver

To improve the situational awareness, a GNSS receiver that allows obtaining the current geographical position of the system is necessary. This position is shared with the squad/platoon with the help of a basic processing unit (defined below). The position receiver is typically part of the radio system.

In the context of the European Armed Forces, the GNSS receiver should be a multi-constellation system supporting as a minimum EU Galileo and US GPS systems.

It is highly recommended that the GNSS receiver has protection against jamming and spoofing, making use of the Galileo Public Regulated Service (PRS) signal.

Input Device (HMI)

The system shall offer to the user a physical interface to perform simple operations, namely, system power off/on (master switch), PTT buttons, and other functionalities that require the interaction of the soldier with the system. Normally, these capabilities are integrated in the radio system but could be separated in a specific device, like a wireless PTT mounted on the weapon or a more complex Keypad, a keyboard or touch screen are essential for the Commander minimum configuration in order to give the squad Commander the ability to write and entry complex information.

Processing Unit

The processing unit provides the DSS with the necessary computing capabilities to allow the exchange of positions. It allows the interchanging of the necessary information to ensure the basic soldier capabilities. It can be a stand-alone device or integrated within a radio, a WPC or a Smartphone.

Headset (featuring ANR)

A hands-free headset is necessary to operate without drawing the attention away. In order to maintain communication in battle conditions, it is necessary to have an ANR device for noise cancellation. This ensures the quality of communications at acceptable levels regardless of environmental conditions.

Other Equipment

The *basic* minimum configuration is also composed of ballistic protection, helmet, and a load-carrying vest. This vest must not limit the movements of the soldier while providing a place to mount the devices comfortably.

Modular Lightweight Load-carrying Equipment (MOLLE), provides additional support for heavier combat loads. It is used to define the current generation of load-bearing equipment and backpacks utilized by a number of NATO armed forces, especially the British Army and the United States Army. This method of attachment has become a de facto standard for modular and tactical transport.

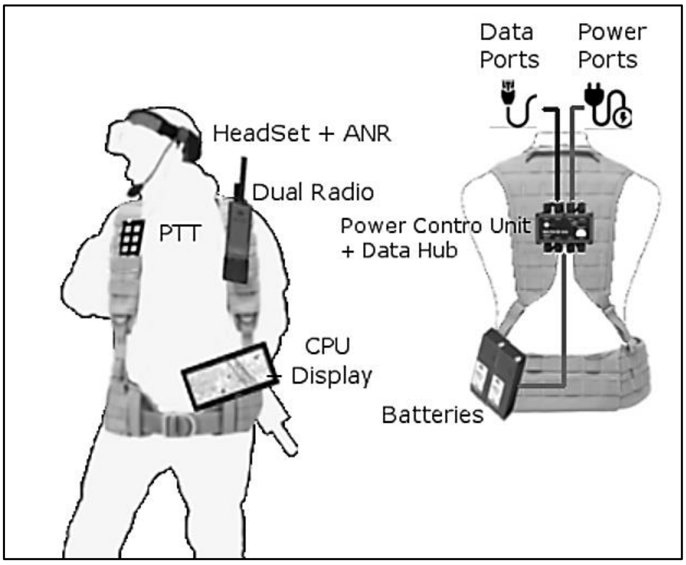


Figure 2-8 – Example of a minimum set of devices on a load-carrying system

New developments in the field of e-textiles (or smart textiles) will enhance the performance of the vests and garments of the soldier, by adding functionalities to them with negligible impact in the SWaP feature of the overall system. For example, the integration in the garment of smart sensors is being considered to monitor the health status of the soldier (i.e.: heart rate, breath rhythm, body temperature, acceleration, etc.) without the need to carry additional devices. The smart sensors, consisting on microelectromechanical systems (MEMS) such as accelerometers, strain gauges, etc., are characterized by their reduced size and power consumption and the high speed and fidelity in data transmission, due to the integration of all the capabilities (sensing, transduction, data processing, transmission of the data and power supply) in the same device, by means of the application of the sophisticated techniques of silicon micromachining used in semiconductor device fabrication.

Other sensors, such as CBRN agent detectors, may be used in the garments belonging to a Role Specific Configuration like that of a CBRN or counter-IED specialist. New technologies, such as quantum dots, allow the integration into the fabrics of very sensitive detectors to a wide range of substances. This approach has been analyzed in some studies financed by the EDA. PROSAFE project had as objective to develop a system to detect the concentration of chemical warfare agents on textile substrates, by adding nanoparticles (quantum dots) to the fabric. VESTLIFE aims to develop a new lightweight and modular bulletproof integral solution, which integrates a CBRN detection system.

E-textiles might provide also a source of power by use of the concept of energy harvesting, that is, capturing energy from an external source such as light (by means of solar cells), heat (by means of thermoelectric generators) or the movement of the soldier himself (by piezoelectric crystals or fibres). Thus e-textiles would be autonomous or at least they would be able to provide some back-up power to their sensors, reducing the usage of the batteries of the soldier system.

Power and Data distribution

The distribution and control of data and energy can be a single device however, head and weapon devices may even have its own processing unit and Power and data distributor with its own power and data hub.

The power and data distribution will consist of the following components:

PCU

The PCU is a power distribution unit designed to work standalone however could be part of the radio or a hub device, the PCU delivers clean filtered power to support a range of standard and special equipment used in the DSS architecture. The PCU protects against overload and monitors the current draw of each output. User-configurable programming makes the PCU a complete power management tool to ensure energy control.

PCU desirable features are:

- The complete power management unit
- High power outputs with built-in overload and short circuit protection
- Current monitoring of each individual output
- Ability to calculate and monitor the battery state of charge
- User-configurable staged shut down to prolong battery life for essential equipment
- Configurable outputs and shutdown characteristics to meet soldier’s requirements
- Compact size to reduce weight

Data Hub

Due to the complexity of the system, which shall allow the addition and interchange of the system devices easily, it is necessary to have a suitable structure to organize the interconnections between the different devices. This hub can be isolated or integrated in a processing unit or in a WPC.

Batteries/Power Supply

The power supply must guarantee the proper performance of the system. The operational requirements (mission profile) and the DSS power needs are the main aspects that can directly influence the power design.

Operational Aspects:

- Mission profile defined by the mission type and duration
- Soldier Role can affect to the configuration needs

DSS power needs:

- Set of devices needed for the selected configuration
- Devices consumption
- Number of connected devices

Wireless power transfer, also known as inductive charging, is another technology in development that could be used in future dismounted soldier power systems. Contactless charging replaces standard connectors with inductive couplings to charge batteries without mechanical or electrical contact.

For wireless power transfer systems, communication between the primary side and the pickup side is a challenge because of the large air gap and magnetic interferences.

Finally, some devices which might be included in the field of exoskeletons can be an additional source of power. Exoskeletons are electromechanical structures attached to the body or the limbs of the soldier which explode the capacity of conversion between electrical energy and kinetic energy. This can be used in both senses: using a source of electrical power to support or multiply the strength of the human movements through electric actuators (this use will be discussed below) or harvesting the kinetic energy of the movement of the soldier to accumulate it as electric charge in a battery. In this last sense, some devices like the Kinetic Energy Harvester The PowerWalk® discussed in the document Extended GOSSRA Architecture - Vol. 11 Upcoming Technologies for Soldier Systems could be used in the Personal Domain

Basic minimum configuration devices provide the core capability: voice and position exchange. They are carried by each soldier in the squad and are present in the basic (core) configuration of the SPS. This basic configuration of a soldier is nation-specific; different nations might define different core devices for the basic system configuration.

In Table 2-2, the power category and location within the soldier system (torso, head, weapon or accessories/supporting) of the devices are shown. Medium power consumers, considered in the soldier power architecture, are connected via USB or Ethernet. High power consumer might be connected to the SPS, but have to be limited in power draw. Low power consumers that are connected to the soldier power system for data sharing might as well use the central energy source to be powered. The power category and location within the soldier system (torso, head, weapon or accessories/supporting) of the devices are shown. Medium power consumers, considered in the soldier power architecture, are connected via USB or Ethernet. High power consumer might be connected to the SPS, but have to be limited in power draw. Low power consumers that are connected to the soldier power system for data sharing might as well use the central energy source to be powered.

		Power consuming devices - Core		
		Low power < 5 Wh < 2.5 W	Medium power 50 – 150 Wh 2.5 – 15 W	High power > 200 Wh > 15 W
Location in the soldier power system	Torso	- Civil GPS	- Intra-squad radio (voice and position)	
	Head	- Headset - Headlight		
	Weapon	- Laser aim point - Flash-light		
	Accessories (backpack)			

Table 2-2 – An example of the core devices that are carried by each soldier. These core devices are present in the basic configuration of the soldier power system

2.3.1.2 Minimum Configuration "*Commander*"

The *Commander* minimum configuration extends the *basic* minimum configurations adding a display with a keypad (or other complex input devices like a touch screen or keyboard), that can be stand-alone or part of a more complex wearable computer, to allow the creation and exchange of tactical information. This hardware and software combination enables the Blue Force Tracking capability and thus, an enhancement of situational awareness. It also enables tactical information management, mission plan management, and navigation.

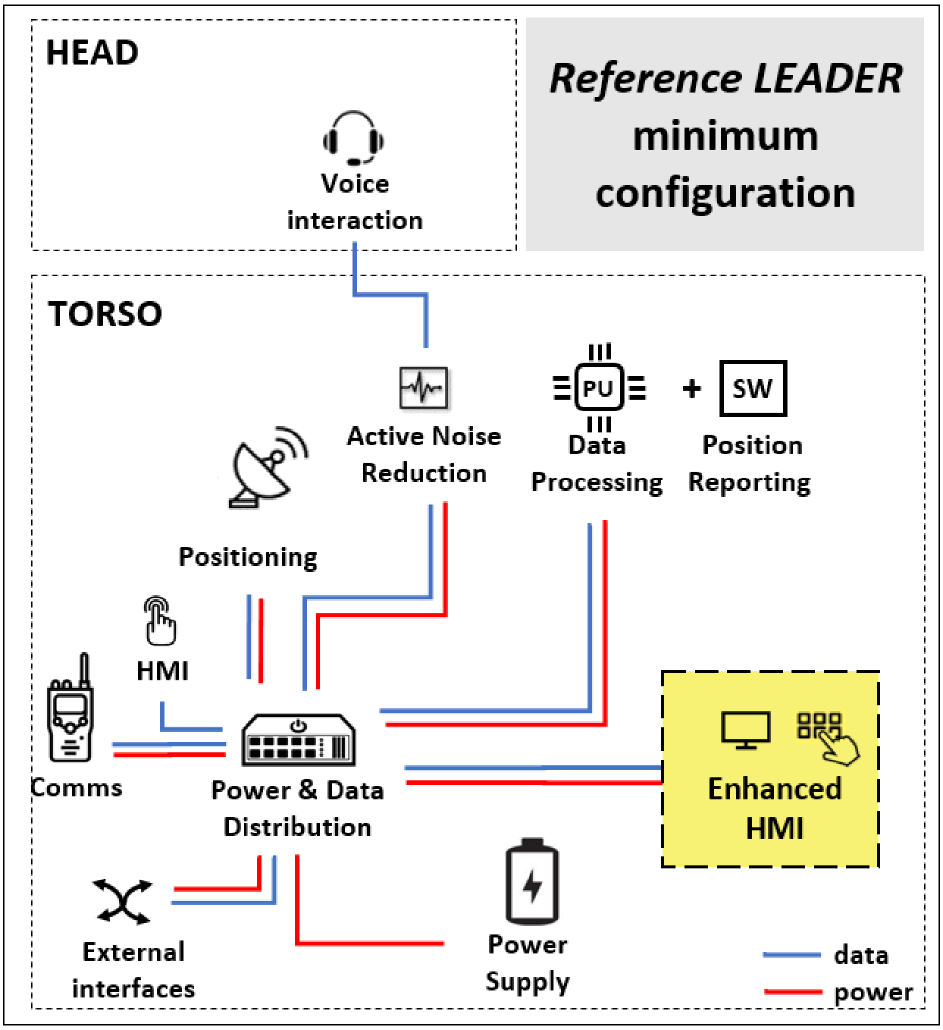


Figure 2-9 – System's *Commander* minimum configuration for a squad/platoon commander

2.3.1.2.1 *Commander* minimum Configuration Components

Display

In a *Commander* minimum configuration, it is essential to have a display system that ensures the operational capabilities of this role, but any soldier could add this device according to their needs in a *role-specific* configuration. The minimum requirements of the display can vary on the mission type and the specific role conditions. These components might be small screens, larger screens that can be placed in the torso of the soldier, or an HMD.

Devices and technologies to improve soldier capabilities

- **Helmet-Mounted Displays**: See-through helmet-mounted displays provide information to the soldier while attending the current situation. Navigation (route guidance) and tactical information, points of interest, and targets can be displayed on the HMD reducing the workload. Non-see-through HMDs limit the field of view.
- **Hand-held/Wrist mounted display**: These devices are similar to the popular smartphones used in daily life, and they can display more complex information than the information that can be shown in an HMD. The drawback is in ergonomics in a combat situation and the fact that these displays require to look down to access the information. Soldier's attention is drawn away from what is happening in the real world.
- **Augmented reality (AR) technology**: Combined with see-through HMD AR delivers heads-up situational awareness with advanced sensors and algorithms that allow soldiers to maintain attention in the operational environment.

An important factor to decrease the soldier's cognitive burden is how to present the information to the operator. In this sense, it is recommendable to take into account the project Multimodal Soldier Interface System (MUMSIS) /12/. This is a research and development project under the framework of the European Defence Agency's (EDA) Combat Equipment for Dismounted Soldier Feasibility Study Programme (CEDS-FSP). It includes an evaluation of the interface between a multimodal (visual, auditory and tactile) wearable system and a soldier from the human factors perspective. The objective of the MUMSIS project is to develop a demonstrator of a wearable system that ensures the timely delivery and collection of reliable and accurate information in a context-adaptive way and supports communication within the chain of command. The project focuses on the human factors in demanding operating environments and tasks. The project utilises and studies technologies including Head-Mounted Displays (HMD) and Augmented Reality (AR).

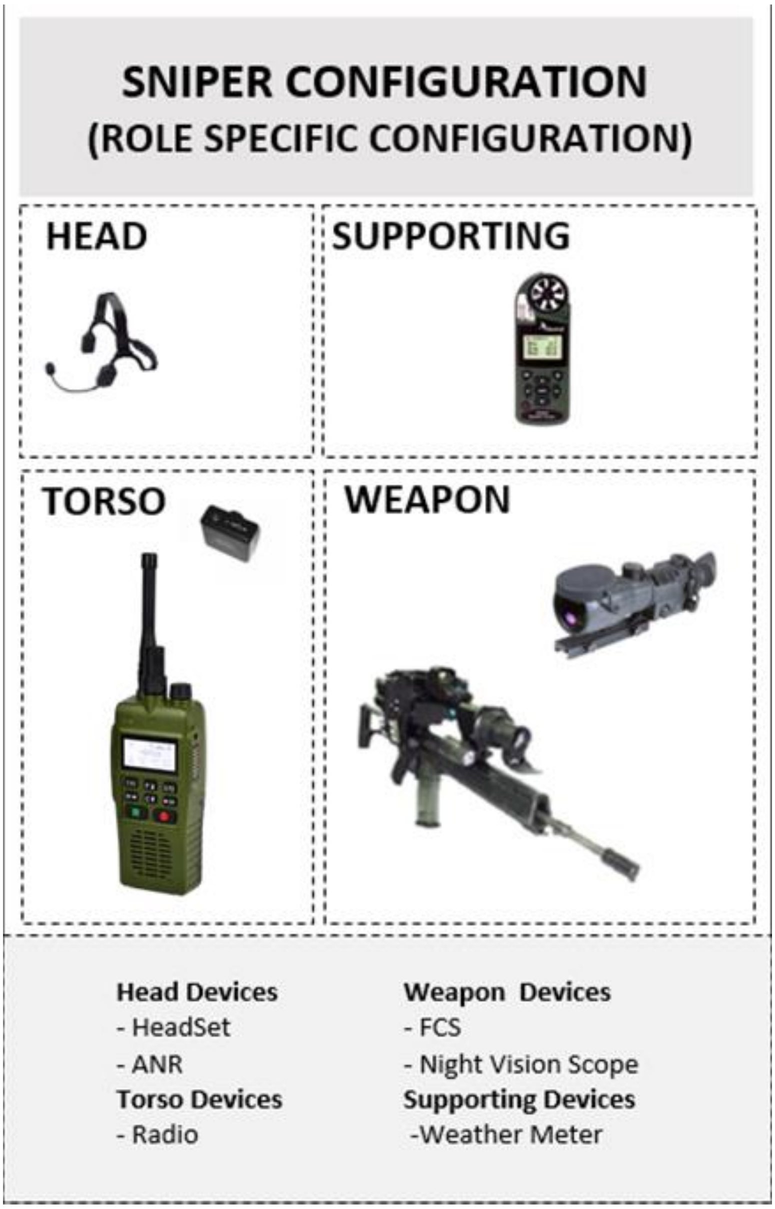
2.3.1.3 Minimum Configuration "*Role Specific*"

With the purpose of reducing system complexity as much as possible, it is considered that the devices added to the *basic* minimum configuration are an extension of the system functionalities that do not belong to the core configuration.

Currently, there are numerous devices to ensure different roles within an army and a particular nation. For this reason, the possible configurations are nation-specific and depend on the operational needs, the mission type to perform (peacekeeping, combat, etc.) and the economic resources.

Also, the type, task, and length of a mission, as defined in the operational view, determine the equipment configuration of the DSS.

As an example, below we can see a target architecture defined for a generic sniper, communications role and SOF, a small set of devices is recommended as a reference, the definition of each type of role as well as the set of available devices to fulfil the necessary functions may vary:



SNIPER CONFIGURATION
(ROLE SPECIFIC CONFIGURATION)

HEAD

SUPPORTING

TORSO

WEAPON

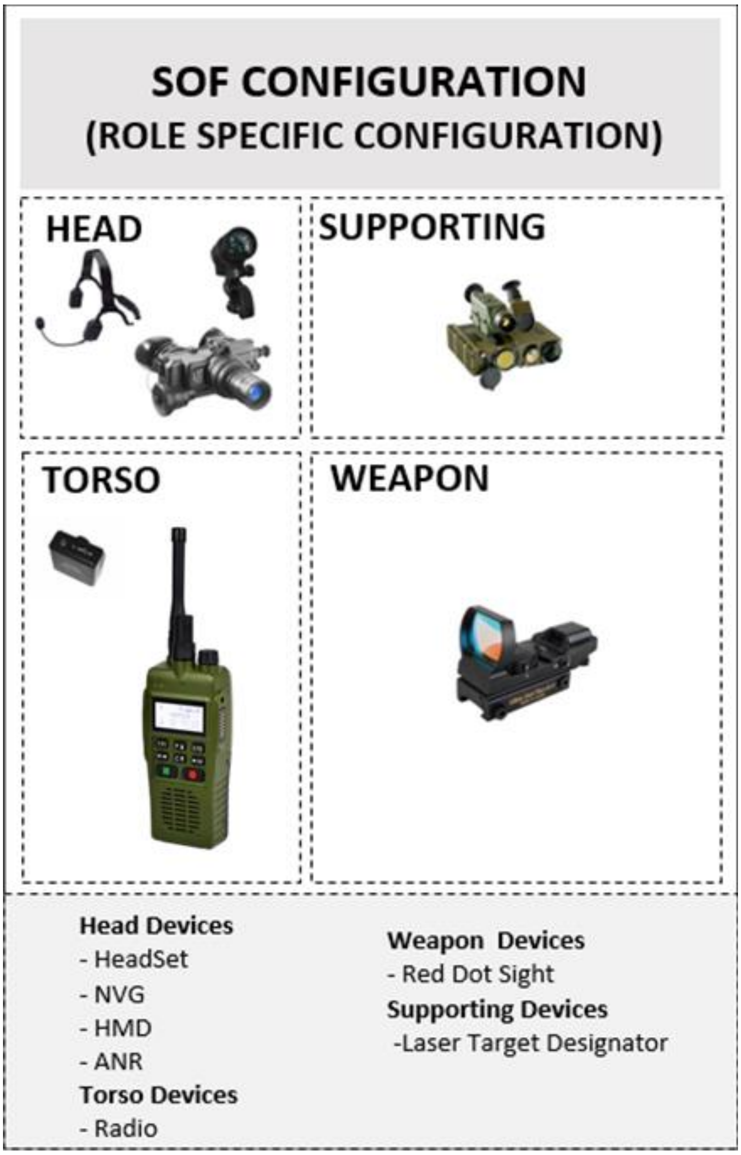
Head Devices
- HeadSet
- ANR

Torso Devices
- Radio

Weapon Devices
- FCS
- Night Vision Scope

Supporting Devices
-Weather Meter

Figure 2-10 – Set of devices for a sniper



SOF CONFIGURATION
(ROLE SPECIFIC CONFIGURATION)

Head Devices
- HeadSet
- NVG
- HMD
- ANR

Torso Devices
- Radio

Weapon Devices
- Red Dot Sight

Supporting Devices
-Laser Target Designator

Figure 2-11 – Set of devices for a Special Ops Force

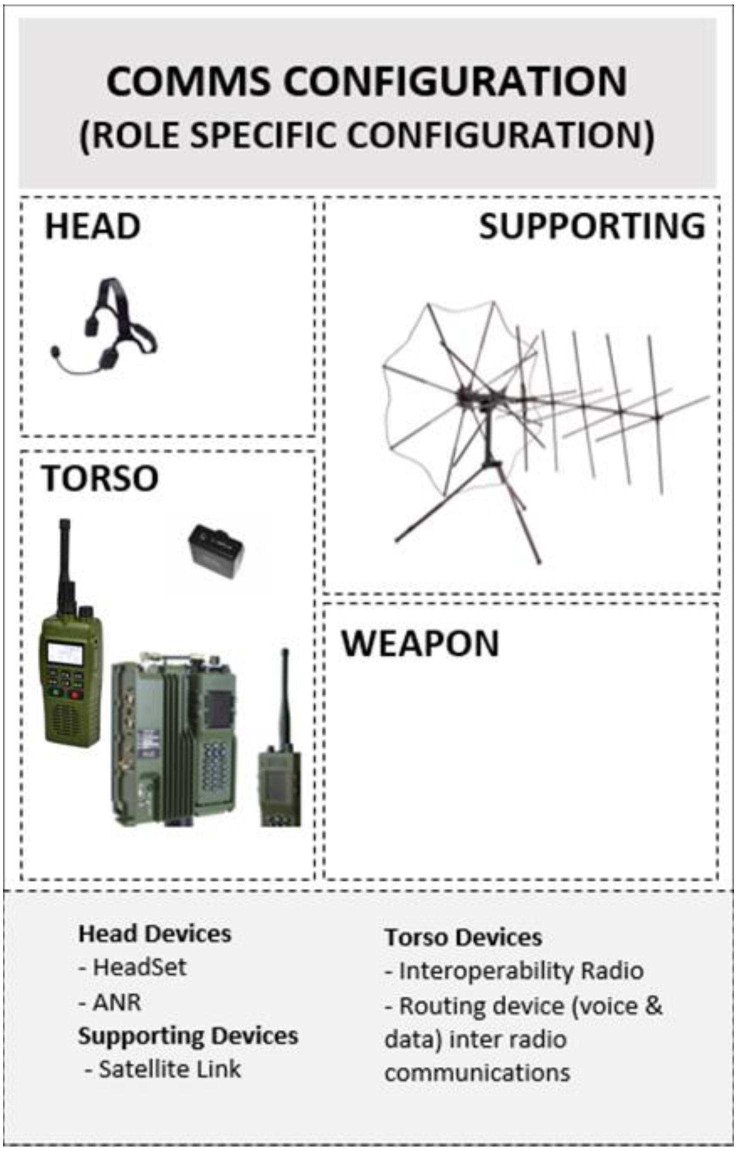


Figure 2-12 – Set of devices for a communication specialist

A *Role Specific* Configuration includes all the elements belonging to the *basic* minimum configuration adding necessary devices to be able to fulfil the specific functionalities of each role. The *Role Specific* configurations detailed in this document are intended as an example, there is an unlimited number of configurations and will depend on the needs of the operational forces of each nation.

2.3.1.3.1 Interoperability Radio

For communications between different forces within a coalition, it is necessary to use an interoperable communication capability. Typically this capability relies on an interoperable radio device assigned to the communication specialist member of the STU or even to each individual soldier. The interoperable radio device can be a physical "Loaned Radio" (as per STANAG 4677) or more simply a common radio based on the same waveform, like the NATO Narrowband Waveform (NBWF) described in the "STANAG 5630" or the European Secure SDR high data rate waveform (ESSOR HDR).

Loaned Radio (STANAG 4677): A Loaned Radio is an interoperability device agreed upon by the involved nations, which is based on the interoperability requirements of the forces. This radio, which fulfils the requirements defined in the STANAG 4677. This radio, which fulfils the requirements defined in the STANAG 4677 VOL 4 /15/ (Loaned Radio for Dismounted Soldier Interoperability), should be provided by one of the nations, (i.e. the supporting nation). It is a radio that meets the necessary waveform characteristics and frequencies to allow communication between coalition soldiers in joint action.

Loaned Radio requirements: The Loaned Radio shall meet the following gateway functionality and hardware specifications at the Local Area Network (LAN) interface towards the JDSS Gateway. If the radio is not compliant with these requirements it is necessary to provide a Radio Adapter to be fully compliant.

- The Loaned Radio shall be connected to the national DSS using the connector defined in the STANAG 4695 /18/
- The Loaned Radio shall have a physical Ethernet layer interface as defined in IEEE 802.3 [9] (minimal 10BASE-T).
- The Ethernet pin assignment shall be as described in STANAG 4695 /18/
- If an IP radio has been selected as the Loaned Radio, it shall have an IPv4 layer functionality.

However, the Loaned Radio should be regarded as an interim solution.

Radios based on common NATO / EU waveform: The implementation of a common waveform can be achieved by traditional radios designed for a specific purpose or by a Software Defined Radio (SDR), the latter being the preferred communication solution.

The NATO C4I WG is currently looking at identifying interoperable waveforms, to be implemented using the SDR technology.

The SDR, in the modern scenarios, provides to the dismounted soldier a tactical communication solution with enhanced capabilities and an extended range over multiple frequency bands; it supports ad-hoc networking (MANET), can manage voice and data over a single or multiple channels, is able to interoperate with legacy radios, can easily adapt to different conditions within a single mission, through selection of the appropriate waveforms.

2.3.1.3.2 Batteries/Power Supply

The SPS distinguishes core devices and group devices (devices for enhanced functionality and devices shared within a squad).

Group devices are only used by specific roles, such as commander display, long-range radio and electronic countermeasures. This can be devices allocated to a specific soldier in the squad or squad devices that can be used by every soldier. For example, a camera can be handed over from one soldier to another. A demining device is used by a combat engineer to detect IEDs.

In Table 2-3, the power category and location within the soldier system (torso, head, weapon or accessories) of the devices are shown.

		Power consuming devices - Group		
		Low power < 5 Wh < 2.5 W	Medium power 50 – 150 Wh 2.5 – 15 W	High power > 200 Wh > 15 W
Location in the soldier power system	Torso	- Digital compass	- Core computer - Military GPS receiver - Control unit with display - Commander Display - Tablet	Exoskeleton
	Head	- Head Torch	- Night Vision Goggle - Enhanced sight - Helmet display	
	Weapon	- Weapon light - Range finder - Laser Light Module	- Thermal imager - Enhanced weapon sight	
	Accessories (backpack)	- Biometric sensor kit - Cable detector - Gas detector	- Handheld NVG - Enhanced sight (observation) - Spotting scope - Counter mining equipment	- Long-range radio - Handheld camera - FLIR - Video camera - Laptop/ portable computer - ROVER - Ground radar - ECM (Jammer) - TACSAT

Table 2-3 – The group devices are devices that might be used by a subset of soldiers within a squad. These group devices should have the possibility to extend the basic configuration.

2.3.2 The DSS Small Tactical Unit (STU) Domain

A DSS Small Tactical Unit consists of individual DSS with full interoperability to improve the functions of the dismounted soldier inside the squad.

The DSS STU provides basic core equipment with sensors, effectors, computers and communication equipment, to each individual soldier according to their specific needs (role-specific configuration). It also includes communication with external systems such as vehicles and other sensors.

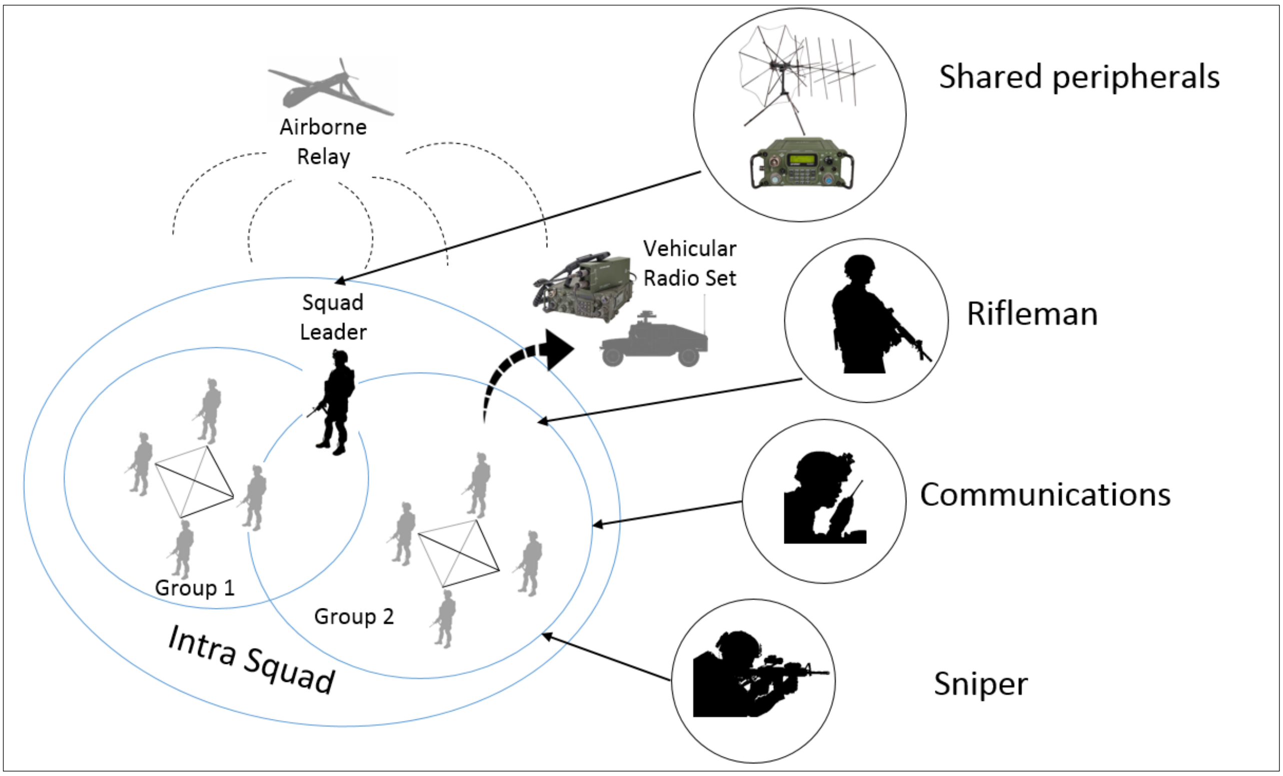


Figure 2-13 – Network Battlefield example with different roles

2.3.2.1 Shared Equipment

In addition to the devices a soldier may carry, at the squad level, there is equipment that can be used by different soldiers. This material includes platforms and devices for mission support, like UGVs, UGSs, UAVs and the squad vehicles.

In some cases, this equipment may be used by a soldier and handed over to another according to the mission needs.

Shared peripherals offer information of general interest, the use of this type of peripherals may not be associated with an independent DSS, for this reason, a special category has been created for this type of devices that cannot be associated with an independent element within the squad.

The list of this type of devices is provided in the Background View (see Shared Peripherals in the Background View). A brief description of the UxVs and UGSs is provided in order to provide an easy understanding of how this set of shared peripherals can help the operational capabilities of the DSS.

UGSs

The UGS systems improve the abilities of the dismounted soldier with easy integration and compatibility with any C4I system. These unattended systems apply advanced algorithms and communication protocols that offer a high probability detection and improves the situational awareness for the DSS. The UGSs are able for real-time target tracking using, for example, seismic or acoustic sensors and Unattended Ground Radars.

UxV

This kind of shared peripherals are powered vehicles that do not carry a human operator, can move autonomously or be managed remotely.

The UAV-aided coverage allows to:

- Provide reliable coverage within the operational scenario
- Provide fast service recovery in case of terrestrial communication failure
- Relaying within the communication network
- Information dissemination and data collection
- Communications between frontline and headquarter

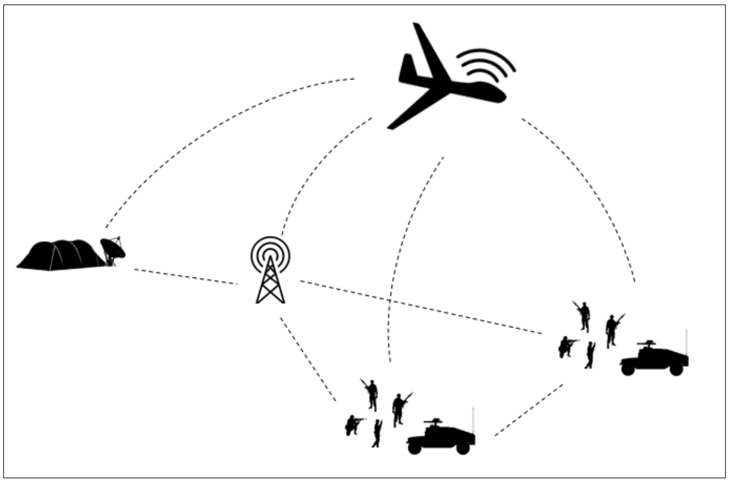


Figure 2-14 – Communication coverage in an operational scenario

DSS capabilities improved with the use of unmanned vehicles:

- Surveillance. Range of vision, advanced processing capabilities and a tactical data link in wide surveillance areas.
- Recognition. Improved threat location with detailed topographic information in real-time.
- Intelligence. Real-time images for immediate interpretation or for greater exploitation to support the joint planning of the mission.
- Acquisition of objectives. Geolocation of the objective to provide direct support to the manoeuvres. Geographic intelligence combined with fire control systems allows the DSS to gain a tactical advantage.
- Easy transport. A wide range of UAV models can be transported in a tactical backpack.

Exoskeletons. *One* application mentioned above is the use of exoskeletons as a means to multiply the strength of the soldier. For example, the system XOS developed by the company Raytheon, is able to multiply the strength of its operator by a factor of 17. The drawback of this kind of systems is that they are strongly power demanding, so they can be used only for specific tasks or members of the squad.

2.3.3 Context of the STU

In this group are the external systems pertaining to Platform, Coalition and Joint domains that exchange data with the DSS. For this exchange, the system provides external interfaces, which can be wired or wireless depending on the needs.

In the case of wireless interfaces the system in its *basic* minimum configuration has a radio that will allow this type of exchange but other possibilities are considered, such as the exchange of data with vehicles through cable, communications with other soldiers in joint actions or communications inter-squad and intra-squad - data and voice.

2.3.3.1 External Data Interface Description

Figure 2-15 shows the DSS Interface Description defining an overarching view on the soldier systems relations to other systems.

Figure 2-16, shows the relationships between external systems and the DSS in a squad/team Commander configuration. The external subsystems will depend on the soldier role and the mission type needs, shows the relationships between external systems and the DSS in a squad/team Commander configuration. The external subsystems will depend on the soldier role and the mission type needs.

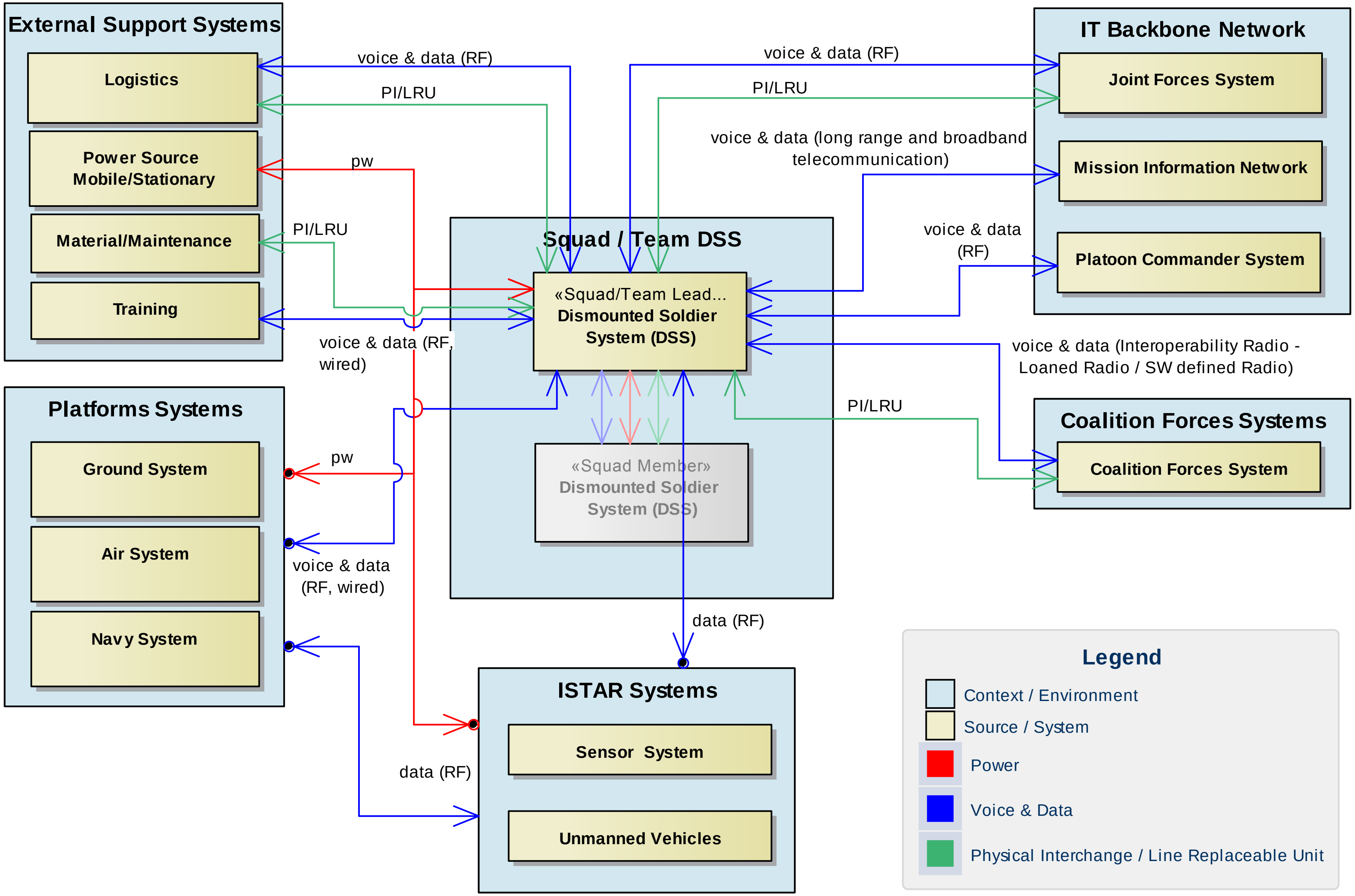


Figure 2-15 – NSV1- DSS Interface Description

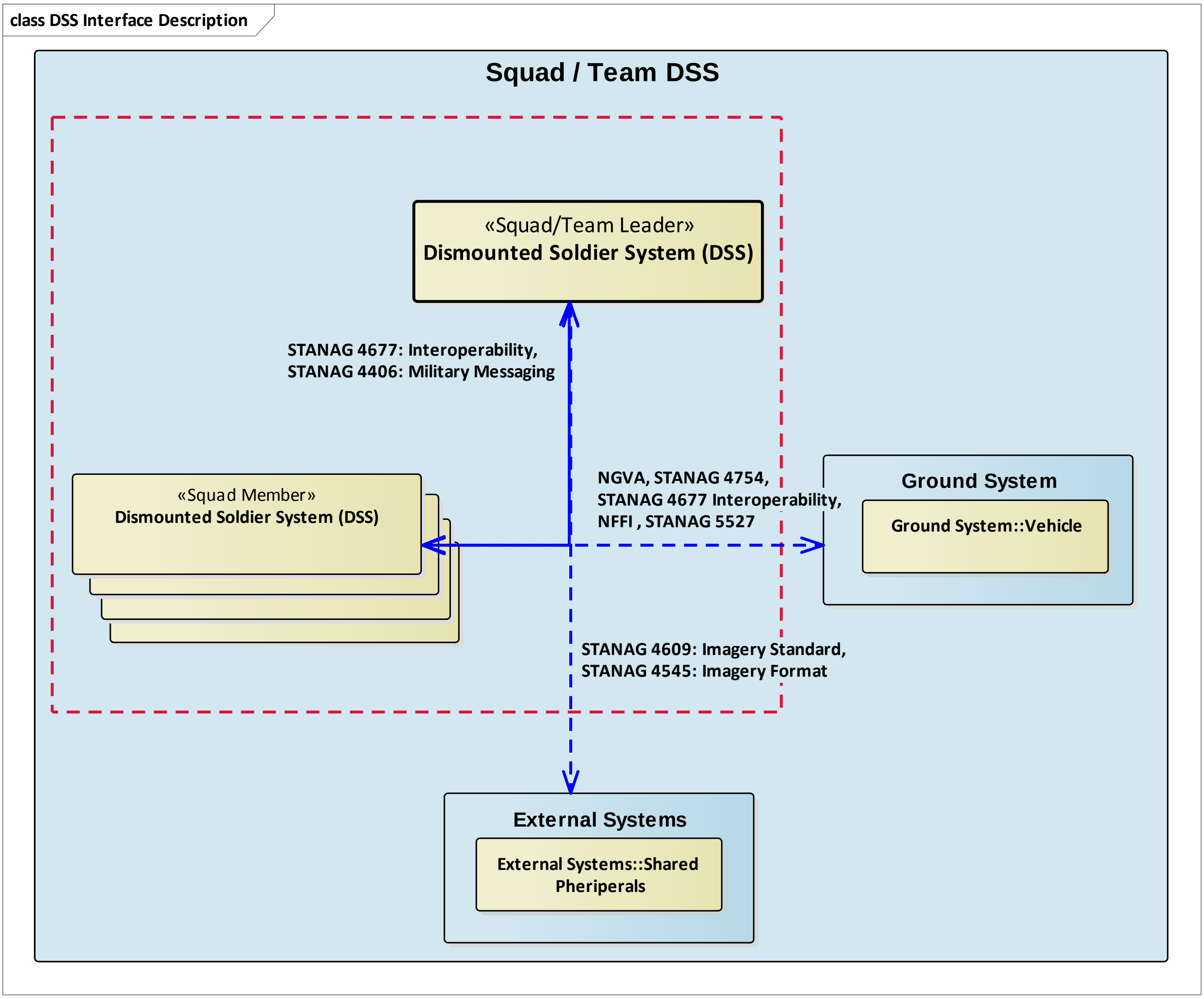

class DSS Interface Description
Squad / Team DSS
«Squad/Team Leader»
Dismounted Soldier System (DSS)
STANAG 4677: Interoperability,
STANAG 4406: Military Messaging
«Squad Member»
Dismounted Soldier System (DSS)
NGVA, STANAG 4754,
STANAG 4677 Interoperability,
NFFI , STANAG 5527
Ground System
Ground System::Vehicle
STANAG 4609: Imagery Standard,
STANAG 4545: Imagery Format
External Systems
External Systems::Shared Pheriperals

Figure 2-16 – NSV1- DSS-Squad System Interface Description

2.3.3.2 External Systems Description

2.3.3.2.1 ISTAR Systems

Sensor System

The external sensors systems provide the necessary functionalities to fulfil the ISTAR capability goal. These sensors provide information to enhance the soldier's situational awareness. The communication between a sensor and the DSS is wireless using typically a radio link.

External sensor types:

- CBRN, Acoustic Sensor, Noise detector, Image Sensor, GNSS…

The system exchanges the following information with the platforms:

- Intelligence report.
- Tactical information.
- Multimedia (image and video)
- Power using a wired connection

Unmanned Vehicles

UxV supports soldier capabilities, especially target acquisition, reconnaissance (battlefield intelligence), combat (attack capability), logistics, remote sensing, surveillance, exploration, and transport.

Unmanned Vehicles types:

- UAV, UGV, mini UAV…

The system exchanges the following information with the platforms:

- Radar information.
- Control data.
- Multimedia (image and video)
- Power using a wired connection

2.3.3.2.2 External Support Systems

Power Source Mobile / Stationary

External power supplies provide direct power to some devices and allow the system to recharge the batteries.

Material Maintenance

This category includes the Logistics Support System, which provides material, maintenance, and Line Replacement Units. An LRU is an essential item that is removed and replaced at field level to restore the item to an operational ready condition.

Training

Systems designed for realistic training that allow military exercises, for example, tactical training systems, laser duel simulator. These systems include live, virtual and constructive simulation as well as serious gaming.

Logistics

The transfer of personnel and materiel from one location to another, as well as the maintenance of that materiel, is essential for a military to be able to support an ongoing deployment or respond effectively to emergent threats. The effective solutions to military supply and logistics decision-makers, result in significant savings, improved readiness and combat support, and unit flexibility.

2.3.3.2.3 Platform Systems

The connection with any type of platform can be wired or wireless, depending on whether the DSS is in mounted or dismounted mode. The platforms are usually equipped with a C4I system that provides the capability to share information and data with the DSS. Platforms can provide a wired connection to share the information obtained by a vehicle's sensors and to exchange power with the system when the soldier is on-board. Furthermore, platforms can provide long-range radio equipment to connect with other systems and to provide access to the Mission Information Network and common radio equipment to communicate with the DSS.

The system exchanges the following information with the platforms:

- voice,
- geographical positioning,
- tactical information,
- multimedia (image and video) and
- power using the wired connection.

2.3.3.2.4 IT Backbone Network

Joint Forces System

The system must be able to exchange voice and data with joint forces without additional equipment. For this exchange, rules and standards must be established to perform direct communication of tactical information, multimedia and voice communication.

The system exchanges the following information with Joint Forces:

- voice and real-time video streaming
- tactical information, geographical positions
- multimedia (image and video),
- power, sharing the rechargeable batteries (physical interchange) and
- consumables (LRU).

Use or disclosure of data contained on this sheet is subject to restriction on the title page of this document

Mission Information Network

A Joint Network Node Network (JNN) provides the full spectrum of infrastructures and information services that allows Soldiers to interchange information on the battlefield. The Mission Network should replace the tactical communications network, which was not designed to support current and future warfighting needs.

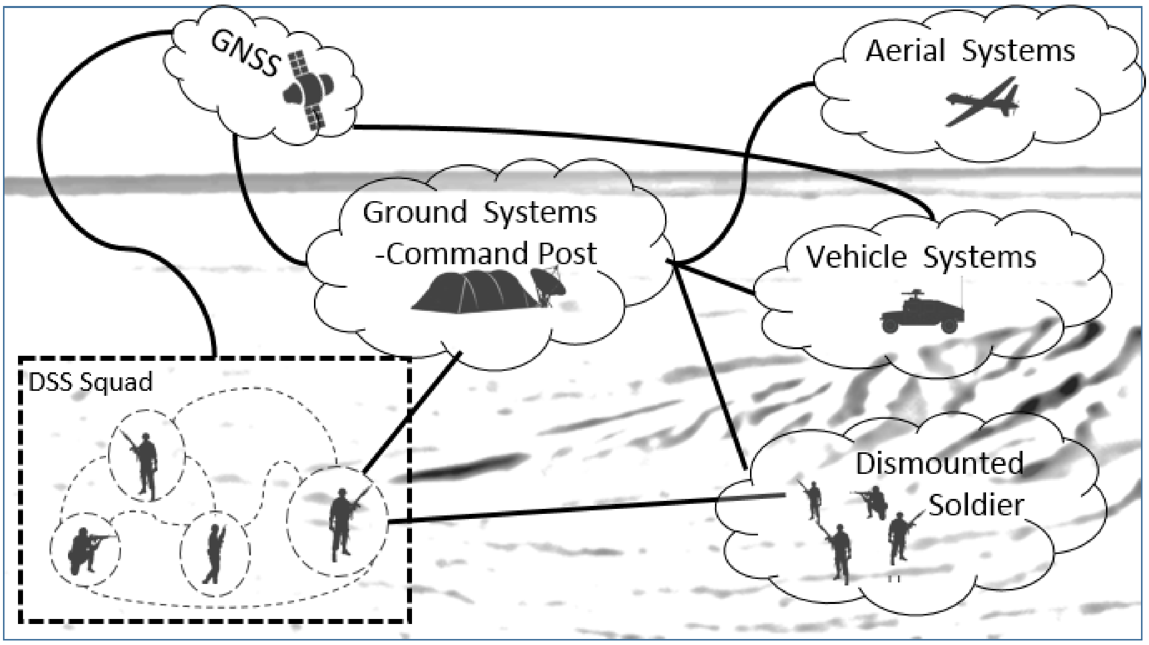


Figure 2-17 – Mission Systems operational concept

Access nodes are of various natures, such as access points in command post vehicles or long-range and broadband telecommunication via mobile satellite equipment, etc.

Mission Information Network provides voice and data communication network down to the battalion level, and the ability to deploy a network in all environments with mobile infrastructures to maintain the connectivity inside the warfare network.

Platoon Commander System

This communication provides mission plans and commander information to support the mission. The connection between the Platoon Commander System and the DSS Soldier-Squad establishes voice and data exchange via common radio frequencies.

The system exchanges the following information with the Platoon Commander System:

- voice and data,
- geographical positioning,
- tactical information,
- multimedia (image and video)
- mission plan information.

2.3.3.2.5 Coalition Forces

The Coalition units deployed in the same mission area, when organized in multi-national forces, need a common communication system. In general and according to today’s doctrine, communication between different nations is established at the company and above. However, NATO recognized a need for timely and non-aggregated data between multi-national soldier groups at the lowest echelon level. A few years ago STANAG 4677 was ratified which defines the technical aspects of establishing such a communication link at the group level. It defines a Data Model as well as an Information Exchange Mechanism which shall be used on an interoperability radio. A loan radio concept was recommended with some minimum requirements as stated in the STANAG.

The Information Exchange Mechanism (JDSSIEM) is optimized for a radio network which only connects when the soldier groups come into reach. The mechanisms, then, synchronizes all available information in order to achieve synchronized shared information set in all participating soldier groups.

The exchange protocol requires an IP protocol stack on which to operate, making it also possible to use JDSSIEM on fixed networks. The Joint Dismounted Soldier System Data Model (JDSSDM), defined in STANAG 4677, provides a set of messages which are exchanged using the JDSSIEM.

An alternative to the Loaned Radio is the usage of a common waveform. This waveform can be implemented by a traditional radio or by a Software Defined Radio (SDR) which is currently considered for v2 of the STANAG. SDR was not available at the time v1 was written. But with the NATO’s Narrowband Waveform for VHF/UHF Radios (STANAG 5630, Ratification Draft), SDR became a good alternative to the loan radio.

The system exchanges the following information with the Coalition Forces:

- voice, geographical positions,
- tactical information,
- power,
- sharing the rechargeable batteries (physical interchange)

Unique ID	Type	Requirement Description
REQ-1	**OE**	The GOSSRA compliant DSS should be divided in 4 subsystems: Torso, Head, Weapon and Supporting devices
REQ-2	**OE**	At **torso** subsystem level, a GOSSRA compliant DSS should differentiate Basic and Role Specific configurations
REQ-3	**OE**	At **torso** subsystem level, a GOSSRA compliant DSS should include a Radio, GNSS Sensor, Power Supply, Processing Unit, Push to Talk / Key Pad and a PDD (Power and Data Distribution) **for the Basic configuration**
REQ-4	**OE**	At **torso** subsystem level, a GOSSRA compliant DSS should include Navigation Aids, Small Display (Display >3.5"), Enemy Detection System, Biometric Sensors and Smartphone / WPC **for the Role Specific configuration**
REQ-5	**OE**	At **head** subsystem level, a GOSSRA compliant DSS should differentiate Basic and Role Specific configurations
REQ-6	**OE**	At **head** subsystem level, a GOSSRA compliant DSS should include a Headset and ANR(Active Noise Reduction) **for the Basic configuration**
REQ-7	**OE**	At **head** subsystem level, a GOSSRA compliant DSS should include Night Vision Goggle and Head-Mounted Display **for the Role Specific configuration**
REQ-8	**OE**	For a Basic configuration, GOSSRA does not specify any **Weapon Supporting** subsystem. At this subsystem level, just the **Role Specific** configuration is defined.
REQ-9	**OE**	At **Weapon Supporting** subsystem level, a GOSSRA compliant DSS should include Night Vision, Corner Aiming, Red Dot Sight, Range-Finder, Holographic Weapon Sight, Laser Pointer and Fire-Control System **for the Role Specific configuration**
REQ-10	**OE**	At **Supporting Devices** subsystem level, a GOSSRA compliant DSS should include Thermal Optical Devices, Monocular/Binoculars, Target Acquisition, Laser Range-Finder, Thermal Imagers, Additional power supply (fuel cell, energy harvesting…), Mine detectors, Drone jamming guns, UxV, External Link-up Modules, Long-range man pack radios and UGS.

Table 2-4 – DSS Personal Domain – Electronic Components Requirements at subsytem levels

2.4 Personal Domain

The following chapters describe the personal domain. The aim is to define an architecture with all needed detail that it can be implemented in an interoperable manner. To achieve this at least five things are necessary.

- **Connectors**, see Section 2.4.1.1.1.2.3
- **Information Exchange Mechanism**, see Section 2.4.2
- **System Bus**, see Section 2.4.2
- **Data Model**
  - Where to find, see Section 2.4.2.4.6
  - How to use, see Section 2.4.2.4
- **Agile Software / Apps**, see Section 2.4.3.1

Rationales for the used technologies and taken decisions can be found in /6/.

2.4.1 Electronic Components

2.4.1.1 Electronic Components Interface Description

In this chapter, the components that are part of the DSS are described. These groups of components are the easiest way to describe subcomponents' interactions and their interfaces.

This section provides information to ensure that the system will communicate properly with external and internal components. A complex system with multiple subcomponents needs to specify separated interfaces or separated system architectures.

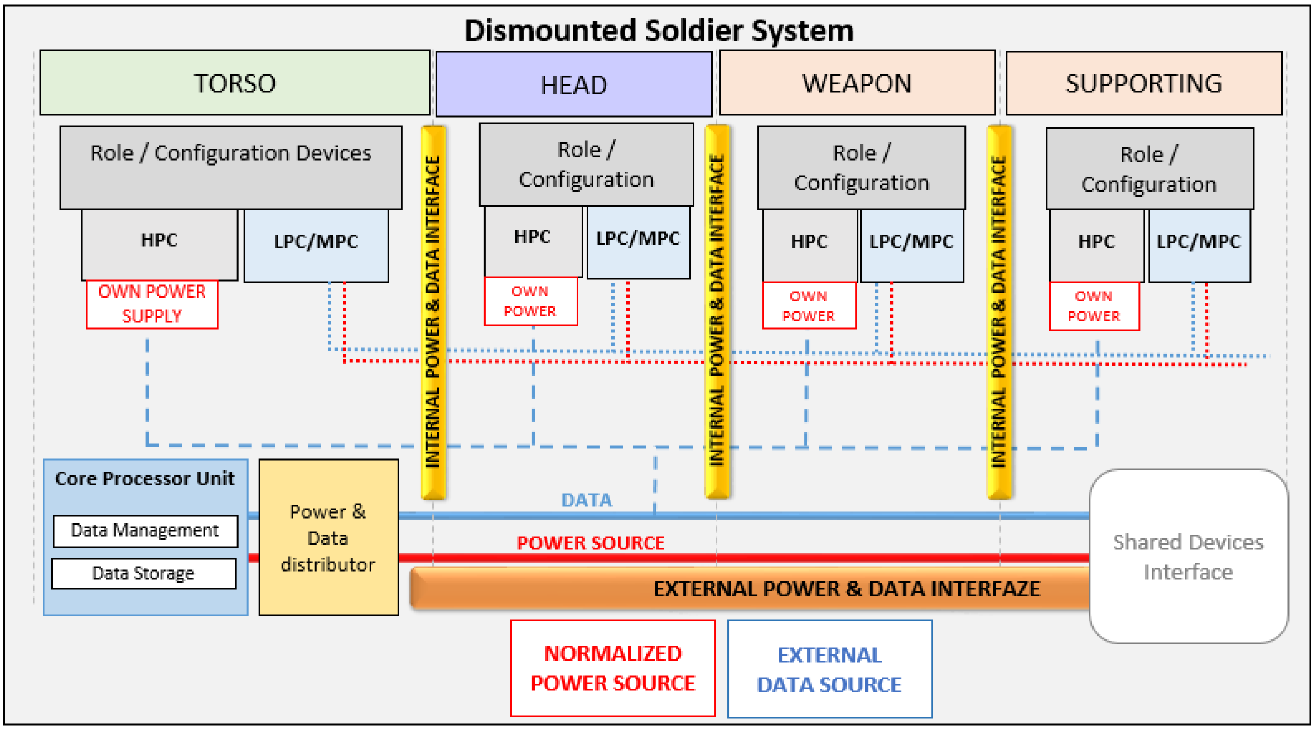


Figure 2-18 – DSS Physical Interface - Physical connection between equipment devices and external systems

The Power and Data distributor can be a more complex system with a power balance mechanism or other complex subsystems. For more detailed power and data distributor description see SDCI of the power system architecture.

To facilitate the understanding of the architecture, the interfaces are divided into two groups, internal interfaces group - for the connection of internal nodes - and external interfaces to ensure communication with external devices and sub-systems as sensors, for example.

The shared devices have an extended list of features and functionalities and require different interfaces in order to communicate the DSS with the systems or devices of this category. This category covers a huge range of devices that shall implement standard physical and logical interfaces so that they can be affordably integrated with the DSS.

2.4.1.1.1 “On-board” Systems and Data Interfaces

This chapter defines the data and power infrastructure requirements and physical interfaces for the soldier system from an internal perspective. The soldier architecture is partitioned into the Torso, Head/Helmet, Weapon and Supporting sub-systems as shown in Figure 2-19 (DSS Physical Interface).

2.4.1.1.1.1 Internal Data Interface Description

The internal system components are so intimately connected that they operate as one in relation to external conditions and other systems. The DSS is a complex system whose elements may also be regarded as a system of subsystems. Communication between these components is defined below.

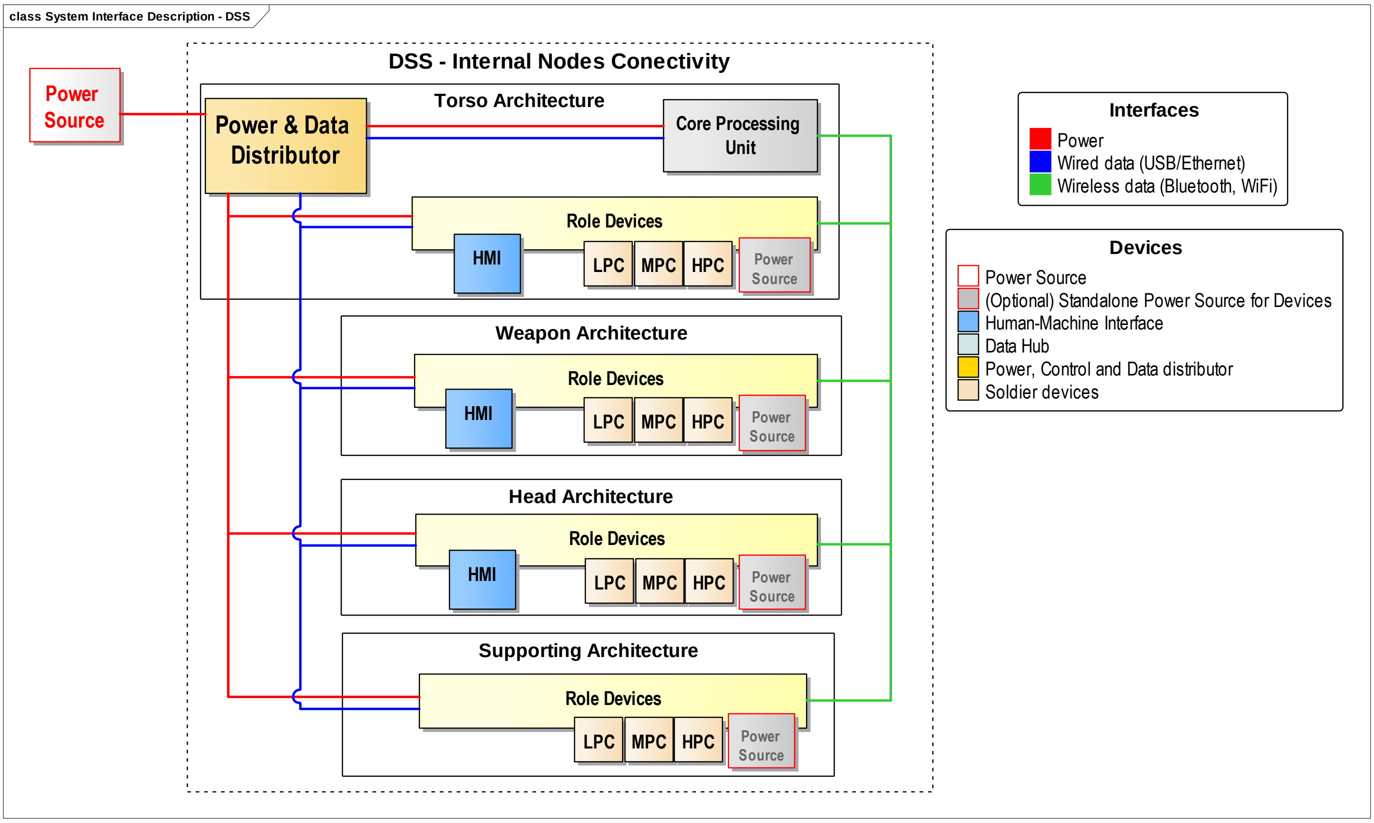


Figure 2-19 – NSV-1 System Interface Description - DSS internal nodes

Figure 2-19 represents the connection between the internal components of an individual DSS. The associations shown in the figure describe the wired and wireless connections used to ensure the communication with:

- **Role Devices**, the equipment will vary depending on the soldier's/squad's role and mission. LPC will have usually a dedicated battery and will not be connected to the power distributor, the HPC usually have a stand-alone energy supply, and the MPC Devices are powered by a common energy source.
- **Core Processing Unit** ensures data processing and allows system communication, storage, and data distribution. The Core Processing Unit is necessary to exchange basic data like positions, to support other devices' needs and to support ISTAR processes. Conceptually, it is considered as a separated system, but in reality, it may not be seen as a specific device but rather as a capability distributed over several components.
- **HMI (Human Machine Interface)** enables the soldier´s capacity to interact with the system. Some examples would be a Helmet Mounted Display (HMD), Tablets, PDA's or a Commander's Display…

The system internal nodes (sensors and devices) are divided into groups considering their power consumption, in addition, there is a module for power management to minimize the cognitive burden and facilitate the power suppliers interchange. The following table shows the description of these modules and groups:

Module	Description
Low power Consumers (LPC)	The LPC use less than 2.5 W per device (usually less than 5 Wh per day) and typically have stand-alone energy supply unless they are connected to the soldier system for data exchange. In that case, the connection can also be used for power supply.
Medium Power Consumers (MPC)	The MPC use between 2.5 and 15 W and (usually less than 50 to 150 Wh per day). These devices are connected to the soldier power system.
High Power Consumers (HPC)	The HPC uses more than 15 W per device (typically more than 200 Wh per day). The HPC usually have a stand-alone energy supply.
Power and Data distributor **(optional SDCI)**	The power distribution, control and information system of the dismounted soldier. It consists of all distribution components like cabling, but also a common energy source. It also provides data distribution.

Table 2-5 – Squad System – Power groups and components

The Data Hub provides data distribution across the torso infrastructure and to the helmet, weapon and supporting devices as required. The Data Hub is responsible for distributing data available from the DSS devices via data connectors. It shall also provide an easy mechanism to connect and disconnect the system devices.

The *basic* minimum configuration comprises a minimum set of devices and can be complemented with other components in a Role Specific configuration. The modularity not only guarantees the possibility of increasing easily the number of devices available in the system but also allows the device exchange and interchange of damaged parts for maintenance work and the inclusion of innovative devices facilitating innovation.

2.4.1.1.1.2 Cables and Connectors

The System View considers basic devices and the role-specific configurations but also devices that are shared within a squad. It defines interfaces and the information network in which different devices can be connected. For this purpose, different types of connections are identified:

- Interfaces and connectors for Power Sources (Clean & Dirty power Sources, Bulk charger, dedicated batteries...) are described below.
- Interfaces and connectors to allow the data management and data control for Low, Medium and High power consumers, following the recommendations of the previous study which focused on power.

After the data management and control needs are specified, it’s necessary to suggest the related connector standards but there is still no standard military connector for all use cases. Therefore, several characteristics and recommendations for cable and connector selection are presented next.

Unique ID	Type	Requirement Description
REQ-11	**OE**	About **Military Connectors** for DSS, the connector and its mating connector **must not allow contaminating fluids or particles to be filtered**.
REQ-12	**OE**	About **Military Connectors** for DSS, the materials that make up the connector **must not present degradation** if they are used in external environments.
REQ-13	**OE**	About **Military Connectors** for DSS, the connector must allow the **connection/disconnection** with gloves and without the need of special tools.

Table 2-6 – DSS Personal Domain – Electronic Components Common requirements for connectors

2.4.1.1.1.2.1 Features and requirements of military connectors for Soldier Systems

- **Size:** The final size of the soldier's equipment will depend on the connectors to be used in the equipment. The size of the connectors should be as small as possible to reduce the size and weight of the system.
- **Weight:** Not only the size of the connector affects the weight, but it is also desirable to reduce the number of connectors in the system, the differences in weight due to connector models can be considerable.
- **Density:** Increasing the number of pins that can contain a connector for a certain size allows to reduce the number of connectors. However, it can complicate a cabling design and cognitive burden.
- **Sealing:** The connector and its mating connector must not allow contaminating fluids or particles to be filtered.
- **Weather Resistance:** The materials that make up the connector must not present degradation if they are used in external environments.
- **Usability:** The connector must allow the connection/disconnection with gloves and without the need of special tools.
- **Frequency of use:**
  - Connections to be connected/disconnected for replacement – seldom connected/disconnected.
  - Connections to be connected/disconnected during mission – several connections/disconnections.
  - Connections to be f - quick and easy connections.
- **Mechanical factors:**
  - **Connect / Disconnect:** The connectors must allow a minimum number of connections/disconnections throughout their life cycle.
  - **Cable attachment:** Aerial connectors must be provided with internal cable fixings in order to prevent the breakage in case of pulling or degradation by use.
  - **Angled Connections:** Mechanical stress due to cable shake from the connector will eventually produce breaks and desoldering problems. To reduce this problem, the aerial connectors should allow 45 degrees angled connections.
  - **Aerial connector length:** the longer the connector’s body out of the receptacle, the higher the strain transmitted by the cable to the connection. Depending on the gap between the aerial connector and its receptacle this factor can be critical.
  - **Rotational forces:** if the connectors are of circular type, they must have mechanisms that allow rotation without disconnection to prevent internal deformations.

2.4.1.1.1.2.2 Characteristics and requirements of wiring for the Soldier Systems

Cabling is a sensitive issue for military equipment. It is important to dedicate efforts in designing a wiring structure suitable for the soldier’s comfort and resistance needs in the field. A good design minimizes entanglement and lowers connectors strain. They are very rigid and robust to resist high temperatures, corrosion by solvents/fuels or abrasions by contact with tools and environmental degradation. EMC is important especially for data as it may reduce the sensitivity (and, thus, the range) of the radio.

- **Longitudinal/transverse and rotational tensions:** Typical military wiring joins equipment inside the vehicles. In a dismounted soldier the equipment to be joined is not in a fixed position which causes tensions and deformations in the cables and reduces the life cycle of the wire.
- **Materials:** increase the wire elasticity improves the resistance of cables against vibration and use degradation.
- **Fixings:** must guarantee the ergonomic needs for the soldier.
- **Overmolding:** Overmolding of cables and connectors reduces the total cost of ownership in cable assemblies and provides strain relief for wire terminations. Thanks to this process the connector's body is shortened. Besides, it offers mechanical advantages such as mounting hardware and angled cable exits.

The field of e-textiles may provide some improvements on the performance of cables. Ergonomy can be greatly increased by seamless integration of the wiring into the garment, by means of conductive materials or inks that might be printed in the fabrics. Some of these developments are further discussed in the document Extended GOSSRA Architecture - Vol. 11 Upcoming Technologies for Soldier Systems.

2.4.1.1.1.2.3 Recommended connectors for wired connections

As already stated, it is currently not possible to find dual-sourced military connectors for all use cases. Especially the helmet and weapon sub-system will need technologies such as “break away”-connectors to connect to the torso. Nevertheless it was possible to find other connectors that can at least standardize the connectors on the torso and within the sub-systems helmet and weapon.

The following connectors are recommended, but not required since the usage of certain connectors is costumer related and upcoming customer requirements may not be possible to satisfy with these connectors. To be compatible between soldier system all signals shall be available in the soldier system, this enforces adaptability between soldier systems.

Manufacturers of peripherals for soldier systems should use the proposed connectors for common equipment. By this it is possible to adapt to all GOSSRA-compliant soldier systems by an adapter and to those who has chosen the connector natively.

In section 2.4.2 the protocol stacks and the used the system busses are specified. Below you will find the connector configuration for the relevant system busses.

For **USB 3.1 2nd Gen** different configurations are available to reduce connector size and pin count to the necessary extend. Table 2-7 and Table 2-8 show the basic pinning. The connectors include all signals that are necessary to provide USB 3.1 2nd Gen. with Power Delivery and alternative modes. Otherwise it would be possible to reduce the Pin-Count further to 9 or 10 pins, but with reduced capabilities. Currently no interoperable USB 3.1 2nd Gen. connector is available. Nevertheless it is recommend to be considered the upcoming standard Micro 38999 for these connectors and check availability before creating a target architecture.

Pin Number	Signal
1	Vbus
2	GND
3	D+
4	D-
5	SSRXp1
6	SSRXn1
7	SSTXp1
8	SSTXn1
9	CC1
10	CC2
11	SBU1
12	SBU2

Table 2-7 – Pining for USB 3.1 up to 5 Gbit/s connection

Pin Number	Signal
1	Vbus
2	GND
3	D+
4	D-
5	SSRXp1
6	SSRXn1
7	SSTXp1
8	SSTXn1
9	CC1
10	CC2
11	SBU1
12	SBU2
13	SSTXp2
14	SSTXn2
15	SSRXp2
16	SSRXn2

Table 2-8 – Pining for USB 3.1 up to 20 Gbit/s connection

For **USB 2.0**, GOSSRA follows the AEP 4695 and the AEP 4851 which defines the following pinning and connectors. AEP 4695 defines the usage side (e.g. the soldier system) and the upcoming AEP 4819 defines the charger side.

Table 2-9 the recommended pinning for USB 2.0 connectors. It is capable of handling all current use cases. Considering PIN 1 on the PAN-Function side can be optionally connected to power. By this it is possible to serve a common USB 2.0 signal using this connector.

Table 2-10 shows a list of vendors and part numbers for the connectors.

Pin #	Power Function	PAN Function
1	Power (10-20 VDC)	Power (10-20 VDC)
2	Ground - extended pin	Ground - extended pin
3	Power to energy source Positive	Power (5 VDC @ 2A Max)
4	SM Bus Data	USB +
5	SM Bus Clock	USB -
6	SM Bus ID	USB Detect

Table 2-9 – USB 2.0 connector pinning (Source:/37/ and /38/)

Vendor	ITT-Cannon[3]	Glenair	TE Connectivity
Push-Pull Plug with pins	MKJ4A6Z6-6PC-K140	8070-1676-06ZNU6-6PY	2226910-1
	MKJ4A6Z6-6EC-K140	807-309-06ZNU6-6PY	
	MKJ4A6Z6-6PY-F261	807-871-06ZNU6-6PY	
	MKJ4##Z6-6**-F261	8070-1153-##ZNU6-6**	
Push-Pull Receptacle with Sockets	MKJ4A1Z6-6SC-K140	8070-1675-01ZNU6-6SY	2226920-1
	MKJ4A1Z6-6FC-K140	807-348-01ZNU6-6SY	
	MKJ4C7Z6-6DC-F261	807-216-07ZNU6-6DY	
	MKJ4++Z6-6SC-F261	807-874-++ZNU6-6SY	
Battery (Flange) Receptacle with Sockets	MKJ4C2-155900-70		2828420-1
Battery (Flange) Receptacle with Sockets	MKJ4C2-155900-14		2828420-2
TE Rear Panel Mount Receptacle (wired assembly)			2828340-1
Glenair ## - select either Front (00) or Rear (07) chassis mounting			
ITT ##-Select either Front (C10), or Rear (C9) chassis mounting			
Glenair ** - select either PC Tail (PC) or Solder Cups (EC) for internal connection			
ITT ** - select either PC Tail (BC) or Solder Cup (EC) for internal connection			
Glenair ++ - select either Front (00), In-line [cable] (01), or Rear (07) mounting options			
ITT ++ select either front (A8), In-Line (cable) (A1), or Rear (A7) mounting options			

Table 2-10 – List of Approved Connectors by Vendor and Part Number(Based on /37/ and /38/)

[3] According to self-disclosure of the company. Matching of connectors was not tested.

Unique ID	Type	Requirement Description
REQ-14	**CR**	The DSS shall provide at least one full featured port with the signals defined in Table 2-8.
REQ-15	**OE**	The DSS should use the connectors defined in Table 2-10 for USB 2.0 within its sub-systems (Torso, Helmet, Weapon, Shared Equipment)

Table 2-11 – DSS Personal Domain - Connector Requirements

2.4.1.1.2 Power Interfaces

An overview of the interfaces within the soldier power system is shown in Figure 2-20. Here, the standards that are a starting point for the interface standards are indicated at the relevant locations.

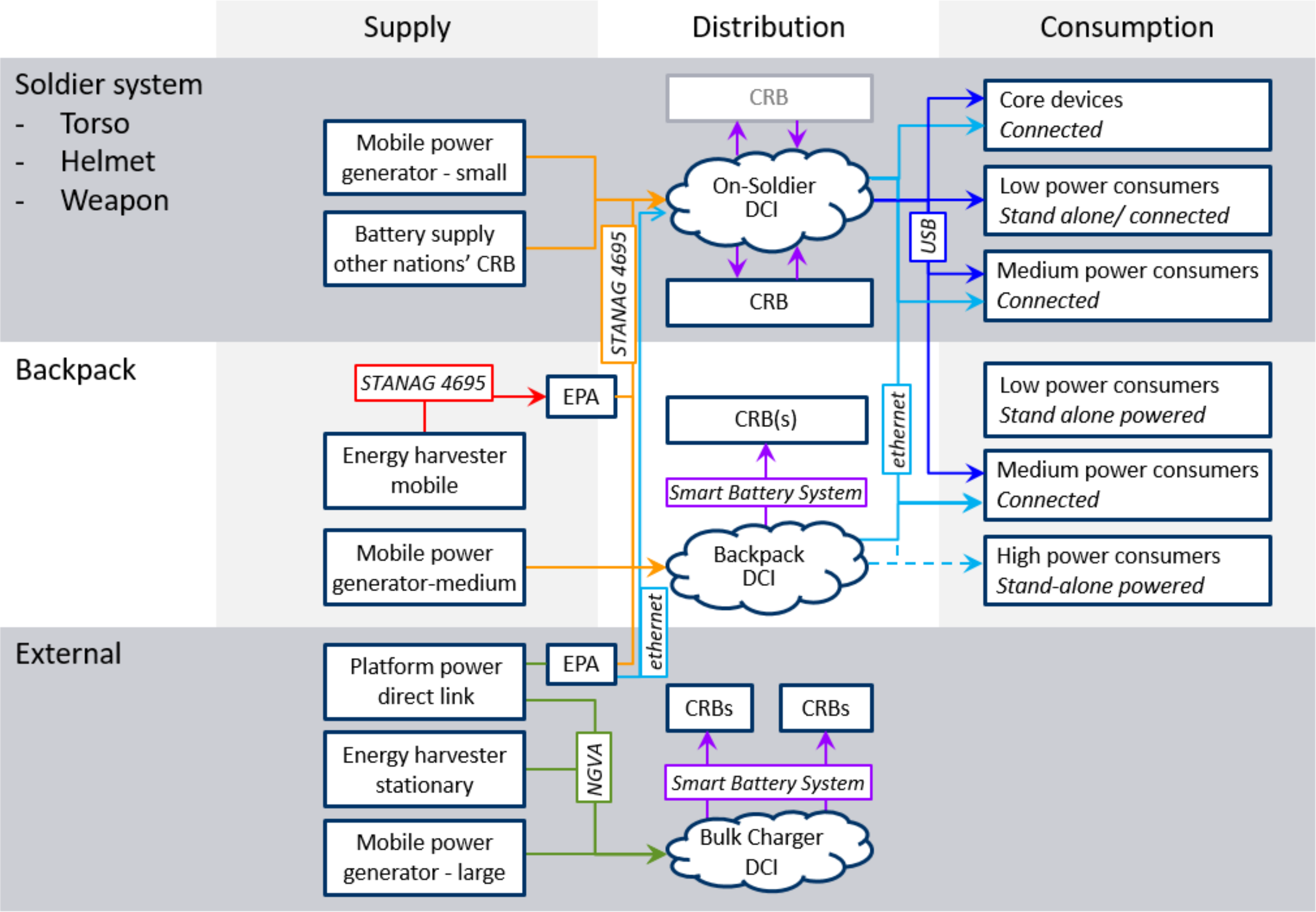

Supply
Distribution
Consumption
Soldier system
- Torso
- Helmet
- Weapon
Mobile power generator - small
Battery supply other nations' CRB
CRB
On-Soldier DCI
CRB
STANAG 4695
USB
Core devices Connected
Low power consumers Stand alone/ connected
Medium power consumers Connected
Backpack
STANAG 4695
EPA
Energy harvester mobile
Mobile power generator-medium
CRB(s)
Smart Battery System
Backpack DCI
ethernet
Low power consumers Stand alone powered
Medium power consumers Connected
High power consumers Stand-alone powered
External
Platform power direct link
EPA
Energy harvester stationary
Mobile power generator - large
NGVA
ethernet
CRBs
CRBs
Smart Battery System
Bulk Charger DCI

Figure 2-20 – The Standards used for the Interfaces in the Soldier Power System

2.4.1.2 Power Management Aspects

2.4.1.2.1 Overview

The amount of energy required by the DSS during a mission depends on several factors, which include:

- average power consumption of the components (loads) of the soldier system;
- average usage time of the components of the soldier system;
- average mission duration.

Even when the same soldier roles and mission types are considered, the above listed elements are probabilistic, and susceptible to large variations. In fact, they can vary significantly from one soldier to another even within the same unit and mission. To increase the probability that enough energy will be available to accomplish the mission, a safety margin must then be added to the list, for instance a factor of two or more, the higher the better.

The estimated amount of energy must be supplied by the energy sources carried by the soldier. But this has a direct impact on size and weight, so the lower the better.

Time must be added to the two diverging energy necessities, both in terms of how quickly the energy reserves could be depleted, and in terms of how rapidly they can be replenished.

The power management architecture of the DSS must take care of all these aspects at different stages:

- at design time, by implementing a power management strategy at system level, and not only at component level;
- at configuration time, by selecting the power sources and the power management policies that best fit the mission profile and the actual carried equipment;
- at mission time, by collecting and processing the energy parameters required to assess the energy status of the system, estimating the remaining autonomy, and suggesting, or applying, measures to extend it according to the priority of the loads with respect to mission goals.

Even if power management is often associated only with the last stage, design and configuration play a key role in making it effective and useful and are definitely part of it. Design time and configuration time power management aspects have been extensively discussed in STASS I (Soldier Power System, see /9/ and /10/). In this section more aspects relevant to the power management architecture are briefly described.

The elements of the architecture include:

- Power sources;
- Power consumers (loads);
- Power distribution network;
- Interoperability standards.

From the power management point of view, power sources should be able to provide energy related parameters like state of health, charge and function (SoH, SoC, SoF), temperature, current drain, and operating voltage. It is to be noted that this is compatible with the specifications of the SMBus most smart energy sources already comply with.

Power loads should offer remote control of operating modes (e.g. on, off, stand-by). This is compatible with USB power management capabilities. Stand-by or low-power mode (or modes, as there can be more than one) can be applied when one or more services provided by the power consumer are not required. The decreased power consumption is paid by requiring some time to restore the service, so it must be taken into account.

The power distribution network should be:

- apt to be worn by the soldier (vest, head, whatever the section), preventing hindrances and excessive or unbalanced weight, with no impact on the soldier's camouflage;
- able to manage power exchange between few sources and multiple loads;
- able to support the (relatively low bandwidth) data exchange that needs to be shared by all the elements of the power architecture;
- layered, to allow power distribution to low, medium and high power loads;
- protected against failures, including overvoltage, overcurrent and overheating;
- segmentable, to prevent the propagation of a failure to the rest of the system;

Standards are required not only for safety or environmental conditions. As stated before, power sources, loads and distribution network must be able to cooperate to form a system. This requires common interfaces relying on proven standards. As an example, standards are required for:

- connectors and wirings;
- voltage and current ranges;
- data exchange protocols;
- architecture modelling.

The USB power management system is compatible with the GOSSRA architecture and can be used as a base when deriving a target architecture.

Once all the aspects have been taken care of, a platform independent model of the power management system may become extremely simple, as shown in Figure 2-21 – Sample Power Management Model.

A graceful degradation is crucial to reduce power consumption without sacrificing important system function. This can reduce the time the soldier is carrying the soldier system as dead weight.

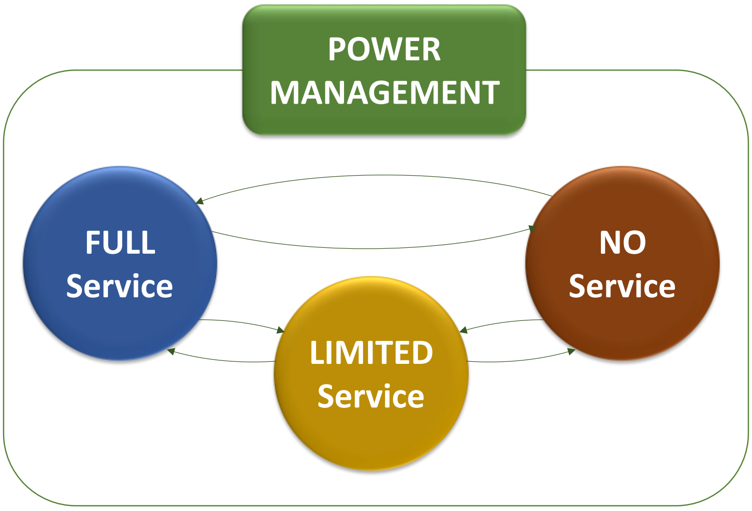


Figure 2-21 – Sample Power Management Model

To identify applicable methods for power consumption reduction it is critical to decide what are the elementary functions of the soldier systems per role.

For example:

- A simple soldier does not need a display, sharing the position is more crucial in the STU
- The STU-Leader needs some sort of display to observe the situation and receive sketches supporting command given.

This can be used for training purposes, so the user is aware of the status of the system and can decide if the reduction of services is acceptable.

It may be useful to implement an override and derive profiles that can be set by the user. By this it is possible to adapt the graceful degradation to the mission intensity. Most importantly the user gets a control on the power state and is not arguing with not working devices in stress situations which can actually reduce the acceptance of the system significantly.

2.4.1.2.2 Possible power saving measures for dismounted soldier systems

In dismounted soldier system the display, as well as the radio are traditionally the high power consumer. There are already common ways to reduce the power consumption on these two domains.

For the display for example it is possible to reduce the update rate or dim the background light. To reduce the power consumption of the radio for example the rate messages are sent can be reduced e.g. the update rate for the own position.

It is critical to reduce the efforts of the user to do power management, hence intelligent methods should be identified. Power management shall never by an additional burden to the soldier. For example it could be possible to use NFC tags in the clothing to identify that the laser range finder is hanging around the neck of the soldier or that the weapon is currently not in use (e.g. if it is standing upright). Additional sensors e.g. at the knee can help to identify movement of the soldier and adapt the rate for sharing the position more easily and precise.

Battery driven devices need additional measures for power management as they are not connected to the central rechargeable battery. As they will be mostly wireless their power modes shall be controllable via the wireless bus. Additionally new concepts should be considered to include chargeable power sources (e.g. Batteries or Capacitors) into them e.g. it could be possible to use the common connector or the pouch with wireless power transmission to recharge the devices using the CRB.

2.4.1.2.3 Possible power saving measures for mounted soldier systems

Mounted soldier systems have the advantage, that they are able to receive power from the vehicle as far as they are connected to it. This power can and should be used to load and maintaining function of the soldier system. That way it is possible to at least maintain the battery level on long transports.

Additionally the mounted information should be distributed in the system, since the information can be used by different devices to reduce service without interfering with the usability of the soldier system.

For CRB-powered components it can be used to reduce the power needed from the vehicle, as power can also be a factor in vehicles. The usage of the high- and medium-power consumers can be reduced to a minimum.

Most importantly this information can be used by all devices that are not powered by the CRB to reduce service.

For example the soldier may not use the optics of his weapons or may not need the laser range finder while mounted. This can reduce the power consumption of the devices significantly and removes the burden of switching them off from the soldier.

Unique ID	Type	Requirement Description
REQ-16	**CR**	The connectors for mounted soldiers shall serve data and power in one connector
REQ-17	**OE**	The connectors for mounted soldiers should use the signals according to section 2.4.1.1.1.2.3.

Table 2-12 – DSS Personal Domain - Mounted soldier connector requirements

2.4.2 Data Exchange Services

2.4.2.1 Data Exchange Interface Description

Figure 2-22 depicts the main components and related interconnection of the Data Exchange Services, which serve a Soldier acting in the Personal Domain.

The depicted architecture is modular, in the sense it includes both mandatory and optional (0..1) system components.

The Data Exchange Protocol is the System Component which implements the Data Exchange Services, the Data Exchange Protocol is hosted by a Computing Platform where it interacts with:

- Execution Environment, which provides services for the execution of the Data Exchange Protocol threads;
- Transport Protocol, which provides for Transport Services
- Application HMI, which requests for Data Exchange Services to exchange user data with the related Service Logic;
- Service Logic, which requests for Data Exchange Services to exchange user data with the related Application HMI;

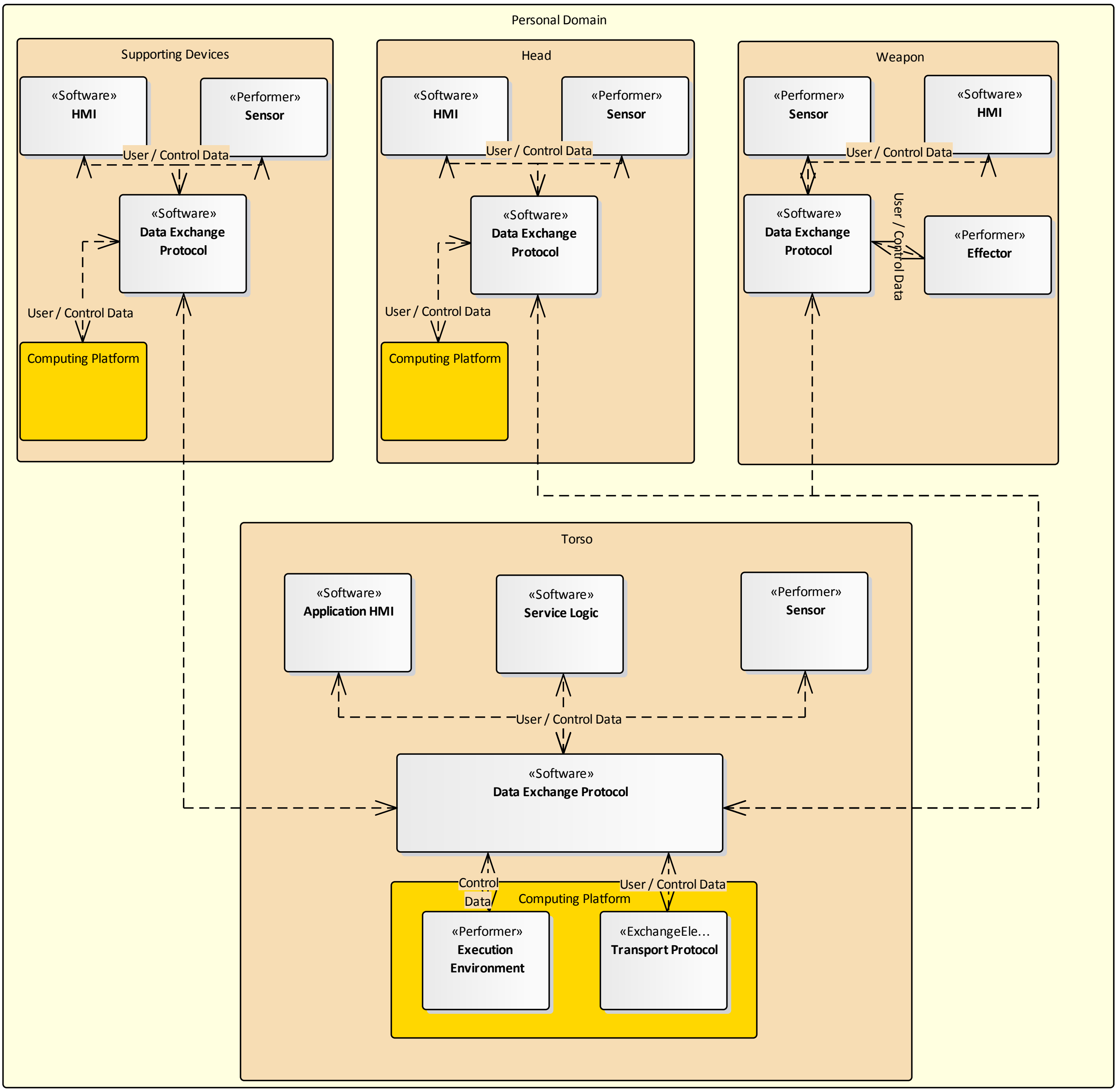


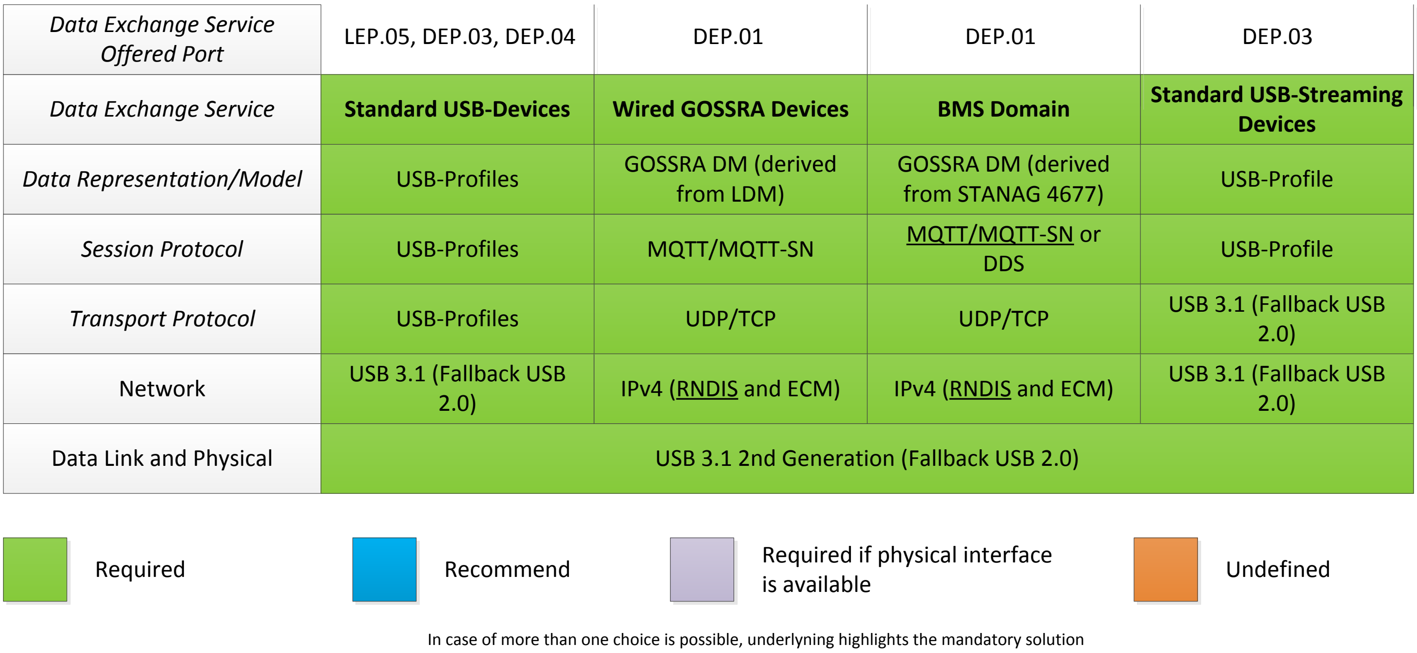
Figure 2-22 – Personal Domain – STU Commander Data Exchange Services

2.4.2.2 Data Exchange Services Port Specification

In the Dismounted Soldier Personal Domain the Data Exchange Services are implemented by the following kind of protocols:

- Date Exchange Protocols (DEP), which provides for data exchange at the session layer. They are characterised by a high abstraction level and hide network-specific details to the served application.
- Link Exchange Protocols (LEP), which provides for data exchange at the Data Link layer. They are strictly depending on the physical infrastructure and request the application to cope with specific network issues.

The following figures show the Port Specification for all data exchange services with devices and describe their protocol stack. The different colors allow to differ if the interface is required or recommend

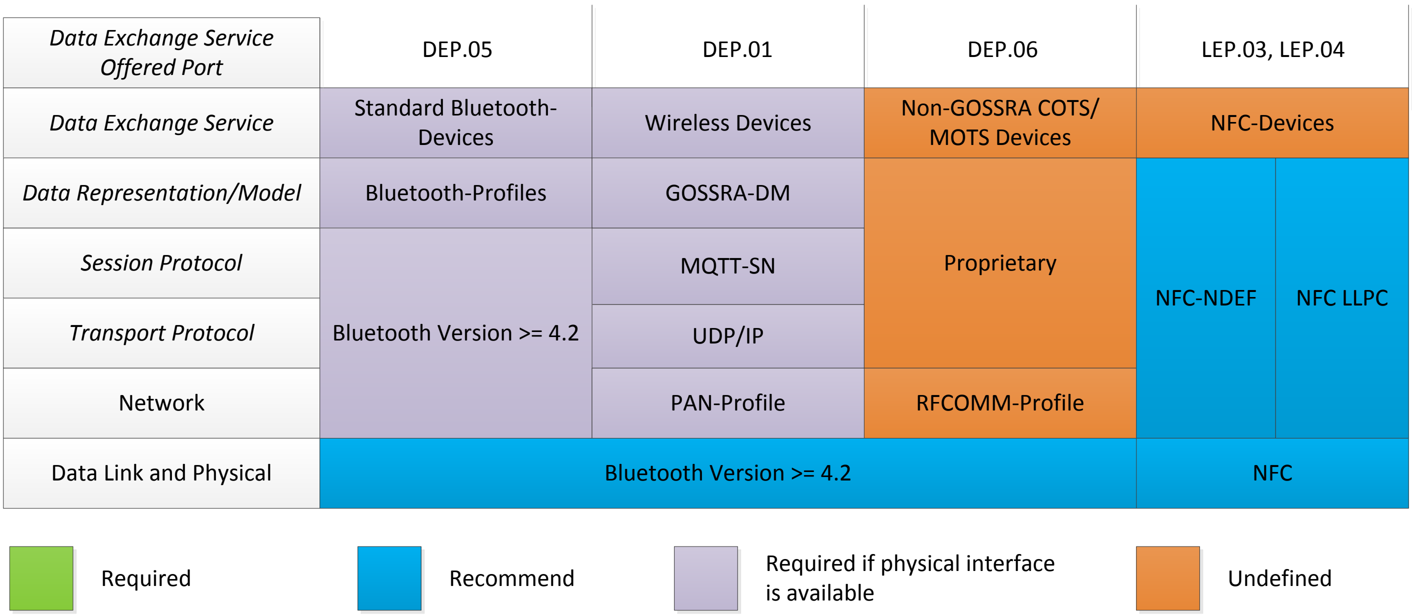


Data Exchange Service Offered Port	LEP.05, DEP.03, DEP.04	DEP.01	DEP.01	DEP.03
Data Exchange Service	**Standard USB-Devices**	**Wired GOSSRA Devices**	**BMS Domain**	**Standard USB-Streaming Devices**
Data Representation/Model	USB-Profiles	GOSSRA DM (derived from LDM)	GOSSRA DM (derived from STANAG 4677)	USB-Profile
Session Protocol	USB-Profiles	MQTT/MQTT-SN	MQTT/MQTT-SN or DDS	USB-Profile
Transport Protocol	USB-Profiles	UDP/TCP	UDP/TCP	USB 3.1 (Fallback USB 2.0)
Network	USB 3.1 (Fallback USB 2.0)	IPv4 (RNDIS and ECM)	IPv4 (RNDIS and ECM)	USB 3.1 (Fallback USB 2.0)
Data Link and Physical	USB 3.1 2nd Generation (Fallback USB 2.0)			

🟩	Required	🟦	Recommend	🟪	Required if physical interface is available	🟧	Undefined

In case of more than one choice is possible, underlyning highlights the mandatory solution

Figure 2-23 – Data Exchange Service Port Specification for wired devices



Data Exchange Service Offered Port	DEP.05	DEP.01	DEP.06	LEP.03, LEP.04	
Data Exchange Service	Standard Bluetooth-Devices	Wireless Devices	Non-GOSSRA COTS/ MOTS Devices	NFC-Devices	
Data Representation/Model	Bluetooth-Profiles	GOSSRA-DM	Proprietary	NFC-NDEF	NFC LLPC
Session Protocol	Bluetooth Version >= 4.2	MQTT-SN			
Transport Protocol		UDP/IP			
Network		PAN-Profile	RFCOMM-Profile		
Data Link and Physical	Bluetooth Version >= 4.2			NFC	

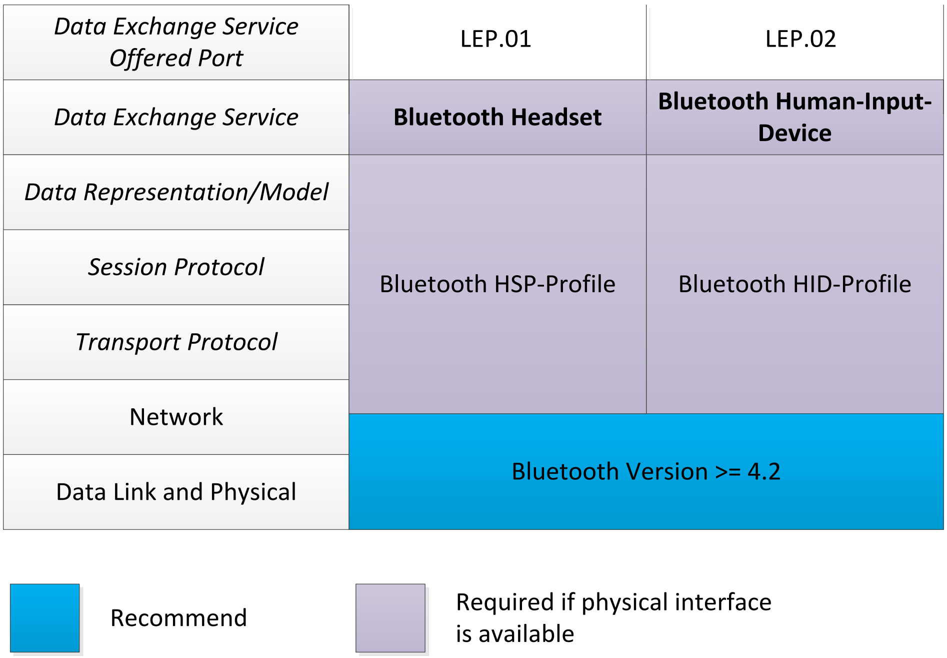
🟩 Required

🟦 Recommend

🟪 Required if physical interface is available

🟧 Undefined

Figure 2-24 – Data Exchange Service Port Specification for wireless devices



Data Exchange Service Offered Port	LEP.01	LEP.02
Data Exchange Service	**Bluetooth Headset**	**Bluetooth Human-Input-Device**
Data Representation/Model	Bluetooth HSP-Profile	Bluetooth HID-Profile
Session Protocol		
Transport Protocol		
Network	Bluetooth Version >= 4.2	
Data Link and Physical		

🟦 Recommend

🟪 Required if physical interface is available

Figure 2-25 – Data Exchange Service Port Specification for special wireless devices

2.4.2.2.1.1 Data Exchange Protocols

Session Exchange Protocols provide the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Personal Domain;
- Required Port, which requests services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the Personal Domain are:

- Offered Ports:
  - DEP.01: Personal Data Services, which provides services for exchanging data among the DSS Components, e.g. sensors, smart display, soldier application(s).
  - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio.
- Required Ports:
  - DEP.03: **Wired Transport Services: USB Generic Profile**, which requests for the transport of data/streaming among the wired personal area network endpoints based on a generic USB profile, as depicted in Figure 2-26.
  - DEP.04: **Wired Transport Services: USB CDC Profile**, which requests for the transport of data/streaming among the wired personal area network endpoints based on the USB Communication Device Class (CDC) Profile, as depicted in Figure 2-26;
  - DEP.05: **Wireless Transport Services: Bluetooth Generic Profile**, which requests for the transport of data/streaming among the wireless personal area network endpoints based on the Bluetooth Generic Profile, as depicted in Figure 2-26;
  - DEP.06: **Wireless Transport Services: Bluetooth RFCOMM Profile**, which requests for the transport of data/streaming among the wireless personal area network endpoints based on the Bluetooth RFCOMM Profile, as depicted in Figure 2-26;
  - DEP.07: **Execution Platform API**, which requests for services supporting the execution of the SEP threads.

Each Offered Port is supported by an appropriated protocol stack as described below:

- DEP.01 provides the API for Personal Data Services based on the protocol stack depicted in Figure 2-26. The following protocols are a candidate to implement the Data Session Protocol for DEP in the Personal Domain:
    - Data Distribution Services for Real-Time Systems[/20/, /21/, /22/,/23/]
    - MQTT for Sensor Network (MQTT-SN) [/29/]

  For IP-over-USB Remote Network Driver Interface Specification (RNDIS) shall be used. It is possible to use the standard USB-Profile Ethernet Control Model (ECM) for compatibility issues. In this cases the resulting emulated IP-Networks shall be merged and traffic shall be routed between them.
- DEP.02 provides the API for Streaming Data Services based on the protocol stack depicted in Figure 2-27. Next, the recommendation to implement the Streaming Session Protocol for DEP in the Personal Domain:
    - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]

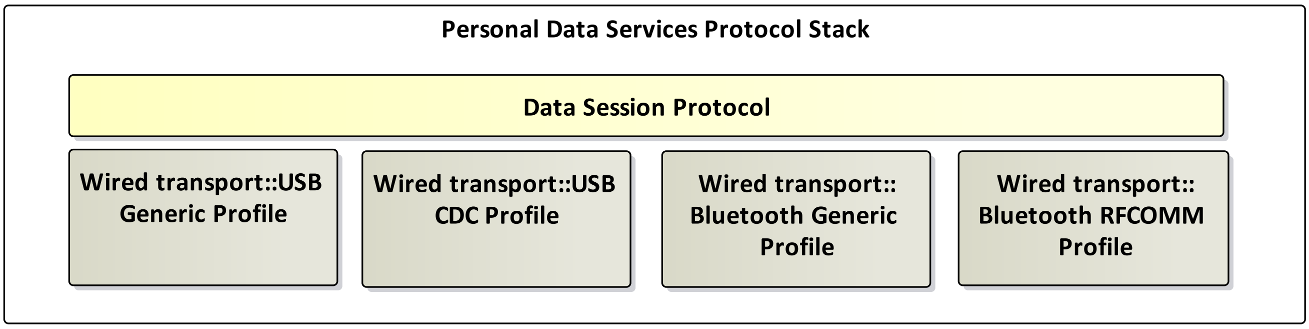

Personal Data Services Protocol Stack
Data Session Protocol
Wired transport::USB Generic Profile
Wired transport::USB CDC Profile
Wired transport:: Bluetooth Generic Profile
Wired transport:: Bluetooth RFCOMM Profile

Figure 2-26 – NSV-2a Personal Data Services Protocol Stack

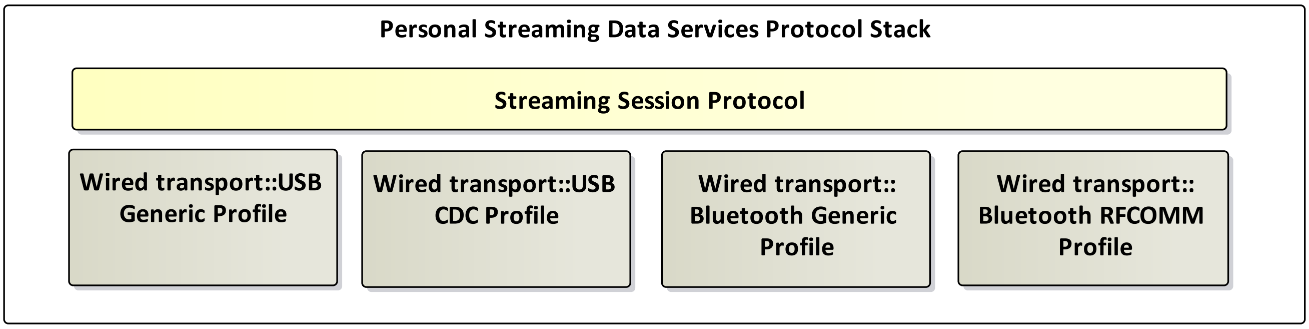

Personal Streaming Data Services Protocol Stack
Streaming Session Protocol
Wired transport::USB Generic Profile
Wired transport::USB CDC Profile
Wired transport:: Bluetooth Generic Profile
Wired transport:: Bluetooth RFCOMM Profile

Figure 2-27 – NSV-2a Streaming Data Services Protocol Stack

2.4.2.2.1.2 Link Exchange Protocols

Link Exchange Protocols provide the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Personal Domain;

The set of logical ports in the Personal Domain are:

- Offered Ports:
  - LEP.01: **Wireless Link Services: Bluetooth HID Profile**, which provides services for exchanging data with the human interface devices. It provides the protocol stack as depicted in Figure 2-28.
  - LEP.02: **Wireless Link Services: Bluetooth HSP Profile**, which provides services for exchanging data with the Headset devices. It provides the protocol stack as depicted in Figure 2-28;
  - LEP.03: **Wireless Link Services: NFC NDEF Profile**, which provides services for exchanging data with the devices supporting the NFC Data Exchange Format (NDEF), as depicted in Figure 2-28;
  - LEP.04: **Wireless Link Services: NFC LLPC Profile**, which provides services for exchanging data with the devices supporting the NFC Logical Link Control Protocol (LLCP), as depicted in Figure 2-28;
  - LEP.04: **Wired Link Services: USB Native**, which provides services for exchanging data with the devices supporting the USB protocol, as depicted in Figure 2-28.

Each Offered Port is supported by its own specific protocol stack, which is invoked by the Application for Data Exchange Services, see Figure 2-28 below.

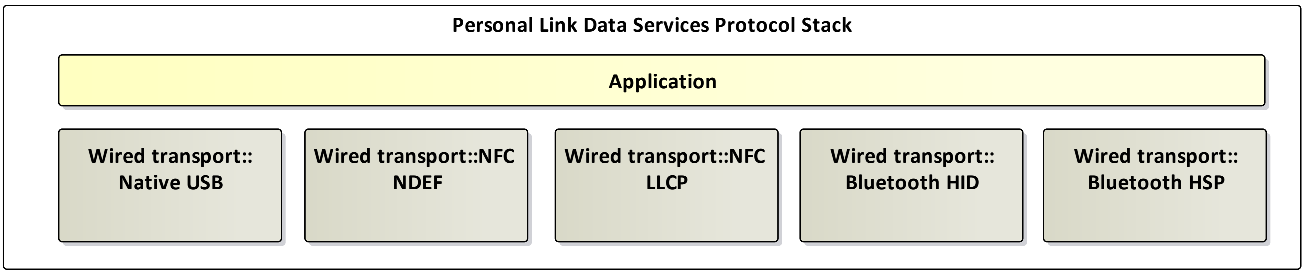

Personal Link Data Services Protocol Stack
Application
Wired transport:: Native USB
Wired transport::NFC NDEF
Wired transport::NFC LLCP
Wired transport:: Bluetooth HID
Wired transport:: Bluetooth HSP

Figure 2-28 – NSV-2a Link Data Services Protocol Stack

2.4.2.3 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component which is serving a DSS node that acts in the Personal Domain exchange data with other DSS system components as specified below.

The Data Exchange Protocol component provides services to STU Commander Application and embedded devices via the following logical ports:

- DEP.01, which interconnects with:
    - The STU Commander HMI Application to:
        - Send / Receive User Data and Service Control Data
    - The STU Commander Application Service Logic to:
        - Send / Receive User Data and Service Control Data
    - The STU Commander Device Service Logic to:
        - Send / Receive User Data and Service Control Data
- DEP.02, which interconnects with:
    - The STU Commander HMI Application to:
        - Send Streaming Data
        - Send / Receive Service Control Data
    - The Soldier Application Service Logic to:
        - Send Streaming Data and Service Control
        - Send / Receive Service Control Data
    - The DSS Embedded Device Service Logic to:
        - Receive Streaming Data
        - Send / Receive Service Control Data

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.03, which interconnects with “Wired Transport Services: USB Generic Profile” to Send / Receive User Data, Streaming Data and Service Control Data.
- DEP.04, which interconnects with “Wired Transport Services: USB CDC Profile” to Send / Receive User Data, Streaming Data and Service Control among the wired personal area network endpoints based on the USB Communication Device Class (CDC) Profile.
- DEP.05: which interconnects with “Wireless Transport Services: Bluetooth Generic Profile” to Send / Receive User Data, Streaming Data and Service Control among the wireless personal area network endpoints based on the Bluetooth Generic Profile;
- DEP.06: which interconnects with “Wireless Transport Services: Bluetooth RFCOMM Profile”, to Send / Receive User Data, Streaming Data and Service Control among the wireless personal area network endpoints based on the Bluetooth RFCOMM Profile;
- DEP.07, which interconnects with “Execution Environment API”, to Send / Receive Service Control Data.

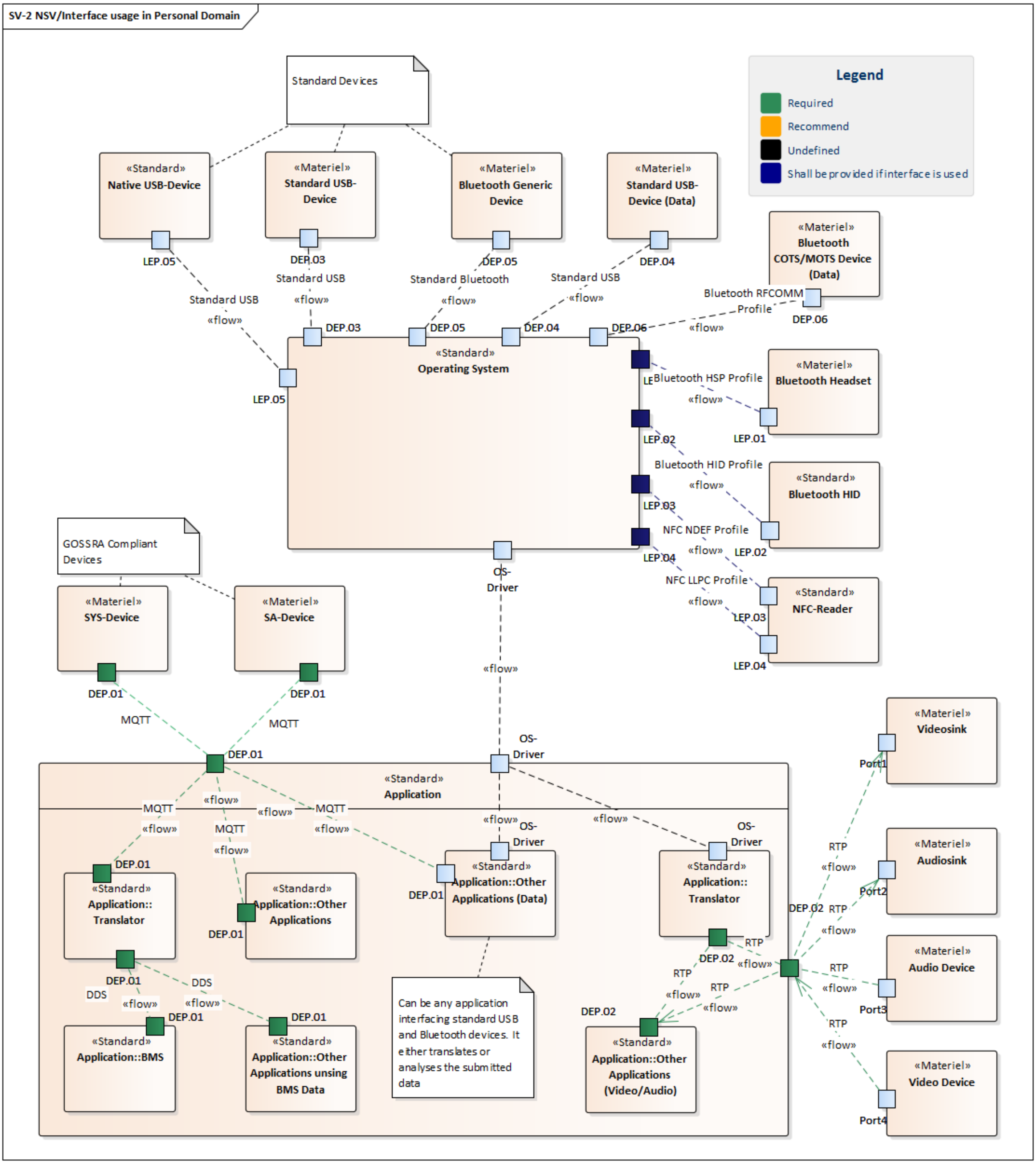

SV-2 NSV/Interface usage in Personal Domain
Standard Devices
Legend
🟩 Required
🟧 Recommend
⬛ Undefined
🟦 Shall be provided if interface is used
«Standard» Native USB-Device
«Materiel» Standard USB-Device
«Materiel» Bluetooth Generic Device
«Materiel» Standard USB-Device (Data)
«Materiel» Bluetooth COTS/MOTS Device (Data)
LEP.05
DEP.03
Standard USB
DEP.05
Standard Bluetooth
Standard USB
DEP.04
Standard USB
«flow»
Bluetooth RFCOMM Profile
DEP.06
DEP.03
DEP.05
DEP.04
DEP.06
«Standard» Operating System
LEP.05
«Materiel» Bluetooth Headset
Bluetooth HSP Profile
LEP.01
LEP.02
Bluetooth HID Profile
«Standard» Bluetooth HID
LEP.03
NFC NDEF Profile
LEP.02
LEP.04
NFC LLPC Profile
«Standard» NFC-Reader
LEP.03
LEP.04
OS-Driver
GOSSRA Compliant Devices
«Materiel» SYS-Device
«Materiel» SA-Device
DEP.01
DEP.01
MQTT
MQTT
DEP.01
OS-Driver
«Standard» Application
MQTT
MQTT
MQTT
OS-Driver
OS-Driver
«Materiel» Videosink
Port1
«Materiel» Audiosink
Port2
«Materiel» Audio Device
Port3
«Materiel» Video Device
Port4
RTP
DEP.01
«Standard» Application:: Translator
«Standard» Application::Other Applications
DEP.01
«Standard» Application::Other Applications (Data)
DEP.01
«Standard» Application:: Translator
DEP.02
RTP
DEP.01
DDS
DDS
DEP.01
DEP.01
«Standard» Application::BMS
«Standard» Application::Other Applications unsing BMS Data
Can be any application interfacing standard USB and Bluetooth devices. It either translates or analyses the submitted data
DEP.02
«Standard» Application::Other Applications (Video/Audio)
«flow»

Figure 2-29 – System to System Port Connectivity Data Exchange Service

2.4.2.4 Data model

Although the agreed protocol for sensory network's data exchange has already been specified (MQTT), to achieve a full compatibility, it is necessary to agree a data model. This way, i.e. if three different manufacturers develop three different GOSSRA compliant devices, any GOSSRA compliant DSS will be able to use them without further integration effort.

To define the data presentation on the data exchange service layer it is important to map the data model and thus the data representation on the given data exchanges to make full use of the introduced middleware.

2.4.2.4.1 GOSSRA Data Model Rationale

2.4.2.4.1.1 GOSSRA Data Model Concepts

The GOSSRA Data Model (GDM) aims to model the standard GOSSRA Concepts, i.e. Rules, Information Elements (IE), Functions, and Services.

GDM is organized in Domains; each domain models a specific GOSSRA concept.

Examples of domains are:

- A system resource, such as a video camera, laser range finder, radio equipment;
- A system service, such as Resource Registration Service;
- A system function, such as power management, land combat operations support.

The GDM is specified in a formal design language, e.g. UML, in order to provide a Platform Independent Model (PIM) of the GOSSRA Concepts, in terms of data, operations, events, interactions.

Starting from the PIM model it is possible to achieve a Platform Specific Model (PSM) which allows for the implementation of the GOSSRA Concepts for a specific execution platform adopted by a target GOSSRA system.

An automatic translation from the PIM to PSM greatly increases the GDM advantages and exploitation.

A Domain module is the implementation of the Domain Specification for a given execution platform. The set of Domain modules build the GOSSRA Domain Layer, which provides for a standard access to the GOSSRA services, which are strictly related to the GOSSRA concepts, e.g. Resources, System Services, System Functions.

As depicted in the Figure 2-30, a GOSSRA Application typically is based on one or more GOSSRA Services offered by the GOSSRA Domain Layer.

The GOSSRA Infrastructure provides for basic services such as data exchange, repository, Operating System.

The Data Model improves key GOSSRA system quality factors such as interoperability and agility.

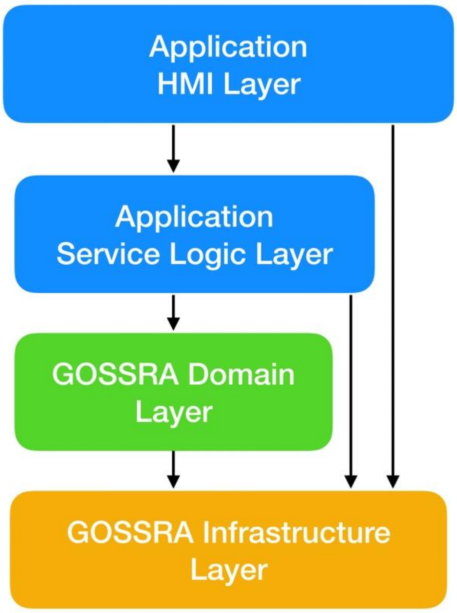


Figure 2-30 – GOSSRA Application Layered Architecture

2.4.2.4.1.2 How Data Model improves Interoperability

Interoperability among the GOSSRA Application Components can act on different levels. Starting from the more basic level they are:

- Binary Level, which guarantees that interacting SW Components adopt a compatible interpretation of the binary packet exchanged.
- Syntactic Level, which guarantees that interacting SW Components adopt a compatible interpretation of the syntax of the data structure translated by the binary packet exchanged;
- Semantic Level, which guarantees that interacting SW Components adopt a compatible interpretation of the semantic of the data represented by a given syntax.
- Procedural Level, which guarantees that interacting SW Components adopt compatible behaviours during the exchange of IEs implementing a standard GOSSRA procedure.

The GOSSRA Infrastructure provides for Binary Level interoperability.

The GOSSRA Data Model provides for:

- Syntactic Level interoperability, due to the specification of a standard data syntax for each IE;
- Semantic Level interoperability, due to the specification of standard naming rules for each kind of IE. Semantic interoperability is further improved by the adoption of DDS as Data Exchange Services protocol, due to its concepts of Topic Name, which adds a semantic value to Data Syntax.
- Procedural Level interoperability, due to the specification of standard GOSSRA Procedures, e.g. via Use case and Sequence Diagrams. It is worth noting that this procedures acts at Application Layer and implements Standard GOSSRA Rules, e.g. object creation, or Services, e.g. Resource Registration.

In conclusion, the GOSSRA Data Model guarantees that interaction Application components is able to correctly exchange a given sequence of IEs, and deal with each IE by assigning compatible syntax and semantic to each elements the IE is composed by.

It is worth noting that, these degrees of interoperability is independent of any specific agreement among the SW Component manufacturers, e.g. Interface Specification Requirements, and directly stems from the standardization process of the GOSSRA Data Model.

2.4.2.4.1.3 How Data Model improves Agility

System agility is the capability of a system to adapt to changing environmental conditions, which include both changing Operational scenarios, and evolution of the Operational needs.

The organization in Domains of the Data Model implements a separation of concerns so allowing for each GOSSRA Concept to evolve independently from the others. It is worth noting that the more focused a given Domain is, the more the system agility, due to a finer granularity of needed changes to adapt to new conditions.

Each Domain is characterized by a bounded context, which standardizes both provided and offered services, so hiding all of the implementation details of the Domain.

The Domains are loosely coupled, they interact via the GOSSRA Data Exchange services, i.e. using message-oriented protocols, whose messages transfer the IE specified by the Data Model of the interacting Domains.

The loose coupling among Domains allows for both evolvability, i.e. agility of the GOSSRA system to adapt to new operational needs evolving only the set of Domains which specifically address those needs, and configurability, i.e. the agility of a GOSSRA system to select the set of Resources, System Services, and System Functions which specifically satisfy the needs of a given mission.

Evolvability is further improved by the adoption of DDS as Data Exchange Protocols, due to its Extensible Types feature, which specifies the rules to deals with different versions of the same data structure (Topic), so allowing Application Components, which adopt different version of the same Domain to maintain the semantic interoperability without any change of their codebases.

2.4.2.4.2 System and Situational Awareness data model

The System and Situational Awareness data model was derived from the LDM using the GVA-Translator-Toolchain and an IDL to XSD converter. It is focused on a components and functions of them. Figure 2-31 show the packages provided by the data model.

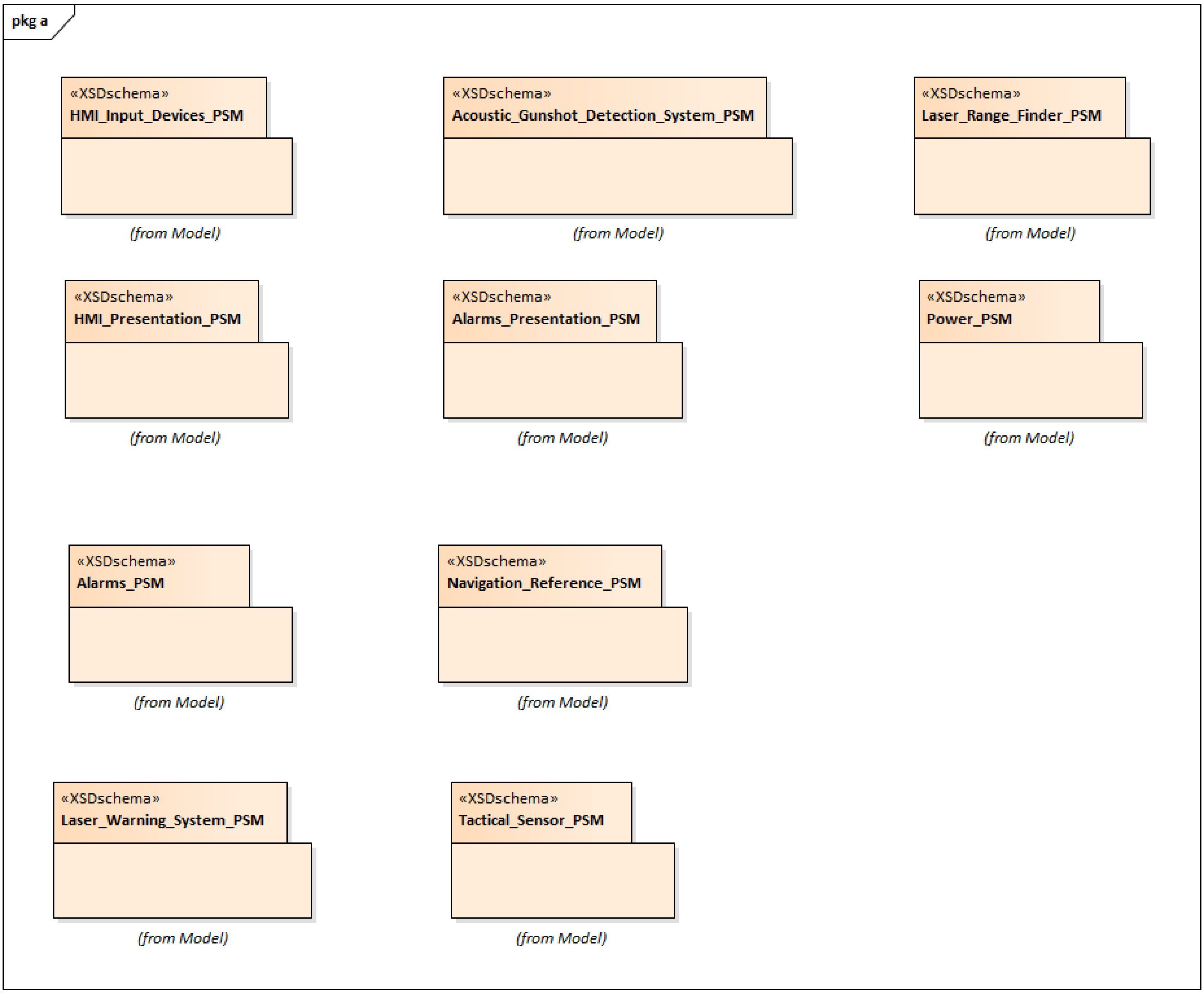


Figure 2-31 – System and Situational Awareness data model basis diagram

2.4.2.4.3 C4I data model

The C4I data model differs from the data model for the System and Situational Awareness domain. While the latter is focused on components, the C4I DM is focused on instances and objects. The GOSSRA C4I DM is deviated from the JDSSDM (see /19/).

Figure 2-32 shows the basis of the C4I Data model. The “GOSSRAMessageType” provides, as for the System and Situational Awareness DM, a “sourceID” with instance and resource id as well as a “datetime” attribute and links to certain information types of the JDSSDM.

Since the domain of the DM is more focused in objects it does not serve the message classification in status, specification and command.

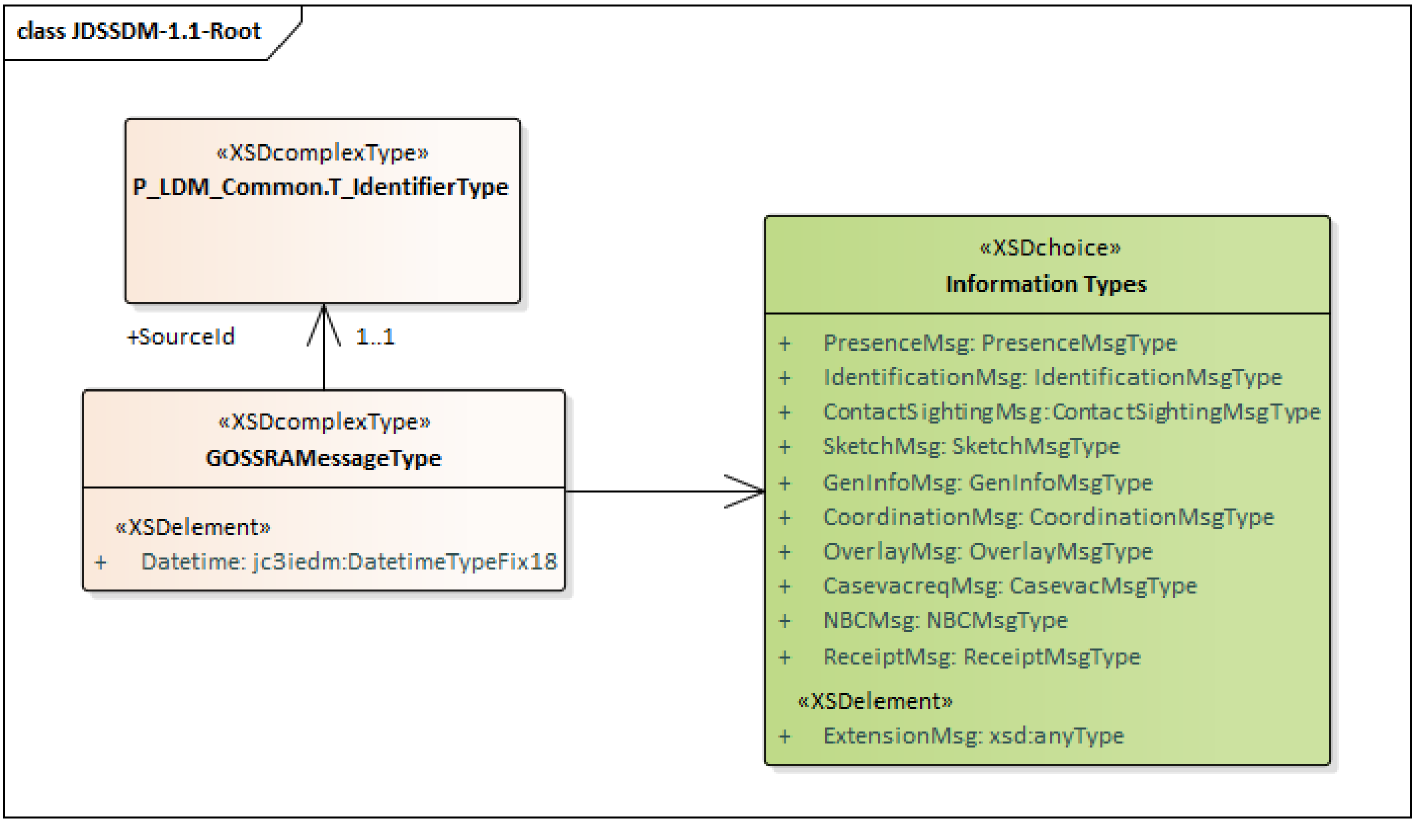

class JDSSDM-1.1-Root
«XSDcomplexType»
P_LDM_Common.T_IdentifierType
+SourceId
1..1
«XSDcomplexType»
GOSSRAMessageType
«XSDelement»
+ Datetime: jc3iedm:DatetimeTypeFix18
«XSDchoice»
Information Types
+ PresenceMsg: PresenceMsgType
+ IdentificationMsg: IdentificationMsgType
+ ContactSightingMsg:ContactSightingMsgType
+ SketchMsg: SketchMsgType
+ GenInfoMsg: GenInfoMsgType
+ CoordinationMsg: CoordinationMsgType
+ OverlayMsg: OverlayMsgType
+ CasevacreqMsg: CasevacMsgType
+ NBCMsg: NBCMsgType
+ ReceiptMsg: ReceiptMsgType
«XSDelement»
+ ExtensionMsg: xsd:anyType

Figure 2-32 – C4I data model basis diagram

2.4.2.4.4 Information Tagging

The all data models will be used with MQTT. To make full use of the features of MQTT it is necessary to use parts of the data model in the topic names.

The System and situational awareness data model differs the information types:

- **Specifications** → Used to show that a component or function is available and is provided at the start of the component. It usually describes values that will not change during runtime. They can be identified by the suffix "_specification".
- **Commands** → used to command actions on a certain component or function (e.g. triggering a measurement). They can be identified by the two elements A_recipientID and A_sourceID)
- **Status** → Is used to show the current status of a component, function or new information (e.g. the lock/unlock status of an LRF or a measurement result). They can be identified, since they are no specifications or commands and only provide a source id, but no recipient id.

The **C4I Data model** has only the status type that describes the status of an object.

The **basic topic name** for each information type will be generated in the following manner:

Packetname/Topicname/sourceResourceID/sourceInstanceID

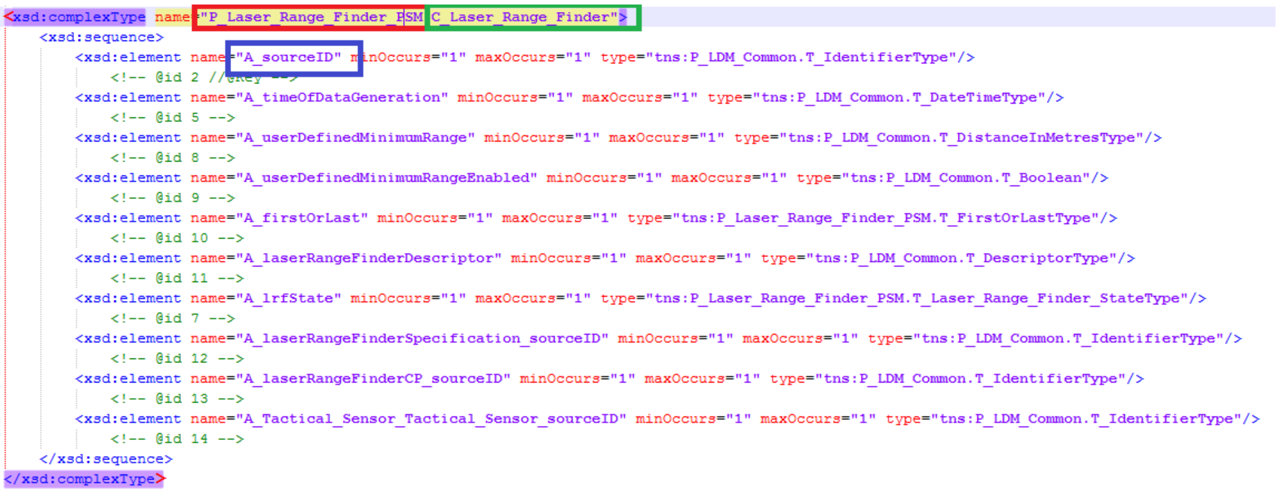
Both, resource and instance id, are derived from the A_sourceID attribute. By this naming convention it is possible to filter Information on MQTT level by using wildcards.

The **command topics** are enhanced by resource and instance id of the recipient. So the actual topic name will have the following pattern.

Packetname/Topicname/sourceResourceID/sourceInstanceID/recipientResourceID/recipientInstanceID

The following examples will further explain the naming conventions.

The following structure shall be given for the System and Situational Awareness data model.



```
<xsd:complexType name="P_Laser_Range_Finder_PSM C_Laser_Range_Finder">
    <xsd:sequence>
        <xsd:element name="A_sourceID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 2 //@key -->
        <xsd:element name="A_timeOfDataGeneration" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_DateTimeType"/>
            <!-- @id 5 -->
        <xsd:element name="A_userDefinedMinimumRange" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_DistanceInMetresType"/>
            <!-- @id 8 -->
        <xsd:element name="A_userDefinedMinimumRangeEnabled" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_Boolean"/>
            <!-- @id 9 -->
        <xsd:element name="A_firstOrLast" minOccurs="1" maxOccurs="1" type="tns:P_Laser_Range_Finder_PSM.T_FirstOrLastType"/>
            <!-- @id 10 -->
        <xsd:element name="A_laserRangeFinderDescriptor" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_DescriptorType"/>
            <!-- @id 11 -->
        <xsd:element name="A_lrfState" minOccurs="1" maxOccurs="1" type="tns:P_Laser_Range_Finder_PSM.T_Laser_Range_Finder_StateType"/>
            <!-- @id 7 -->
        <xsd:element name="A_laserRangeFinderSpecification_sourceID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 12 -->
        <xsd:element name="A_laserRangeFinderCP_sourceID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 13 -->
        <xsd:element name="A_Tactical_Sensor_Tactical_Sensor_sourceID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 14 -->
    </xsd:sequence>
</xsd:complexType>
```

Figure 2-33 – Example status information data structure for system and situational awareness DM

The color scheme is as following

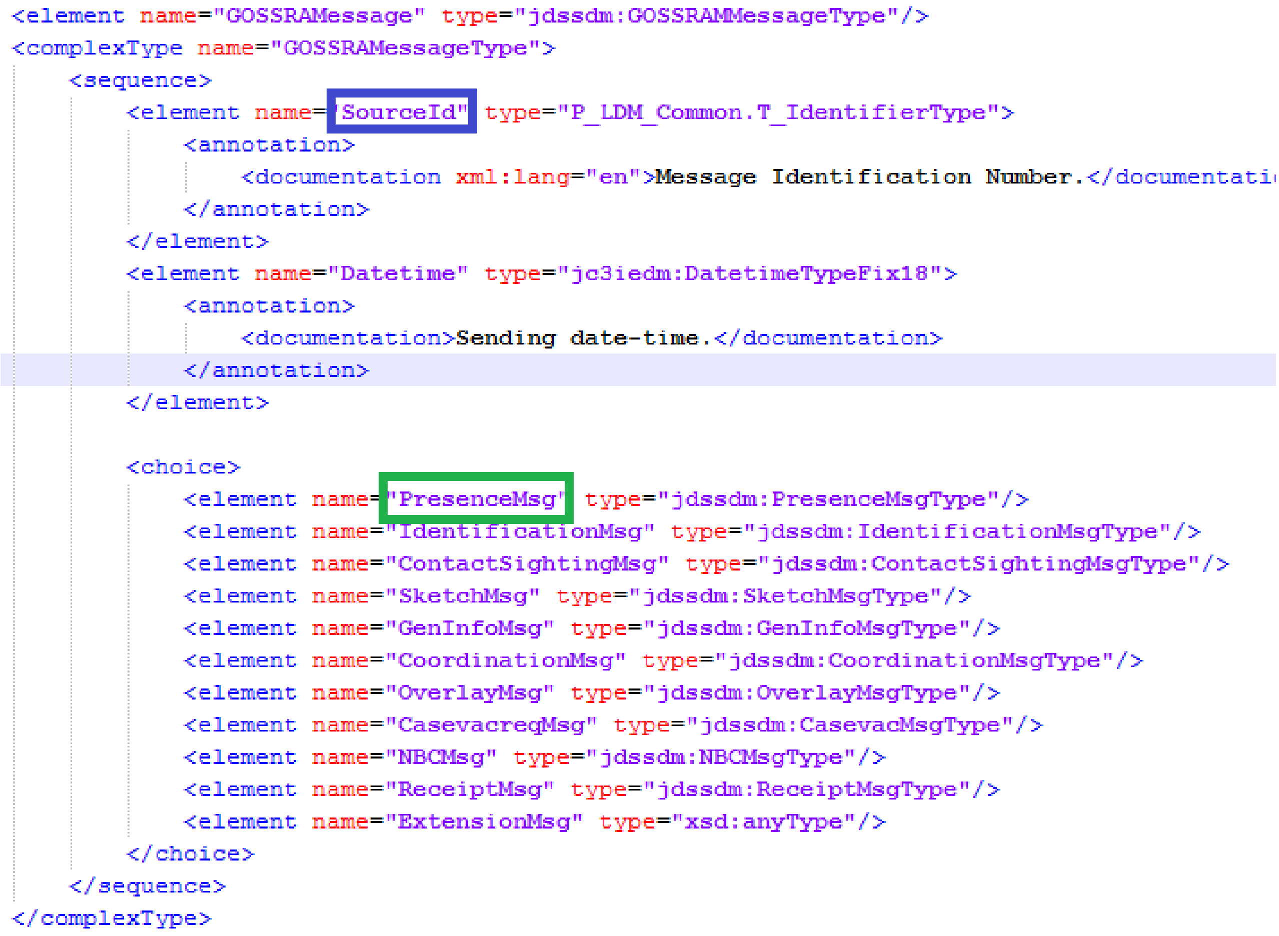
- Red marks the packet name
- Green is the topic name
- Blue is the source id consisting of Resource (set to 13) and instance id (set to 37)

The resulting topic name would be:

- P_Laser_Range_Finder_PSM/C_Laser_Range_Finder/13/37

The C4I Data model has no packet name as shown above, since it is derived from another data model. Thus, the packet name is set to “P_C4I”. The topic name is set to the element used.

So considering the following use case / structure:



```
<element name="GOSSRAMessage" type="jdssdm:GOSSRAMMessageType"/>
<complexType name="GOSSRAMessageType">
    <sequence>
        <element name="SourceId" type="P_LDM_Common.T_IdentifierType">
            <annotation>
                <documentation xml:lang="en">Message Identification Number.</documentati
            </annotation>
        </element>
        <element name="Datetime" type="jc3iedm:DatetimeTypeFix18">
            <annotation>
                <documentation>Sending date-time.</documentation>
            </annotation>
        </element>

        <choice>
            <element name="PresenceMsg" type="jdssdm:PresenceMsgType"/>
            <element name="IdentificationMsg" type="jdssdm:IdentificationMsgType"/>
            <element name="ContactSightingMsg" type="jdssdm:ContactSightingMsgType"/>
            <element name="SketchMsg" type="jdssdm:SketchMsgType"/>
            <element name="GenInfoMsg" type="jdssdm:GenInfoMsgType"/>
            <element name="CoordinationMsg" type="jdssdm:CoordinationMsgType"/>
            <element name="OverlayMsg" type="jdssdm:OverlayMsgType"/>
            <element name="CasevacreqMsg" type="jdssdm:CasevacMsgType"/>
            <element name="NBCMsg" type="jdssdm:NBCMsgType"/>
            <element name="ReceiptMsg" type="jdssdm:ReceiptMsgType"/>
            <element name="ExtensionMsg" type="xsd:anyType"/>
        </choice>
    </sequence>
</complexType>
```

Figure 2-34 – Example status information data structure for C4I DM

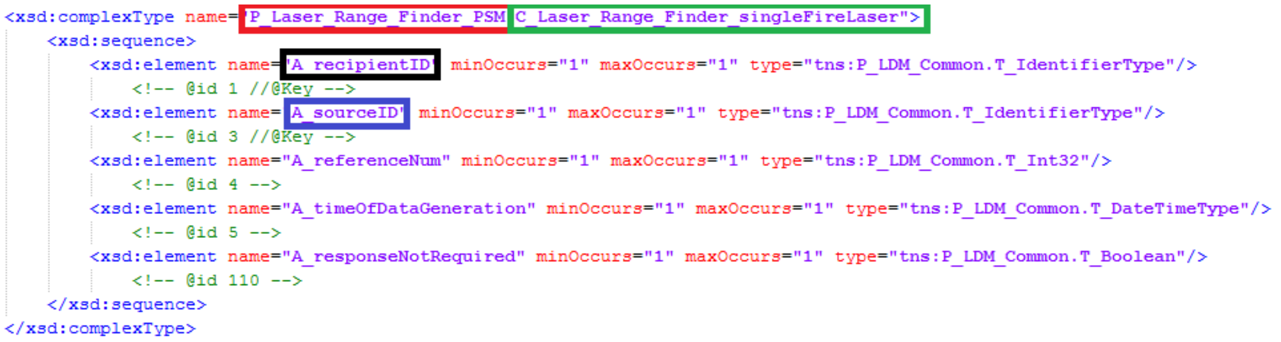
The color scheme is as following

- Green is the topic name
- Blue is the source id consisting of Resource (set to 13) and instance id (set to 37)

It describes a presence message. As the packet name is static set to “P_C4I” the following topic name will result:

- P_C4I/PrecenceMsg/13/37

To command a measurement to the laser range finder (if possible) the following structure is used.



```
<xsd:complexType name="P_Laser_Range_Finder_PSM C_Laser_Range_Finder_singleFireLaser">
    <xsd:sequence>
        <xsd:element name="A_recipientID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 1 //@Key -->
        <xsd:element name="A_sourceID" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_IdentifierType"/>
            <!-- @id 3 //@Key -->
        <xsd:element name="A_referenceNum" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_Int32"/>
            <!-- @id 4 -->
        <xsd:element name="A_timeOfDataGeneration" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_DateTimeType"/>
            <!-- @id 5 -->
        <xsd:element name="A_responseNotRequired" minOccurs="1" maxOccurs="1" type="tns:P_LDM_Common.T_Boolean"/>
            <!-- @id 110 -->
    </xsd:sequence>
</xsd:complexType>
```

Figure 2-35 – Example command data structure for system and situational awareness DM

The color scheme is as following

- Red marks the packet name
- Green is the topic name
- Blue is the source id consisting of Resource (set to 47) and instance id (set to 11)
- Black is the recipient id consisting of Resource (set to 13) and instance id (set to 37)

The resulting topic name would be:

- P_Laser_Range_Finder_PSM/C_Laser_Range_Finder_singleFireLaser/13/37/47/11

2.4.2.4.5 Identifiers

The data model introduces two identifiers for components and their objects.

The resource Id describes which resource is providing the information. The resource id should be configurable for devices and components and will be assigned by the system integrator.

The instance Id describes which instance of a topic is providing the information and can be used to differ between objects on one component of the same device or information created the software.

Every entity in the network that uses the same resource id has to ensure the unique generation of the instance id.

2.4.2.4.6 Data model availability

The Data model is available, as the documents, on the GOSSRA-Website. A deviating availability will also be stated on the GOSSRA-Website.

2.4.2.5 Network Bootstrapping

MQTT uses a centralized broker which subsystems and peripheral devices need to connect to. Additionally other sub-systems may also serve their own MQTT-Broker for their subsystem. To enable an integration without a specific configuration of new devices in a system a bootstrapping method is necessary.

2.4.2.5.1 MQTT-Bootstrapping

For connecting to a MQTT-Broker the following network services are necessary.

- DHCP-Server
- DNS-Server
- MQTT-Broker

The DHCP Server provides the device with an IP-Address and a DNS-Address. Setting a standard-gateway may not be necessary and is thus optional. Only one DHCP-Server per DSS is allowed.

The DNS-Server contains is used to resolve hostnames. It needs at least one entry called “Broker” with a relation to the brokers IP-Address. By that an application can find the central broker to connect to.

The Application then uses the resolved IP-Address of the broker to connect to the MQTT-Broker successfully.

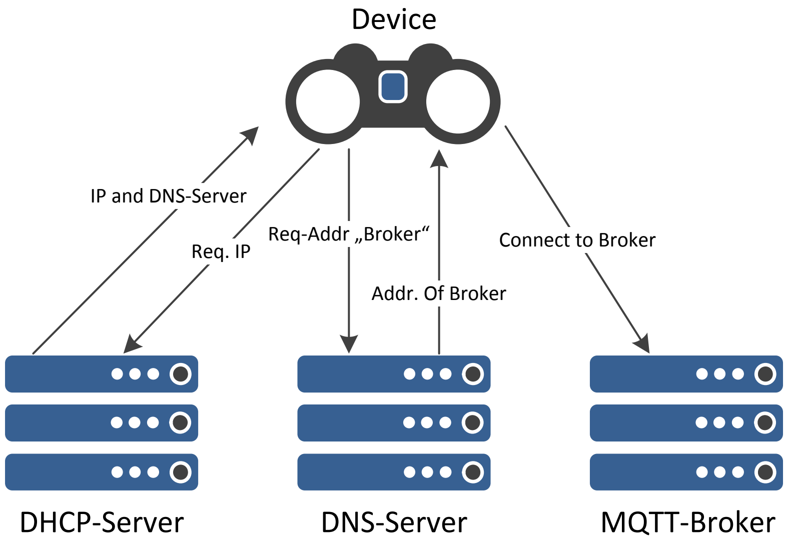


Figure 2-36 – How to find the MQTT-Broker

2.4.2.5.2 Multiple MQTT-Broker

In some cases it may be possible, that more than one MQTT-Broker is used within the system. In this case it is critical to bridge the additional MQTT-Broker to the main MQTT-Broker that can be found using the DNS-Protocol and the name “broker”. This could be useful if only a subset of messages shall be transmitted to the central MQTT-Broker until no entity subscribes to them.

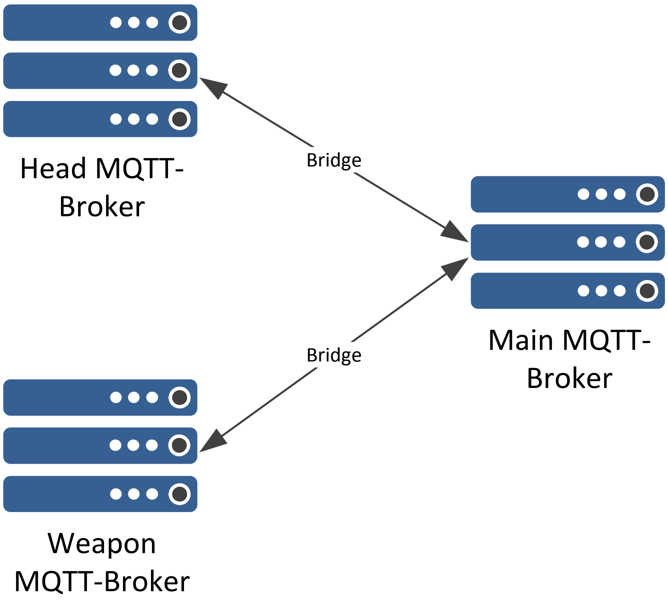


Figure 2-37 – Example on an target architecture using different MQTT-Broker

Unique ID	Type	Requirement Description
REQ-18	**CR**	The DSS shall use USB ≥2.0 for wired components (Fall-back Technology)
REQ-19	**OE**	The DSS should use USB ≥3.1 2nd Generation for wired components
REQ-20	**CR**	The DSS shall use MQTT as exchange mechanism for Data (according to DEP.01)
REQ-21	**OE**	The DSS shall use Data Distribution Service as exchange mechanism for Data in the BMS Domain (according to DEP.01)
REQ-22	**CR**	The DSS shall use the GOSSRA Data Modell for Data Representation
REQ-23	**CR**	The DSS shall translate the events of USB-HID-Devices to MQTT (according to DEP.01)
REQ-24	**CR**	The DSS shall translate the data of proprietary USB-Devices to MQTT (according to DEP.01)
REQ-25	**CR**	The DSS shall translate the streaming data of USB-Devices according to DEP.02
REQ-26	**OE**	The DSS should use Bluetooth ≥4.2 for the personal area network connecting wireless components
REQ-27	**RE**	The DSS shall translate the events of Bluetooth-HID-Devices to MQTT (according to DEP.01)
REQ-28	**RE**	The DSS shall translate the data of proprietary Bluetooth-Devices to MQTT (according to DEP.01)
REQ-29	**RE**	The DSS shall translate the streaming data of Bluetooth-Devices according to DEP.02
REQ-30	**CR**	Wired GOSSRA Devices shall comply with DEP.01
REQ-31	**CR**	Wired GOSSRA Devices shall use MQTT or MQTT-SN
REQ-32	**CR**	Wireless GOSSRA Devices shall comply with DEP.01
REQ-33	**CR**	Wireless GOSSRA Devices shall use MQTT-SN
REQ-34	**OE**	The DSS should use NFC for Near Field communication (according to DEP.01)
REQ-35	**RE**	The DSS shall translate the data of NFC-Devices to MQTT (according to DEP.01)
REQ-36	**CR**	The DSS shall provide exactly one DHCP-Server service.
REQ-37	**CR**	The DSS shall provide a DNS-Server service
REQ-38	**CR**	The DNS-Server service of the DSS shall resolve the name “broker” to the IP-Address of the main broker in the DSS
REQ-39	**CR**	The DSS shall provide at least one MQTT-Broker
REQ-40	**OE**	The DSS shall provide at exactly one MQTT-Broker
REQ-41	**CR**	Additional MQTT-Broker in the DSS shall be bridged to the main broker of the DSS
REQ-42	**CR**	The main broker of the DSS shall be accessible for all connected MQTT-clients

Table 2-13 – Requirements on the Data Exchange Service

2.4.3 Soldier Application

2.4.3.1 Soldier Application Architectural Concepts

This paragraph describes the key application architecture concepts for a Soldier System. The term Soldier Application refers to a self-standing SW Component which implements one or more services, e.g. C4I Services.

To promote open competition and avoid vendor lock-in Soldier Applications should be based on open interfaces so that they can be manufactured from parties independent of the original system developer. To achieve this, a Reference DSS Application architecture is required to ensure a standardised interaction between DSS and display systems, enabling HMI Application configuration to accommodate new DSS devices and the promotion of reusability wherever possible.

An Application for Agile Soldier Platform should fulfil the following objectives:

- **Objective 1:** *Portable Soldier Applications* that execute on any OS and on any hardware;
- **Objective 2:** *Reusable Soldier Applications*, through adopting an App Store concept system integrators can obtain, reuse and deploy existing software;
- **Objective 3:** *Configurable Application HMI*, where widgets can be added or removed, displayed or hidden and positioned in the screen through a configuration file;
- **Objective 4:** *Interoperable Soldier Application* with existing vehicle devices and sub-systems.

The terms used throughout this document have the following definitions:

Term	**Definition**
Widget	A self-contained graphical program that displays data and enables a user to perform a function.
Graphical User Interface (GUI)	The collection of widgets displayed on a DSS HMI display to visually present data to the User.
Multi-function or Multi-purpose HMI (term used interchangeably)	Ability to operate the majority of subsystems from one HMI to enable the concept of flexible user role e.g. squad commander can take RSTA role by controlling a given UAS from his/her terminal. Thus, the DSS terminal HMI can be used for more than one role.
DSS Terminal	The term used for the Soldier display screen and bezel buttons mounted around the edge.
DSS Station	Comprised of hardware e.g. input and output devices such as a joystick, display, and headset, that allow a user to perform one or more roles.
DSS sub-system	Collection of hardware and software that provide required capabilities to fulfil a role in a DSS.
HMI Input Device	Any device used by DSS station operator to interact with and command the mission subsystem, like a joystick, and bezel buttons.
HMI Output Device	Any device used to display data, inform and warn DSS such as screen, warning lights, headsets, and tactile devices.

Table 2-14 – Definition of Terms for Soldier Application Elements

Figure 2-38 depicts the logical components a possible Soldier Application Reference Architecture can be based upon. This is a logical architecture then there is no constraint on the physical location of the execution of the Application components.

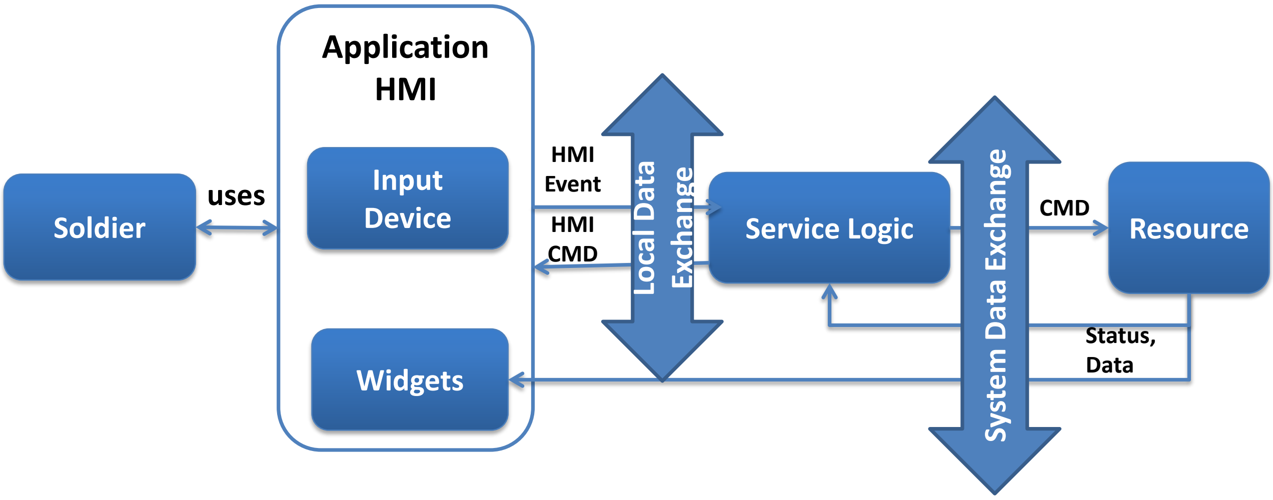


Figure 2-38 – Soldier Application Logical Architecture

The Soldier Application Logical Architecture includes the following components:

- **Application HMI**: A collection of self-contained widgets that display data and enable the operator to perform a function.
- **Service Logic**: The set of services to control the DSS Resources, e.g. sub-system/devices.
- **Data Exchange Service Components:** DSS data exchange services provides the needed support for the interactions among different software components:
    - **Local Data Exchange** services support the interaction between the Application Components, namely Application HMI and Service Logic
    - **System Data Exchange** services support the interaction between the Application and external System Components, i.e. the Resources.

2.4.3.2 Soldier Application Interface Description

The figure below depicts the main components and related interconnection of a Soldier Application, which serves a soldier acting as Commander of an STU in the Personal Domain.

A Soldier Application can exchange data with other Applications via the Data Exchange Services.

Due to the equipment assigned to a Commander Role, the Application main components, i.e. Application HMI and Service Logic, might be hosted by the Commander Display and the Commander Processing Unit respectively. This solution allows for the computation-intensive service logic to be hosted on a dedicated computation platform typically allocated on the Soldier Torso, while a lightweight HMI Component to be hosted by one or more wearable displays such as Wrist Device, Head-Up Display, and so on.

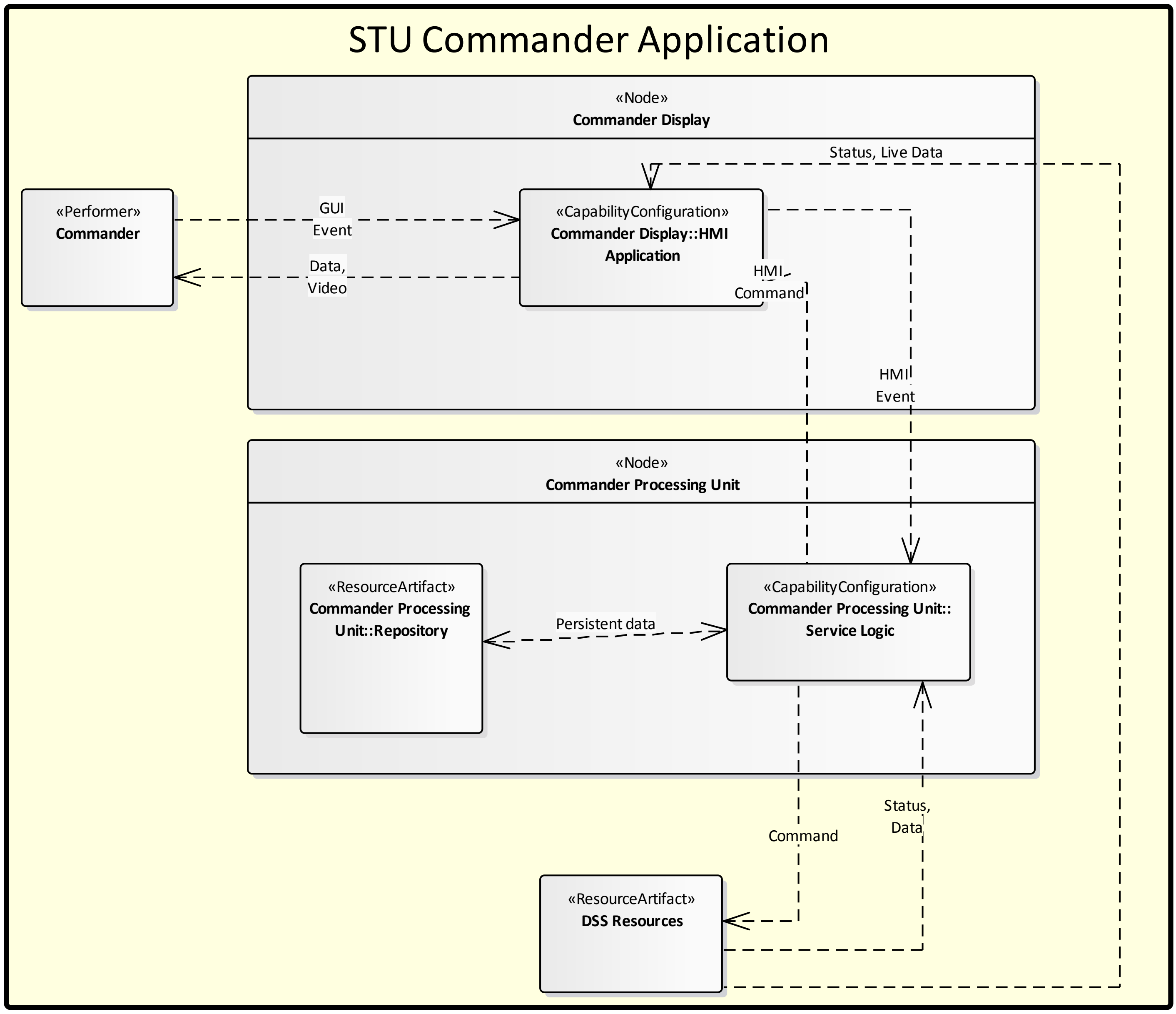

STU Commander Application
«Node»
Commander Display
Status, Live Data
«Performer»
Commander
GUI Event
Data, Video
«CapabilityConfiguration»
Commander Display::HMI Application
HMI Command
HMI Event
«Node»
Commander Processing Unit
«ResourceArtifact»
Commander Processing Unit::Repository
Persistent data
«CapabilityConfiguration»
Commander Processing Unit:: Service Logic
Status, Data
Command
«ResourceArtifact»
DSS Resources

Figure 2-39 – DSS Personal Domain - Commander Application

Unique ID	Type	Requirement Description
REQ-43	**OE**	The Commander Application should allow allocating the Application HMI component and the Service Logic components on separate computing platforms.
REQ-44	**OE**	The Commander Application should allow the Application HMI to be hosted on a wearable computing platform such as Head-Up display or Wrist Computer.
REQ-45	**OE**	The Specialist Application should allow allocating the Application HMI component and Service Logic components on the same platform.

Table 2-15 – DSS Personal Domain - Commander Application Requirements

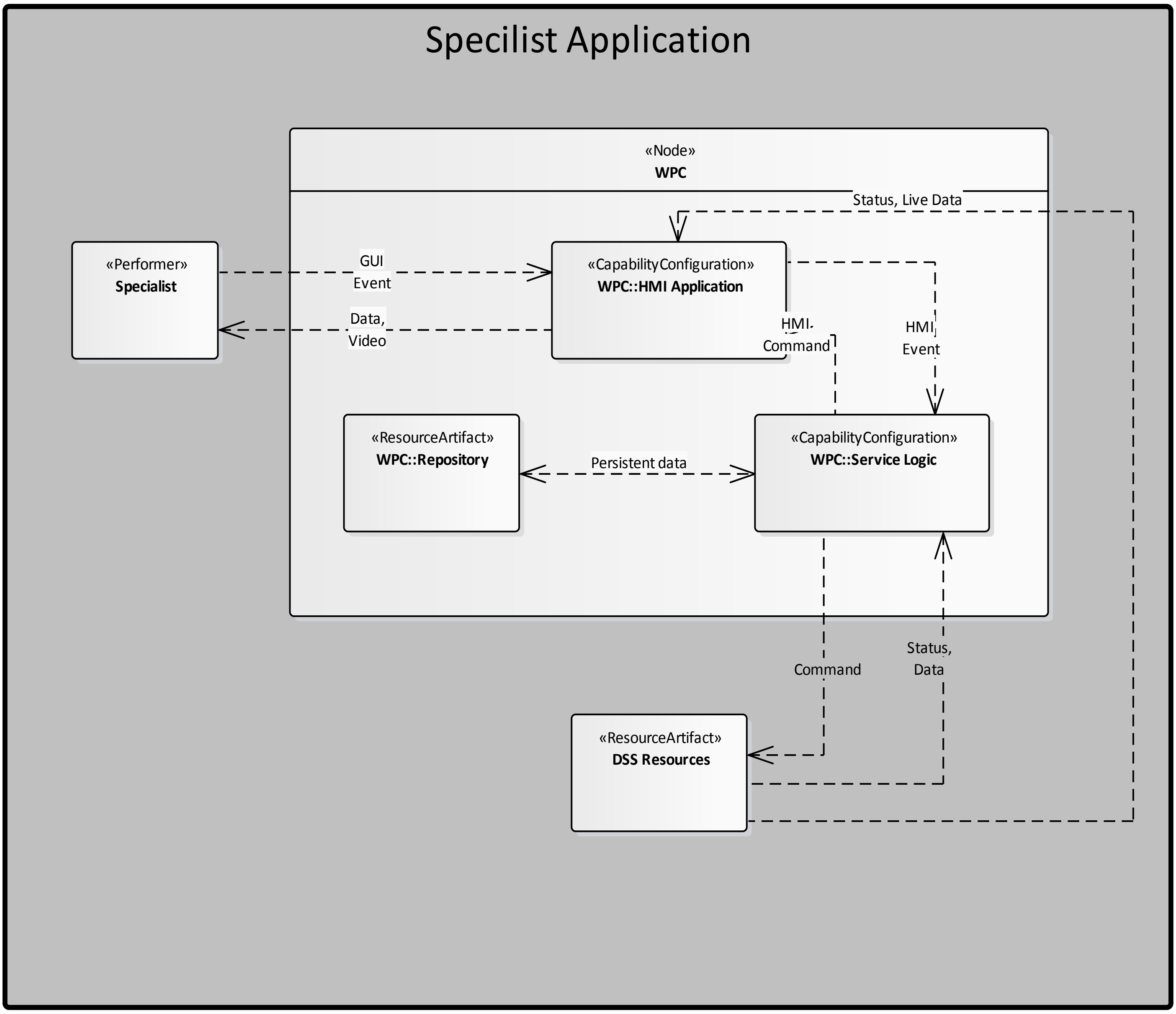


Figure 2-40 – DSS Personal Domain - Specialist Application

The figure below depicts the main components and related interconnection of a Soldier Application, which acts in the Personal Domain of a soldier acting as Specialist.

Due to the equipment assigned to a Specialist Role, the Specialist Application's main components, i.e. Application HMI and Service Logic, will be both hosted on the same computing platform, e.g. Smartphone, Wrist PC.

The adoption for the Specialist Application of the same architectural scheme as the one described for the Commander Applications will still result in an agile soldier platform as described in Section 2.4.3.1.

2.4.3.3 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers system components in the Personal domain supported respectively by (i) the Application HMI and (ii) the Application Service Logic.

The Application HMI provides the following logical ports:

- HMI.01, which supports the Application HMI Services in the Personal Domain and is mapped on Personal Data Services, as described in Section 2.4.2.2
- HMI.03, which supports the Streaming for the Application HMI Services and is mapped on Streaming Data Services as described in Section 2.4.2.2

The Application Service Logic provides the following logical ports:

- ServiceLogic.01, which supports the Application Service Logic in the Personal Domain and is mapped on Personal Data Services, as described in Section 2.4.2.2
- ServiceLogic.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in Section 2.4.2.2.

2.4.3.4 Soldier Application System to System Port Connectivity

2.4.3.4.1.1 STU Commander Application

The Soldier Application which is serving an STU Commander, who acts in the Personal Domain exchange data with peers system component as specified below.

The Application HMI component exchanges data via the following logical ports:

- HMI.01, which is based on Personal Data Services, and interconnects with:
  - the STU Commander Application Service Logic to:
    - Receive HMI Command, Data
    - Send HMI Event
  - The set of STU Commander Resources to
    - Receive Data
- HMI.03, which is based on Streaming Data Services, and interconnects with:
  - The set of STU Commander Resources to:
    - Receive Streaming of live data, e.g. Video

The Application Service Logic component exchanges data via the following logical ports:

- ServiceLogic.01, which is based on Personal Data Services, and interconnects with:

  - The STU Commander HMI Application to:
    - Send HMI Command, Data
    - Receive HMI Event
  - The set of STU Commander Resources to
    - Send Command
    - Receive Data
- ServiceLogic.06, which is based on Streaming Data Services, and interconnects with:
  - The set of STU Commander Resources to
    - Receive Streaming of live data, e.g. Video

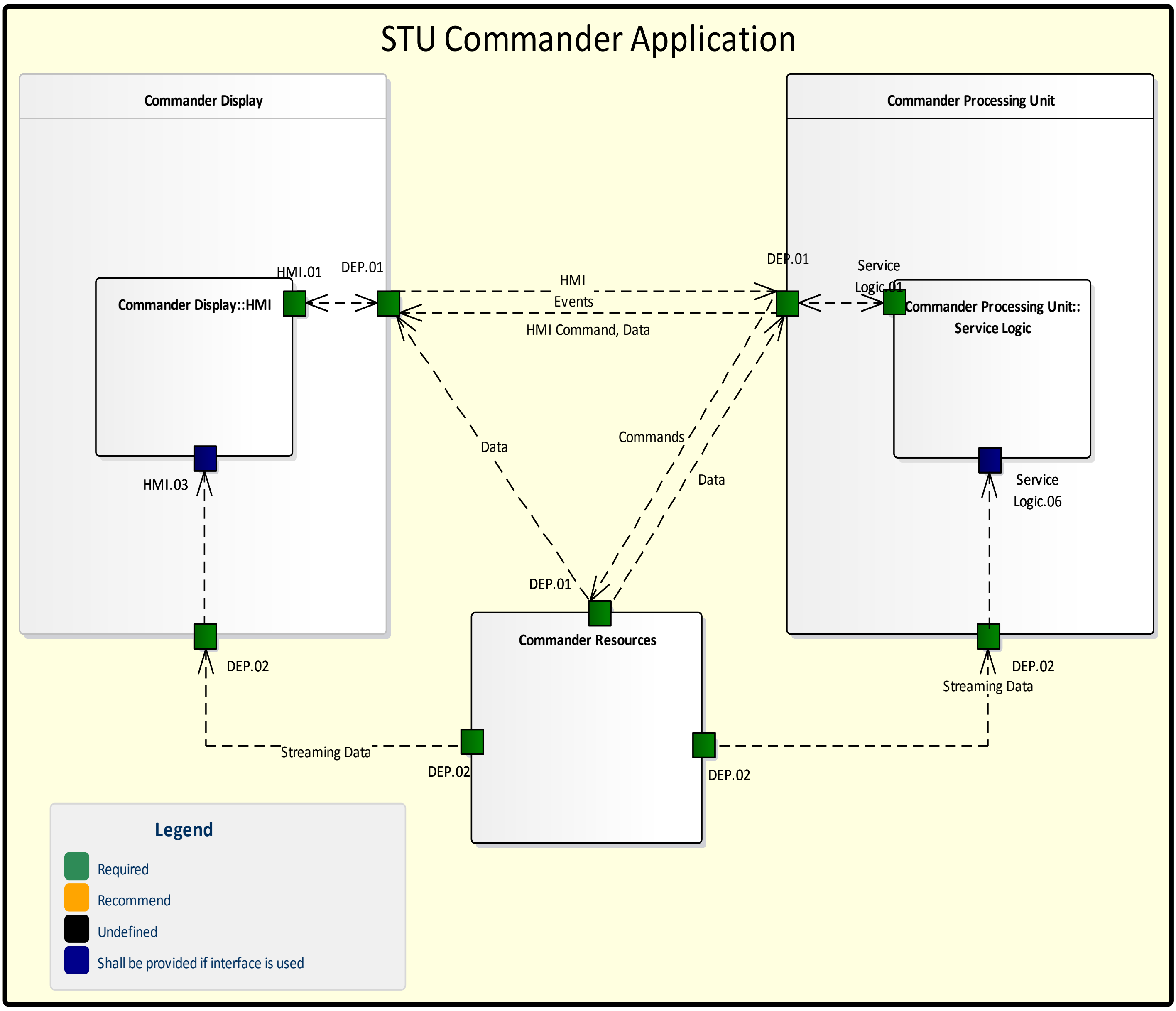


Figure 2-41 – System to System port connectivity of Soldier Application at Personal Domain for STU Commander Application

2.4.3.4.1.2 Specialist Soldier Application

The Soldier Application which is serving a Specialist Soldier, who acts in the Personal Domain exchange data with peers system component as specified below.

The Application HMI component exchanges data via the following logical ports:

- HMI.01, which is based on Personal Data Services, and interconnects with:
  - The set of STU Commander Resources to
    - Receive Data
- HMI.03, which is based on Streaming Data Services, and interconnects with:
  - The set of STU Commander Resources to:
    - Receive Streaming of live data, e.g. Video

The Application Service Logic component exchanges data via the following logical ports:

- ServiceLogic.01, which is based on Personal Data Services, and interconnects with:
  - The set of STU Commander Resources to
    - Send Command
    - Receive Data
- ServiceLogic.06, which is based on Streaming Data Services , and interconnects with:
  - The set of STU Commander Resources to
    - Receive Streaming of live data, e.g. Video

It is worth noting that the data exchange between Application HMI and Application Service Logic is based on the internal Smartphone/WPC inter-process communication services.

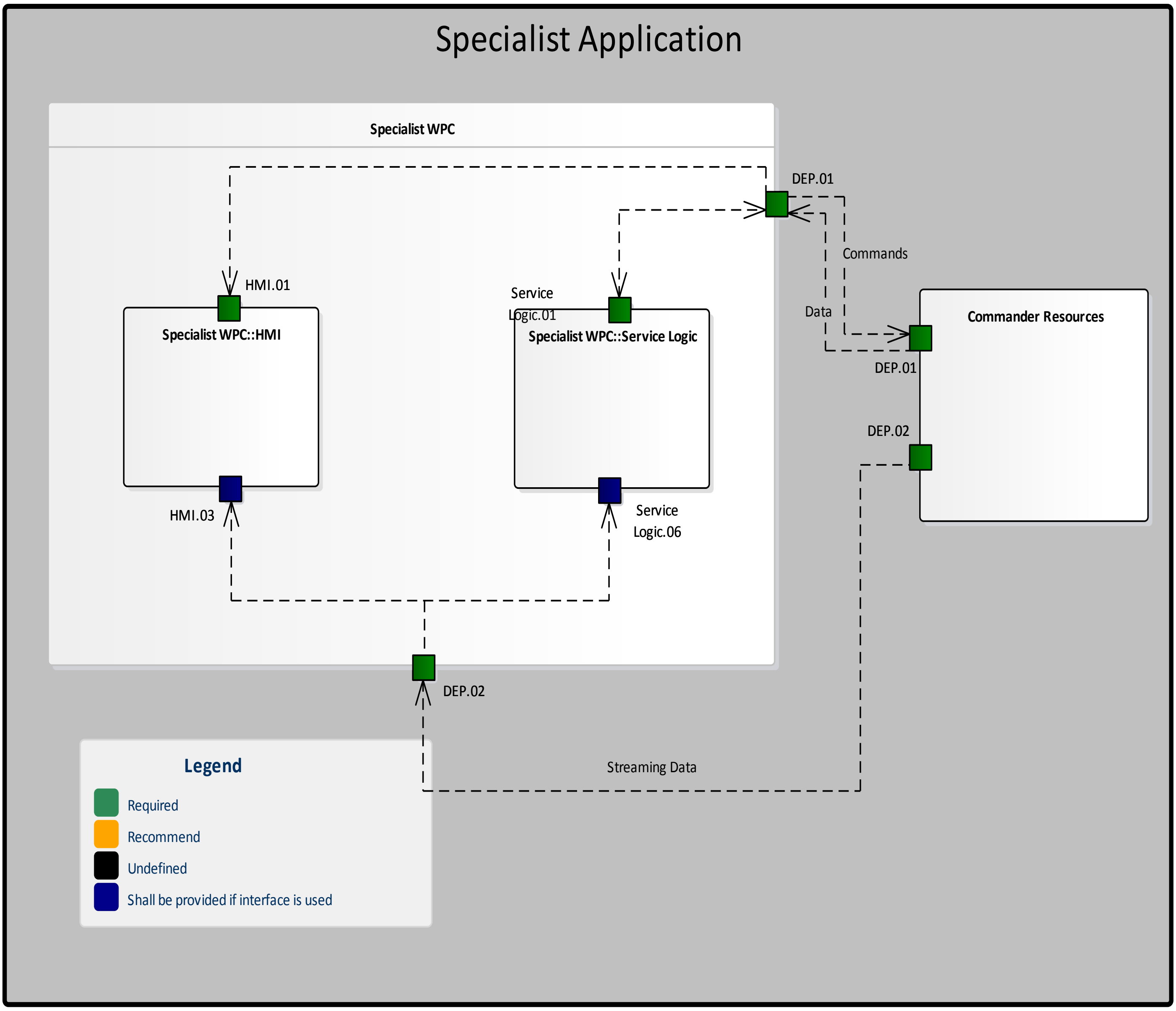


Figure 2-42 – System to System port connectivity of Soldier Application at Personal Domain for Specialist's Application

2.4.4 Communication Components

2.4.4.1 Communication Components Interface Description

The Communication System includes all the components and functionalities providing to the DSS the ability to exchange voice and data, such as mission information, Blue force tracking, command and control, messaging, etc., and in general to communicate with other entities during the mission.

The functionalities include the services in the two defined User and Radio domains. The User services are the ones that the DSS uses directly through interactions with the local devices, while the Radio ones are transparent to the user, yet delivering needed functionalities and providing solutions to mission requirements.

As for the radio services, two macro functional areas identified: LOS (Line-of-Sight) and B-LOS (Beyond Line of Sight).

Also, security (COMSEC) mechanisms are used for protected transmissions.

Unique ID	Type	Requirement Description
REQ-46	**CR**	DSS communication system shall be radio agnostic (e.g. Software defined radios)
REQ-47	**CR**	DSS communication system shall provide a security solution for voice & data protection (COMSEC)

Table 2-16 – DSS Personal Domain – DSS Communication Requirements

The DSS Personal Domain includes interconnections of resources physically located on the DSS' user's body, in order for them to be directly used -locally- by the DSS itself.

Figure 2-43 – Radio DSS Personal Domain

For this case more than one technology (wired or wireless) could be used to achieve interconnection among devices operating in the System, such as sensors, computers, effectors, etc., which overall provide information from and for the DSS.

Hence, the Communication DSS System component, in the Soldier Personal Domain (SPD), is composed of the radio (or multiple radios), and those devices which could use it/them for Personal Domain applications, such as: GNSS receiver data or PAN (Personal Area Network) for worn sensors or pre-recorded voice messaging. Another interface could be the supplementary power section, when available for additional supply power.

The figure below depicts the main components and related interface of a Radio Communication system in SPD Domain.

The Radio Device has the following interfaces:

- Data interface with WPC for traffic transfer
- Voice interface with Headset
- Power supply interface

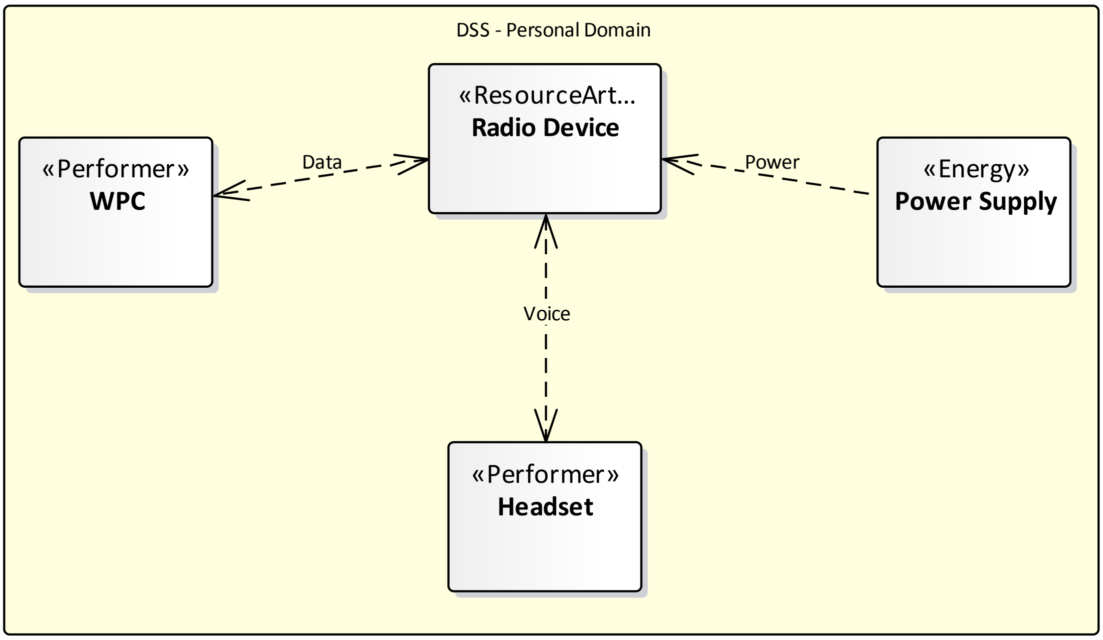


Figure 2-44 – Radio Device Interfaces in SPD domain

2.4.4.2 Communication Components Port Specification

The Radio Device includes the following ports:

- RD.1: Radio Device Voice Port
- RD.2: Radio Device Data Port
- RD.3: Radio Device Power Port

Component ports descriptions are provided in the next paragraphs.

2.4.4.2.1 Radio Device Voice Port

The Voice Port is the interface through which the DSS can access the Voice User Service or, simply, make voice calls within the radio network domain.

The analogue audio port is present on the radio device for connection with a headset, typically composed of loudspeaker/in-the-ear speaker, microphone and Push-To-Talk device.

From background analysis, the voice port is typically part of radio equipment with its proprietary ancillary set. In addition to the basic headset, an advanced configuration could entail headphones, earbuds, in-the-ear headset, microphone and osteophones, noise reduction module and ear protection system

Given the above considerations, the radio device voice port is not amenable to the generalized port definition.

2.4.4.2.2 Radio Device Data Port

The Data Port is the connection through which data sources and/or network-enabled devices, such as a wearable PC, can be attached to the Radio to exchange data on the networked wireless domain.

The most commonly used wired interfaces for the Radio Device Data Port are:

- USB (USB 2.0, USB OTG)
- Ethernet (LAN, 10/100 Ethernet)
- Serial port (Serial SMBus, RS-232, RS-422, RS-485)
- Bluetooth (Bluetooth V2.0+EDR)

Wired data ports are generally gathered in a single data connector.

2.4.4.2.3 Radio Device Power Port

The commonly adopted architecture for the radio power supply is a dedicated battery.

In order to extend the radio working time during the overall mission, an external auxiliary power source could be connected through a power port to the radio system.

Refer to the power system component description for more details about the radio device power port.

2.4.4.3 Communication Components System to System Port Connectivity

In the Personal Domain the Communication Components ports interconnect with the DSS system components as reported below.

- Radio Device Voice Port (RD.1) interconnects with the Headset;
- Radio Device Data Port (RD.2) interconnects with the Wearable PC (WPC);
- Radio Device Power Port (RD.3) interconnects with the Power Supply.

2.4.5 Human Interface Devices

2.4.5.1 Human Interface Device Interface Description

2.4.5.1.1 Audio exchange interfaces

Audio exchange mainly occurs between the headset in the Head section and the Torso, where the radio and the personal computing platform are usually allocated.

The headset usually includes one microphone (either mono or stereo) and one pair of earpieces (left and right), possibly mechanically integrated.

Wired Audio HIDs rely on:

- Analogue interface, following electrical and impedance levels specifications compliant to Intel AC'97 specifications, High Definition Audio Specification or similar standard (see /30/, /31/);
- Digital interface, complying with USB Device Class Definition for Audio (see /32/).

In the case of HIDs including active signal processing devices (protect and enhance services), external power can be supplied via USB or similar very low power line.

Wireless Audio HID interfaces will comply with Bluetooth advanced audio distribution profile (A2DP) or Headset Profile (HSP). Audio HIDs with a wireless interface must be powered locally to the Head section, thus requiring a local dedicated battery or a central Head power source.

2.4.5.1.2 Video exchange interfaces

The head-up display (HUD) in the Head section can be fed with data coming from vision enhancement sensors (NVG, IR, sight aids, etc.), augmented or virtual reality information (AR, VR) and also information from weapon sights, radio, and torso computing platform.

In the case of see-through, transparent HUDs, there is no need to provide high-resolution, very low-latency video. Data throughput can be kept limited, compatible with wired USB 2.0 connections or wireless Bluetooth compressed Video Distribution Profile (VDP).

For fully-opaque, high-resolution HUD, a much wider bandwidth must be provided, so that USB3.1G2 seems the only possibility.

The head-down display (HDD) shows data from the computing platform in which it is usually integrated, even in case of very small wrist-worn HDDs. Most of the time the display is used for an occasional browsing of maps or messages, with limited data exchange requirements. However, there could be the need to display real-time, high-resolution video received from shared cameras (e.g. from a UAV). Wireless communications with a UAV does not require an additional external device to communicate with if the interface is integrated with the computing platform. If the video is received from the radio, then it is sent through the same interface that connects the computing platform.

2.4.5.1.3 Remote control interfaces

Simple remote controls (e.g. keys and buttons) can rely on USB connections. For custom controls, a local conversion to USB can be provided.

More advanced controls, like touch-screen based virtual keyboards and keypads, are usually integrated into the HDD. A small camera to detect position and movement of the eyes may provide feedback to the AR and VR management units, improving the HUD experience. Again, USB may provide sufficient bandwidth for this purpose.

Biometric credentials may be supplied once per session or polled periodically, to ensure that the user has the rights to use the system. Even in case of polling, the power required and the amount of data exchanged with the computing platform is limited and suitable to be transferred over USB connections.

2.4.5.1.4 Warnings and feedbacks

Warnings and feedbacks are mainly provided through visual and audio devices (HUD, HDD, and a headset) with the exception of tactile feedback. Tactile feedback is provided by arrays of tactile transducers integrated in the vest or worn under it. Feedback is provided in the form of dynamic patterns, with a very limited amount of data and power requirements suitable for USB connections.

2.4.5.2 Human Interface Device Port Specification

The HID category includes headsets, remote PTTs, displays, cameras, biometric sensors, motion and position sensors, keyboards, pointing devices, haptic feedback effectors, etc. featuring a wide range of data throughput and power consumption characteristics. This section includes only the HIDs that are not already integrated into other soldier system components, for which no interface standard is necessary.

The placement must comply with the body part the HID interacts with, so relatively long cables are common, and some connections may cross the torso/head boundaries. When cables are not an option (e.g. wrist devices) power must be supplied by a local battery and data exchange must rely upon a wireless interface.

Also, some HIDs may be mutually exclusive (e.g. NVG and HUD) or used only occasionally during the mission, so plug and play must be considered a standard feature.

Standard USB 2.0 connections (slave) can provide enough bandwidth and power supply for the most common wired HIDs. Very high bandwidth communications (e.g. high-resolution video) could be supported by using USB 3.1G2.

Wireless HIDs shall support Bluetooth, see also sensors and effectors wireless port interface requirements for the details. In addition, NFC connections may be used in case the data exchange is limited to occasional short data bursts. For example, a wrist device for biometric data collection used for soldier's identification and system access (obviously this requires the computing platform or another specific device, including another HID, to have an NFC interface too).

Unique ID	Type	Requirement Description
REQ-48	**CR**	The DSS shall be equipped with a headset-capability for audio exchange. The headset shall comprise microphone and earpieces or equivalent technologies.
REQ-49	**CR**	Wired Audio analogue interface shall be compliant to: Intel AC'97 specifications, High Definition Audio Specification or following standards Or USB Device Class Definition for Audio
REQ-50	**CR**	Wired Audio interfaces including active signal processing devices (protect and enhance services), shall be provided with external power supplied via USB or similar very low power line.
REQ-51	**CR**	Wireless Audio interfaces shall be compliant to Bluetooth advanced audio distribution profile (A2DP) or Headset Profile (HSP).
REQ-52	**CR**	Wireless Audio HIDs shall be powered locally to the Head section, thus requiring a local dedicated battery or a central Head power source.
REQ-53	**CR**	The DSS shall be equippable with a head-up display and/or a head-down display for video vision
REQ-54	**CR**	For see-through, transparent head-up displays (HUD), data interface shall be compliant to wired USB 2.0 connections or wireless Bluetooth compressed Video Distribution Profile (VDP).
REQ-55	**CR**	For fully-opaque, high-resolution HUD, data interface shall be compliant to USB3.1G2.
REQ-56	**OE**	Wireless communications interface with a UAV should be integrated with the DSS.
REQ-57	**OE**	If the UAV video is received from the radio, it should be shared within the DSS compliant to DEP.02
REQ-58	**CR**	Remote controls shall relay on USB connections.
REQ-59	**OE**	An audio hub or similar mixing capability should be included to manage the routing of the audio within the DSS
REQ-60	**CR**	The DSS shall be equipped with a remote PTT control with the ability to talk on at least two separate channels

Table 2-17 – DSS Personal Domain – HID Requirements

2.4.5.2.1 Wired HIDs

The generic wired HID includes:

- Data and Power interface (see Figure 2-23): USB connections are well suited for this purpose, as they support virtually any HIDs data and power requirements.

When required, external support for NFC data exchange includes also:

- NFC interface (see Figure 2-23): As mentioned before, in case of occasional short bursts of data, an NFC to USB "dongle" may be used.

2.4.5.2.2 Wireless HIDs

The generic, self-powered wireless HID include:

- Wireless interface (see Figure 2-24 and Figure 2-25): Bluetooth interface complying with the requirements described in other relevant paragraphs, to provide support for wireless data exchange.

The rechargeable wireless HID include also:

- Battery charge input interface (see section 2.4.1.1.1.2.3): If the local battery needs to be occasionally recharged during mission time, this port shall comply with a standard DSS USB port (see Figure 2-23). When recharge is not intended to occur at mission time, the recharge input shall comply with common USB power chargers, possibly using an external adaptor to ensure mechanical and electrical compliance.

2.4.5.2.3 Voice Communication HID

The human interface device required for voice communications must include support for the custom audio and PTT connections of the specific radio it is intended for. The Voice Comm HID include at least:

- Voice and PTT port: this interface is specific to the radio device in use, but shall include microphone, earphones and PTT control.
- Headset port: in addition to mic and ears connections, this port may optionally include power, e.g. to supply a local ambient noise suppression device.
- External PTT port: used for chest-mount PTT remote control.

The voice communication HID may optionally include:

- Power and data port (see section 2.4.1.1.1.2.3): a standard USB port can be conveniently used to support local battery recharge and configuration data exchange. This is an optional port.
- Wireless remote control (see Figure 2-24 and Figure 2-25): this port will be able to support external wireless PTT remote control. This is an optional port.
- External audio source port (see Figure 2-25 and section 2.4.4.2.1): this port will allow audio exchange other than the standard one offered by the headset/radio connection. The audio connection with the computing platform allows, for instance, text to speech and speech to text for voice commands, message listening, etc. This is an optional port.

2.4.5.3 Human Interface Device System to System Port Connectivity

2.4.5.3.1 Audio exchange

The headset is the most common device for voice communications and may feature wired analogue, wired digital or wireless digital audio interface.

Although the main exchange of audio occurs between the headset and the radio, the local computing platform should be included in the path to support services like warnings and feedbacks. Speech to text and text to speech applications also require a patch from the headset to the computing platform (CP). Moreover, it is to be considered that the DSS may host more than one radio, e.g. Bowman, and more than one CP, e.g. Head and Torso CPs. It is, therefore, necessary to include an audio hub or a similar audio mixing capability to manage the routing of the audio within the DSS.

2.4.5.3.2 Video exchange

Video data may arrive from a local device (e.g. an IR camera), a remote device (e.g. a UAV) or from the processing of a computing platform (augmented reality devices, sensors, etc.)

The HDD is typically integrated in the EUD of the soldier, by today's standards, so that it shares the same ports as the computing platform of the EUD itself. USB 2.0 connections running at maximum speed (480Mb/s) will ensure high-resolution video in theory. Anyway, the quality of the video displayed to the viewer is upper bounded by the throughput of the slowest component in the chain, which is usually not USB but the radio/wireless bus.

The HUD is less standard, being usually composed of custom devices placed in the helmet interconnected with dedicated custom connections. One example is the Harris system, which includes a transparent HUD, an augmented reality unit for C4 (ARC4) and a night vision goggle unit (TM-NGV). A more open solution is under development by the Revision Military company, which is developing an android-based computing platform module in their Batlskin Viper P2 helmet. The module is able to drive the HUD and allows standard Bluetooth and USB connections, making it nearer to comply with GOSSRA.

With the computing platform integrated in the helmet, video display, forward and processing can be performed in the same way as the Torso CP does.

2.4.5.3.3 Remote Controls

The radio spends most of the mission time in a pouch, permanently connected to the system in voice and data. The soldier may have the need to bring two radios, or even a single device with two channels that may operate at the same time. For this reason, a remote PTT control must be included in the system, with at least the ability to talk on two separate channels.

2.4.6 C4I Application

2.4.6.1 C4I System Taxonomy

C4I System is composed of the following components:

- The Battlefield Management System (BMS) Component, which supports the Commander in the organization and control of the Small Tactical Unit and its coordination with peers to execute higher echelons commands.
- Situational Awareness (SA) Component, which improves (i) the Awareness, Understanding and Decision quality at both individual (i) level, i.e.: the single (dismounted) soldier, and (ii) at the collective level, i.e. Squad, Team.
- System Management (SYS), which manages the individual DSS as a system.
- Human RAS Interaction (HRI), which manages the usage of RAS, e.g. (squad of) UxVs, as support to both individual and collective tasks executions.

BMS, SA, and SYS support the Commander(s), then they can be considered as the key components of a C4I Application. Each of them can be either an Application Components or a Soldier Application (see Section 2.4.1) by itself.

Human - RAS Interaction (HRI) supports the Specialist Team who operates a RAS, then it is to be considered a separate specialised node.

For safe of clarity the C4I System views include separate sections for the C4I Application and the Human - RAS Interaction.

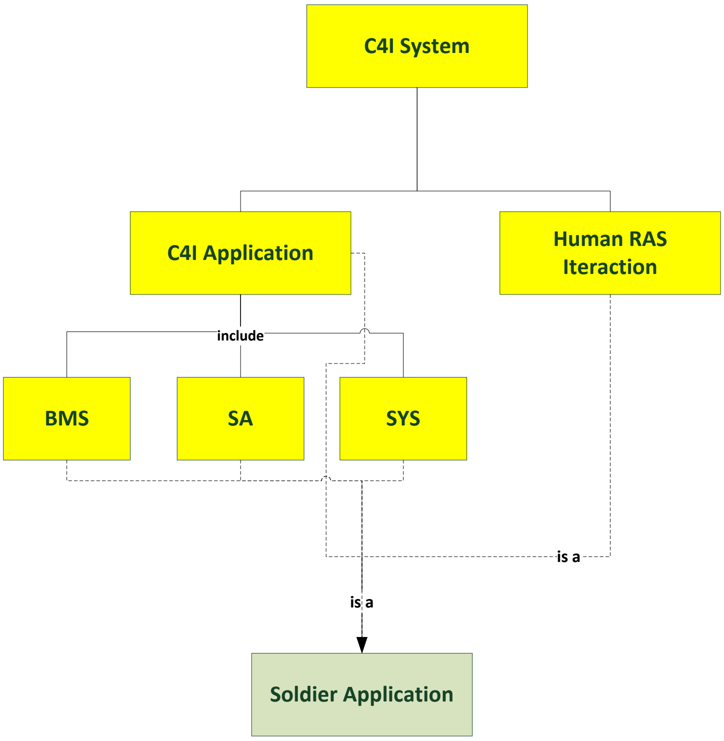


Figure 2-45 – C4I System Taxonomy

2.4.6.2 C4I Application Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equips an STU Commander who acts in the Personal Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant DSS Components, which equips the DSS of an STU Commander.

The HRI component is not shown because it is described in a dedicated paragraph.

The Interconnections among each C4I component with the other DSS Components is described below:

- BMS component interacts with STU Commander Effectors and STU Commander Sensors to control them and gather the needed Data.
- SYS component interacts with STU Commander Effectors and STU Commander Sensors to manage them as a system component, e.g. monitor & control, configuration, security.
- SA component interacts with STU Commander Sensors to control them and gather the needed data and streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Unique ID	Type	Requirement Description
REQ-61	**CR**	STU Commander C4I Application shall interact with STU Commander Effectors and STU Commander Sensors to control them and gather the needed Data.
REQ-62	**CR**	STU Commander C4I Application shall interact with STU Commander Effectors and STU Commander Sensors to manage them as a system component, e.g. monitor & control, configuration, security.
REQ-63	**CR**	STU Commander C4I Application shall interact with STU Commander Sensors to control them and gather the needed data and streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Table 2-18 – DSS Personal Domain – C4I Application Interface Requirements

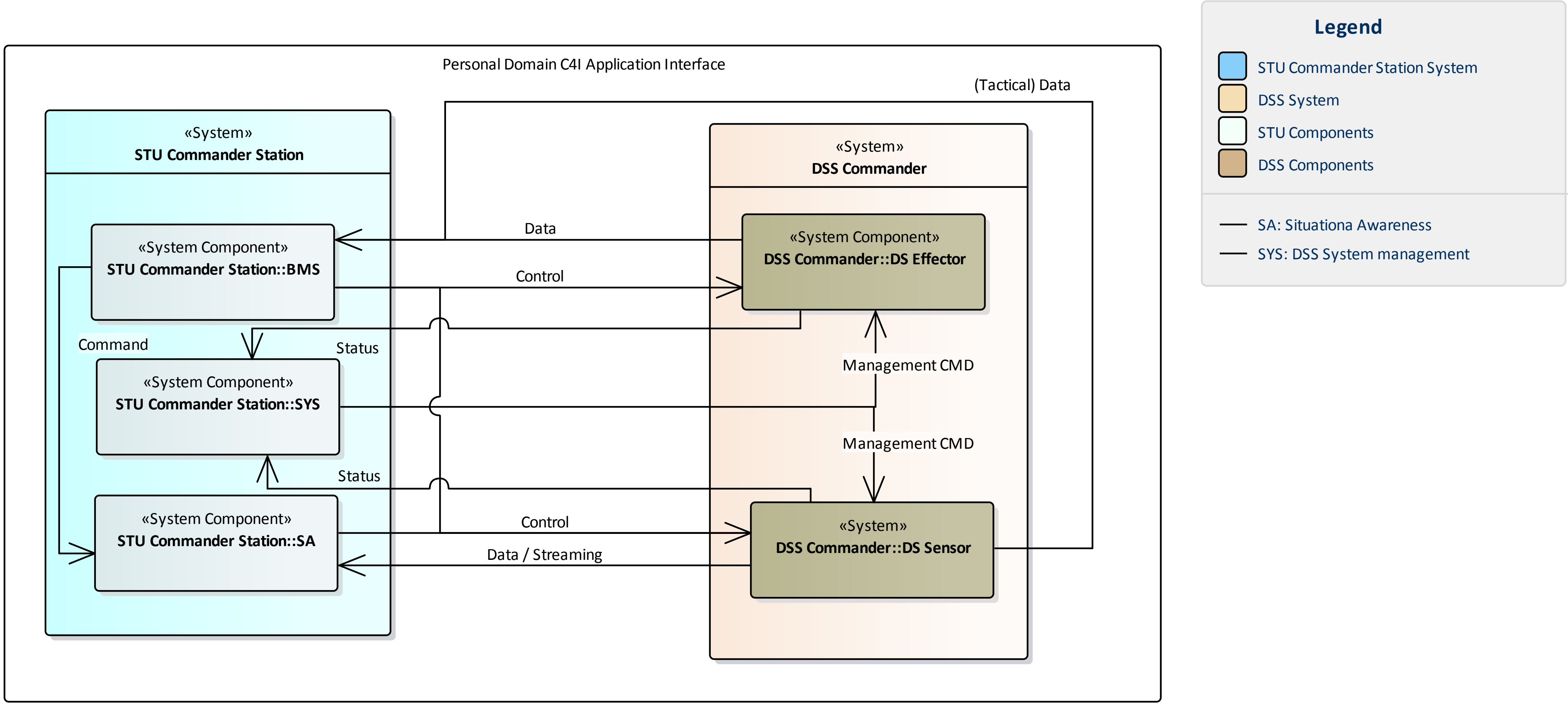


Figure 2-46 – Personal Domain – STU Commander C4I Application

2.4.6.3 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the BMS Service Logic, (ii) the SA Service Logic, and (iii) the SYS Service Logic are listed below.

The BMS Service Logic provides the following logical ports:

- BMS.01, which supports the BMS Services in the Personal Domain and is mapped on Personal Data Services, as described in Section 2.4.2.2 (DEP.01)
- BMS.06, which supports the Streaming for the BMS Services and is mapped on Streaming Data Services as described in Section 2.4.2.2. (DEP.01)

The SA Service Logic provides the following logical ports:

- SA.01, which supports the SA Services in the Personal Domain and is mapped on Personal Data Services, as described in Section 2.4.2.2 (DEP.01)
- SA.04, which supports the Streaming for the SA Services and is mapped on Streaming Data Services as described in Section 2.4.2.2. (DEP.01)

The SYS Service Logic provides the following logical ports:

- SYS.01, which supports the SYS Services in the Personal Domain and is mapped on Personal Data Services, as described in Section 2.4.2.2 (DEP.01)

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.4.3.3.

The ISR data exchanged through SA.01, SA.04, BMS.01 and BMS.06 ports, should be according to the STANAGs referred in the NATO Standard ISR Library (STANAG 4559 /35/).
This standard is the result of the project MAJIIC2 which stands for Multi-Intelligence All-Source Joint Intelligence Surveillance and Reconnaissance Interoperability Coalition. The MAJIIC2 program is a multination program, formed by 9 NATO nations aiming to maximize the military use of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) resources. For that purpose, the MAJIIC2 program develops the tactics, techniques and procedures (TTPs) and the architecture and technical common data format to achieve that aim.
In the STANAG 4559 the following ISR products are defined:

- Imagery SAR, EO, IR (STANAG 4545 NSIF).
- GMTI – Ground Moving Target Indicator (STANAG 4607).
- Video (STANAG 4609).
- LINK 16 (STANAG 5516):
  - PPLIs (msg. J2.2, J2.3, J2.5).
  - Tracks (J3.0, J3.1, J3.2, J3.3, J3.5).
  - Tracks Management (J7.0, J7.1, J7.2, J7.3).
- CESMO:
  - ESM (STANAG 5516) (J3.7, J14.0, J14.2).
  - NEDB/EOB (STANAG 6009).
- HUMINT:
  - HUMINTREP (STANAG 2578 – AintP-5).
  - PENTAGRAM (STANAG 2433 – AintP-3).

- Exploitation Reports (xxEXREP):
  - STANAG 3377.
  - Targets Category (STANAG 3596).
  - Reliability and Credibility of Information Sources (STANAG 2511).
  - Country Codes (STANAG 1059).
- Intelligence Reports (STANAG 2511):
  - INTREP.
  - INTSUM.
- Intelligence Plans (STANAG 3277):
  - Intelligence Collection Plan (ICP).
  - Collection Task/Requirements List (CTL (/CRL)).
  - Collection and Exploitation Plan (CXP).
- Request For Information - RFI (STANAG 2149).
- ISR Request - ISRR (STANAG 2149).

As for the data to be exchanged through port SYS.01, intended to control RAS, STANAG 4586 /36/ is proposed, which defines the standard interfaces of UA control systems for NATO UA interoperability.

Unique ID	Type	Requirement Description
REQ-64	**CR**	STU Commander C4I Application shall provide a personal data interfaces described in Section 2.4.2.2 (DEP.01)
REQ-65	**OE**	STU Commander C4I Application shall provide a streaming data interfaces described in Section 2.4.2.2 (DEP.02)

Table 2-19 – DSS Personal Domain – C4I Application Port Requirements

2.4.6.4 C4I Application System to System Port Connectivity

The C4I Application which is serving an STU Commander, who acts in the Personal Domain exchange data with peers system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.01, which interconnects with:
  - The set of STU Commander Effectors to
    - Send Commands
    - Receive Data
  - The set of STU Commander Sensors to
    - Send Commands
    - Receive Data
- BMS.06, which interconnects with:
  - The set of STU Commander Sensors to:
    - Receive Streaming of live data, e.g. Video

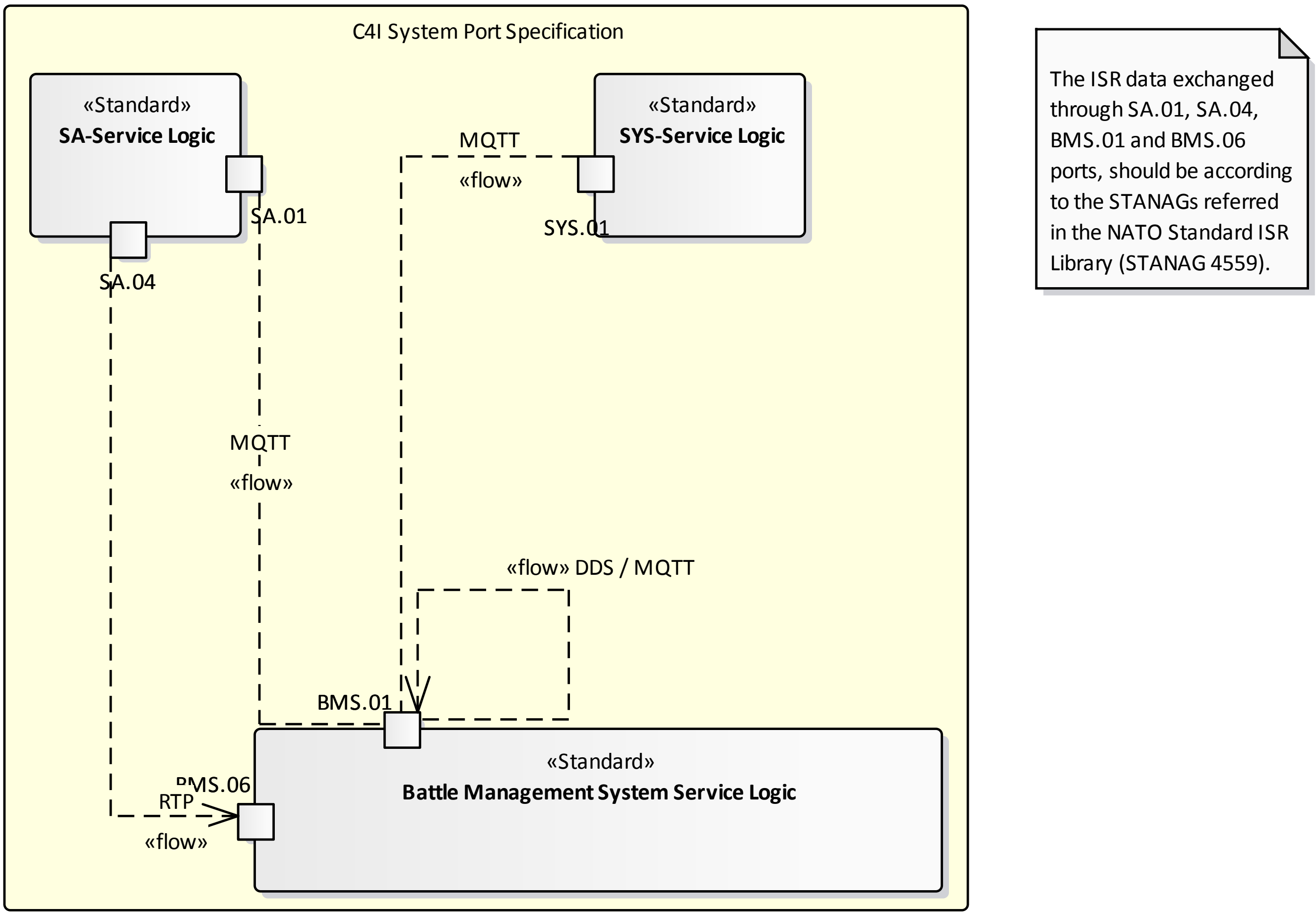
The SYS Service Logic component exchanges data via the following logical ports:

- SYS.01, which interconnects with:
  - The set of STU Commander Effectors to

        - Send Management Commands
        - Receive Status Data
    - The set of STU Commander Sensors to
        - Send Management Commands
        - Receive Status Data

The SA Service Logic component exchanges data via the following logical ports:

- SA.01, which interconnects with:
    - The set of STU Commander Sensors to
        - Send Commands
        - Receive Data
- SA.04, which interconnects with:
    - The set of STU Commander Sensors to:
        - Receive Streaming of live data, e.g. Video



The ISR data exchanged through SA.01, SA.04, BMS.01 and BMS.06 ports, should be according to the STANAGs referred in the NATO Standard ISR Library (STANAG 4559).

Figure 2-47 – System to System Port Connectivity C4I-Application

2.4.7 Sensors

2.4.7.1 Sensors Interface Description

As already described the DSS personal domain is separated into four core groups: torso, head, weapon and supporting devices. A sensor on the torso, head, and weapon belongs to the DSS and are therefore listed in this section. Data and Information exchange details are already described in sections 2.4.2.2, 2.5.2.2 and 2.6.2.1.1 and are therefore not repeated.

Concerning Sensors, the DSS domain is extremely heterogeneous and the market is already settled. Hence it is foreseeable that sensors may not provide full GOSSRA Compliance for the next years or some devices may never be compliant. Never the less it is important to integrate these legacy-systems into a GOSSRA-Compliant DSS. Thus, the following graphic introduces a legacy gateway.

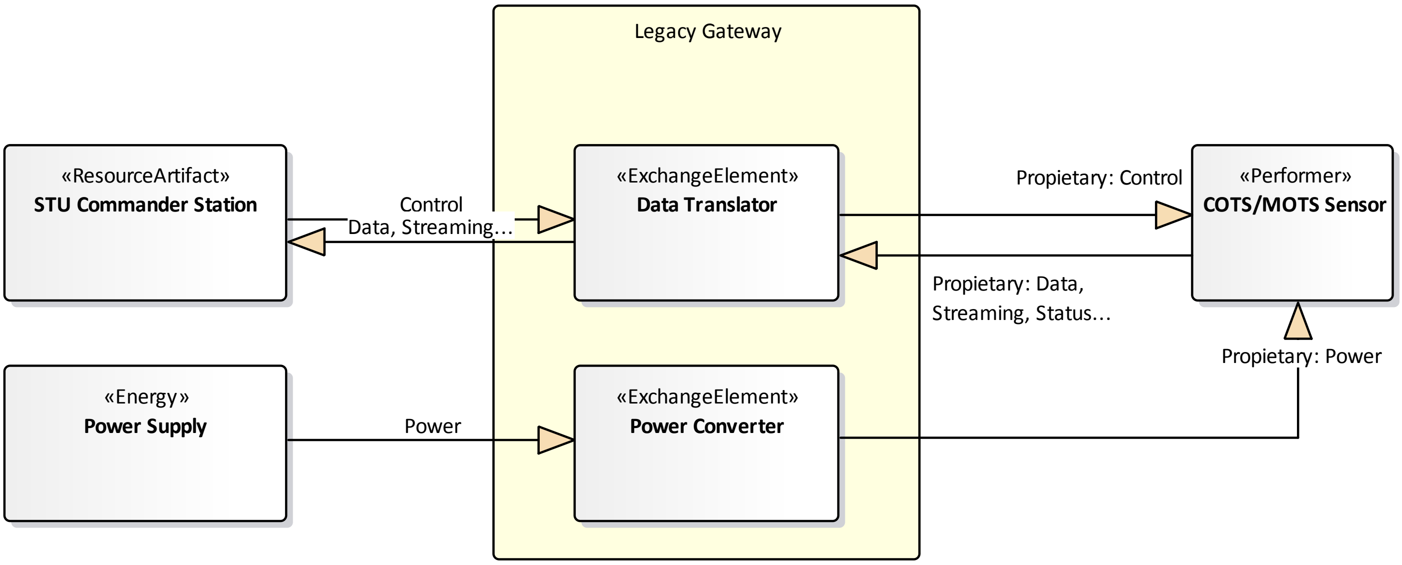


Figure 2-48 – Legacy Gateway

2.4.7.2 Sensors Port Specification

Due to the variety of sensors on the market, it is necessary to adapt the sensor interface on the common forms of the used transmission standards. It would be possible to request GOSSRA conform equipment to provide all data by a GOSSRA conform data model and exchange mechanism, but it is not practical. For example, a Bluetooth keyboard will use the HMI-Profile of Bluetooth with the correct drive suite on the torso side usually provided by the operating system. That way these devices can natively be integrated into the connected devices. These devices need to provide translator applications, which transform the information for GOSSRA.

The protocol stacks are specified in section 2.4.2.2.

DEP.06 defines the protocol stack for the exchange of custom data. For this reason, the RFCOMM profile of Bluetooth is used. The RFCOMM profile is usually realized by operating systems like Linux or Windows by creating a virtual serial connection which can be used as a transparent tunnel for information. From the sensor side, this information can either be GOSSRA conform or proprietary. **DEP.06** may also have a special format in which devices use the

RFCOMM-Profile with proprietary data structures/protocols. In this case, a Translator-Application shall translate the information to a GOSSRA conform format.

LEP.01 defines the protocol stack for the integration of the human interface devices in case the common Bluetooth HID Profile is used. The application is requested to transfer the submitted data to a GOSSRA conform format.

LEP.02 defines the protocol stack for the integration of the headsets or microphones in case the common Bluetooth Headset Profile is used. The application is requested to transfer the submitted data to a GOSSRA conform format.

DEP.05 defines the protocol stack for all other Bluetooth profiles as a placeholder in case another profile is used. The application is requested to transfer the submitted data to a GOSSRA conform format.

LEP.03 and LEP.04 are referring to the NFC communication and describe how NFC communication of sensors shall be used. They define the protocol stacks for common NFC usages in which the devices transmit proprietary messages. The application is requested to transfer the submitted data to a GOSSRA conform format.

LEP.03 may be enhanced by a protocol stack for the usage of NFC as a data transfer for custom messages compliant to GOSSRA. The application is requested to transfer the submitted data to a GOSSRA conform format.

DEP.03 defines the protocol stacks for common USB-Devices. The operating system of the USB-Host will provide functionalities such as a keyboard that is connected to the bus. This ensures, that every common USB-Device can be connected to the Bus and used in a common manner. That way the implementation effort is reduced and COTS/MOTS devices can be used indirectly. To provide this information to other participants in the GOSSRA network a translator application is necessary. Providing the information to the GOSSRA network is extremely important, since another application in the network may need to use the devices (here the keyboard) to for example of two displays with a separate computer are used.

DEP.04 defines the real protocol stack of GOSSRA with the GOSSRA conform data format.

2.4.7.3 Sensors System to System Port Connectivity

Several sensors can be a source for a video signal. All video-sources that actually stream video to the DSS shall be connected via DEP.03 port wire since the defined wireless standards are not sufficient to stream video. Some video sources may only record the video and store it on internal storage. In this case, it is possible to connect the video sources wireless and only control their functionality via DEP.04 port.

COTS/MOTS audio devices such as headsets may be connected via Bluetooth. In this case, these devices shall use the LEP.02 profile.

COTS/MOTS audio devices such as headsets may be connected via Bluetooth. In this case, these devices shall use the LEP.01profile

External gateways are used to exchange information with external systems such as Unattended Ground Sensor Networks, UAVs or UGVs. These devices shall be connected via DEP.04 port and, due to the fact that they are actually defined for GOSSRA, shall interconnect with GOSSRA on its native interface. By this, the information provided by the external system is available to all participants in the GOSSRA network.

2.4.7.4 Example of port usage

Usage of the described ports is critical and ports need to be carefully chosen. Devices should use common profiles of the defined standards e.g. Bluetooth-HSP for headsets. That way even COTS-Equipment is interchangeable and no special GOSSRA-Equipment is needed. This improves the market situation and reduces integration costs.

Figure 2-49 shows an example configuration of a soldier system consisting of a GNSS-Receiver, End-User-Device, LRF and a Headset. Figure 2-50 shows how these devices are connected to the End-User-Device which is used as the USB-Host, Bluetooth-Host (optional) and NFC-Host (optional). The EUD is the USB-Host handling all connection with its driver suite supported by the OS. The GNSS, as common, opens a virtual serial connection in the operating system using a common USB-Profile on which it provides NMEA 0183 Strings. This information is converted by a Translator application and can be supplied to other systems using the system bus. The headset is connected via Bluetooth using the common Bluetooth HSP-Profile. A translator app converts the audio stream to a GOSSRA compliant manner. This way the Headset, as well as the GNSS-Receiver, are replaceable since any other MOTS/COTS Device will serve these interfaces, too. The LRF is connected via Bluetooth as well and uses a proprietary protocol to provide information to the system. This protocol is vendor-specific and not standardized. A translator app converts the received information to be available in the information space.

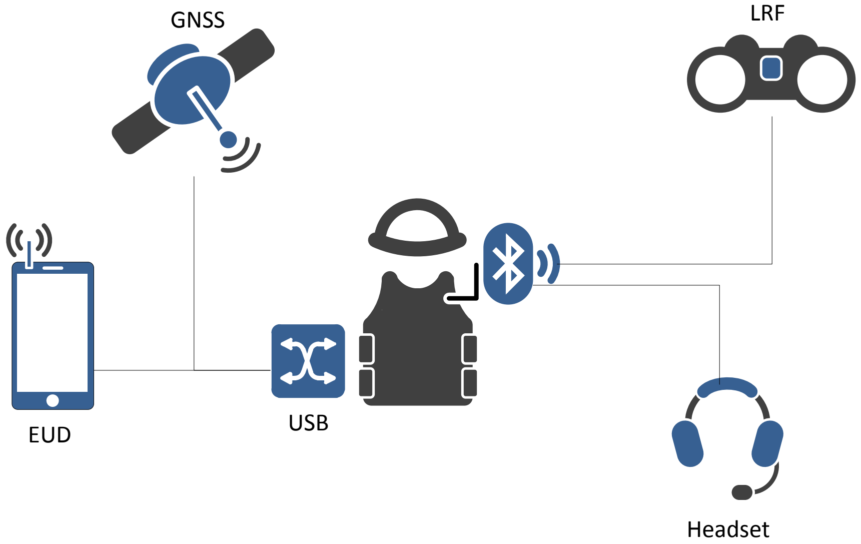


Figure 2-49 – Example configuration of peripherals for a basic dismounted soldier system

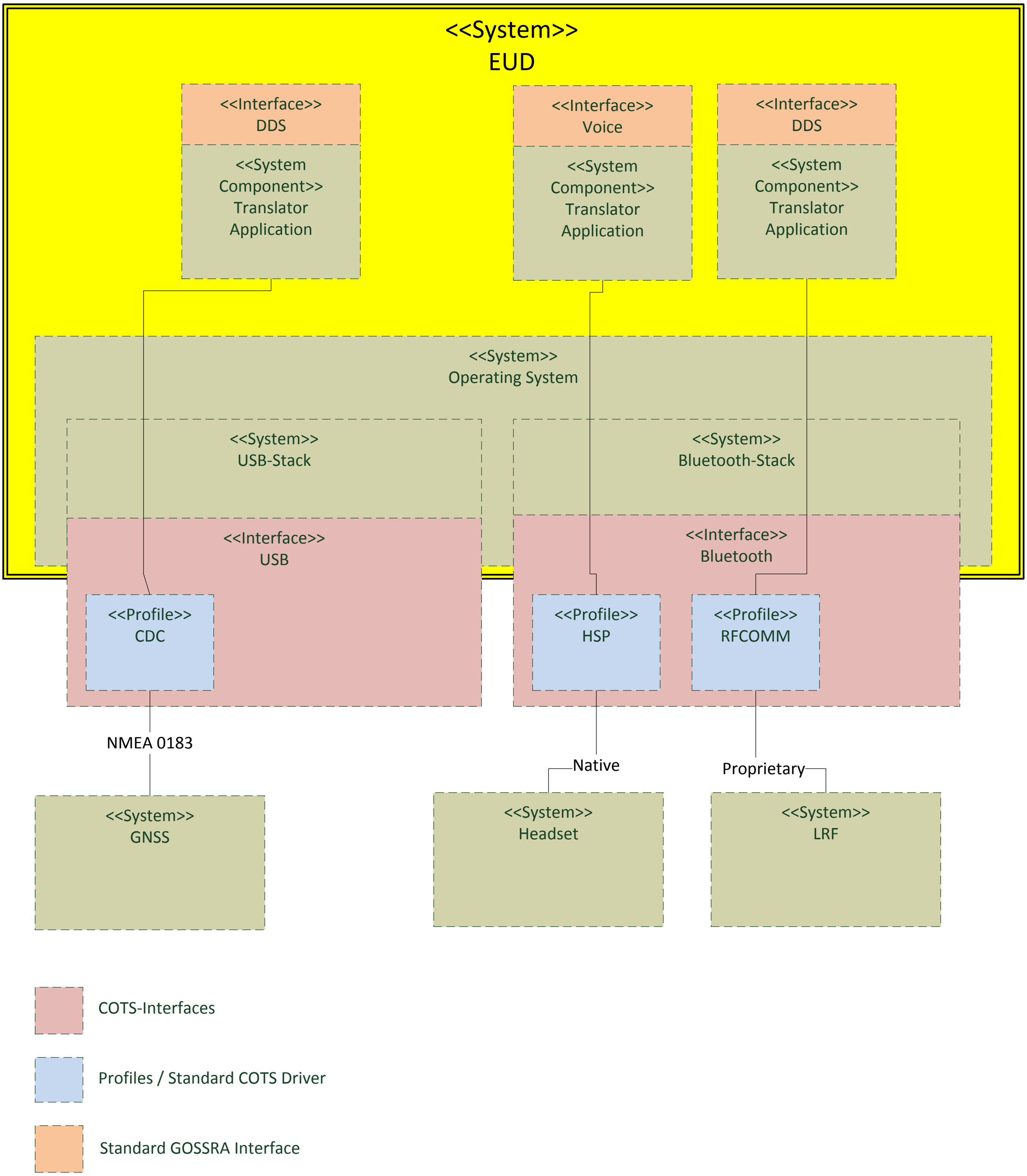


Figure 2-50 – Example configuration of peripherals for a basic dismounted soldier system – Communication View

Figure 2-51 shows an enhanced soldier system, on which a bodycam, NBC-Sensor, Fire Control and access to an unattended ground sensor network were added.

Figure 2-52 shows the communication view for the enhanced soldier system. The devices introduced in Figure 2-50 did not change. The bodycam is attached as a standard USB-Camera, its video stream is converted to a GOSSRA compliant format. The UGS-Gateway, Fire Control, and the NBC-Sensor are all GOSSRA-Compliant devices using MQTT for data exchange. They can all be served by one MQTT/DDS-Converter that basically just converts between the two exchange mechanisms. More advanced components such as the UGS-Gateway may directly use DDS to provide their information to the system.

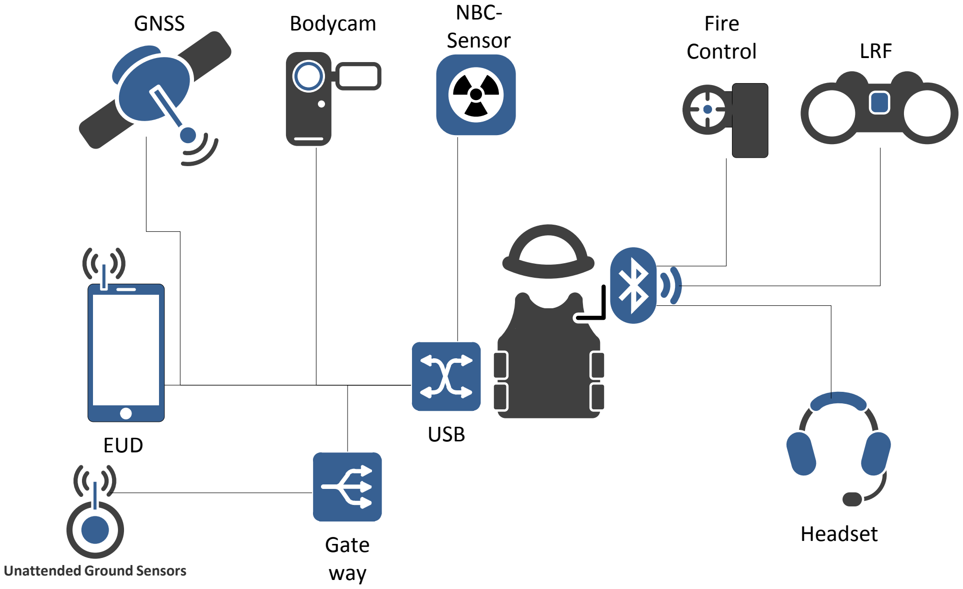


Figure 2-51 – Example configuration of peripherals for an enhanced dismounted soldier system

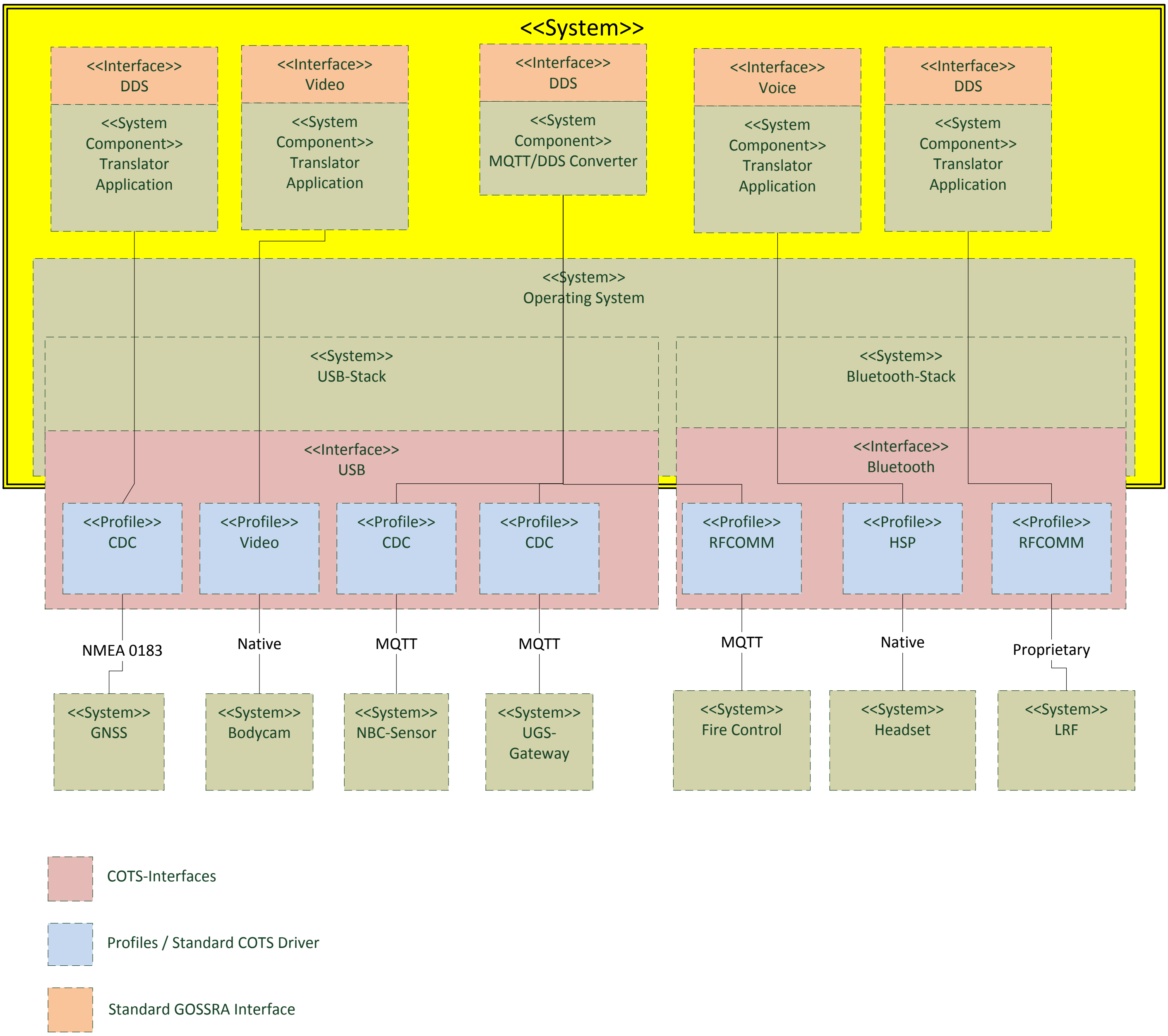


Figure 2-52 – Example configuration of peripherals for an enhanced dismounted soldier system – Communication View

Figure 2-53 shows a soldier system with an NFC interface, on which a second EUD and a Bio-Sensor were added.

Figure 2-54 shows the communication view for the enhanced soldier system. The devices introduced in Figure 2-50 did not change. Both devices are connected via NFC but use different ports.

The second EUD is connected via LEP.04 (LLCP) to allow a bidirectional data flow, which is the main purpose of LEP.04. This could be useful to connect e.g. a tablet without a connector to the harness. Besides LEP.04 also LEP.03 is capable of handling peer-to-peer communication and may be used as well for this purpose.

The Bio-Sensor is connected via LEP.03, since it may only serve as a data provider. LEP.03 may also be used to interface with NFC-Tags or other sensors.

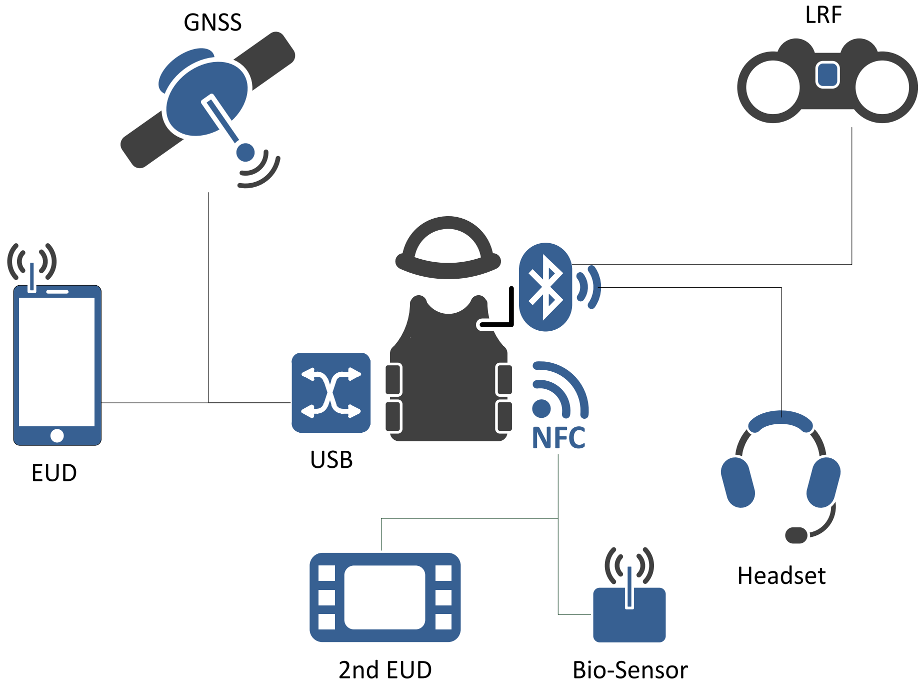


Figure 2-53 – Example configuration of peripherals for a dismounted soldier system with NFC

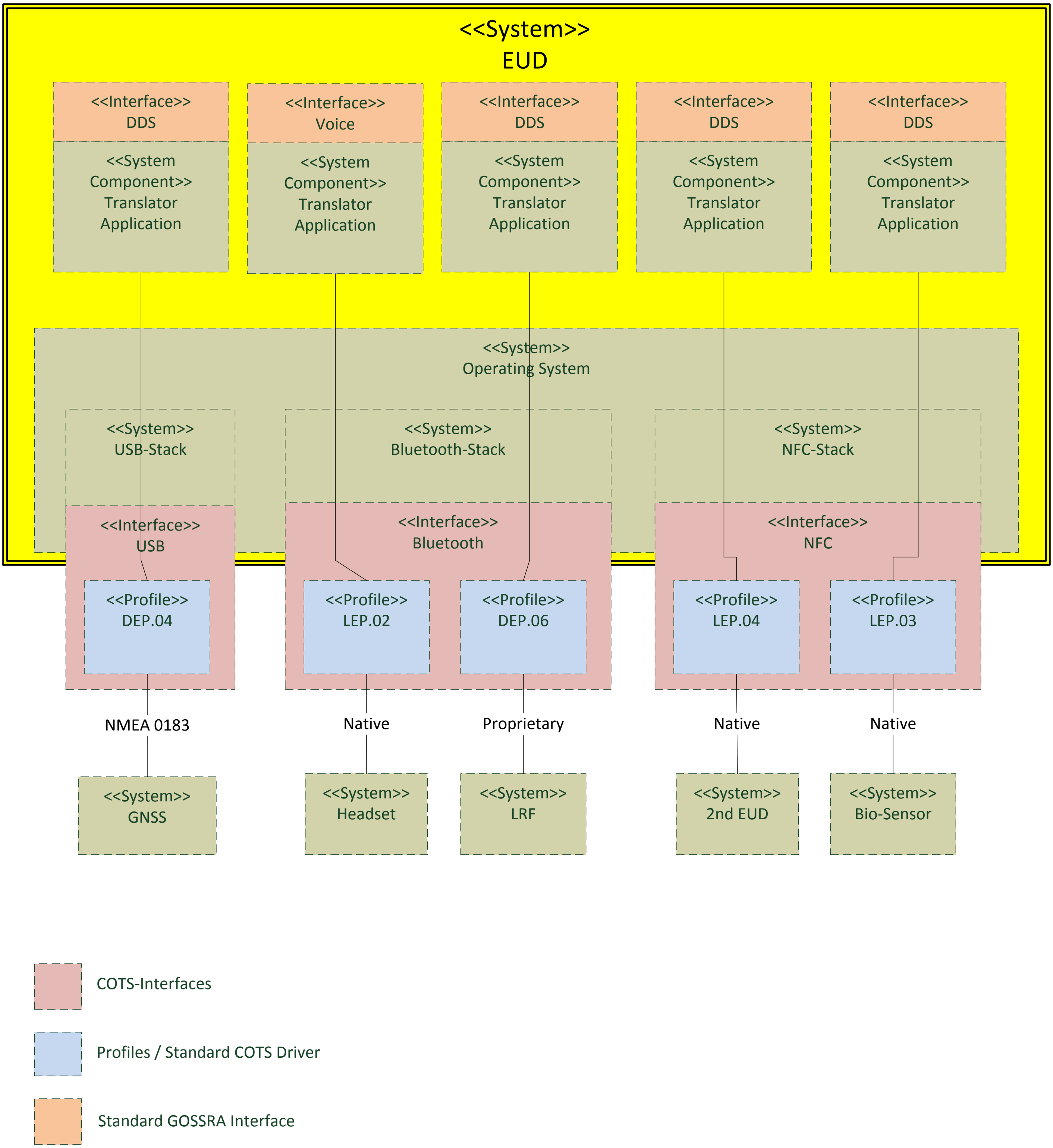


Figure 2-54 – Example configuration of peripherals for a dismounted soldier system with NFC – Communication View

2.4.7.5 Protocol Stack identification

Since different protocol stacks are used on one data bus it is critical to decide, which one needs to be used.

This is easy e.g. for LEP.02 and LEP.03 since Bluetooth handles the access, but is complicated for the data transfer. In case of the usage of Publish/Subscribe mechanism the underlying protocol will identify, what is used, but considering e.g. DEP.06 identification is up to the translator applications. DEP.06 will create a virtual com-port on the host system for every connected device. The devices provide the data in their proprietary protocol, which may contradict other proprietary protocols. So a translator application needs to connect to these ports and identify if it connected to the correct device. Since the protocols may contradict a request/response scheme may not be feasible. Hence, sending e.g. a version request to a device and waiting for a response may lead to malicious system behaviour. Since these devices are usually no standard devices their integration into every system needs special measures.

Regarding the different forms of devices, two device types can be differentiated. Those that send cyclic information and those that do only send information on an event.

For both devices, the translator application needs to be robust enough to handle malicious traffic without crashing.

Devices with cyclic information can be identified by analysing the information grabbed from the ports. The translator application connects cyclic to open ports (one at a time) and listens for correct data. Commonly the data transferred are accommodated by framing and/or checksums etc. All data passing the parser of the translator application successfully should be valid data. The system integrator shall identify and handle contradicting protocols.

Devices that only submit data on an event need a paring method. In this case, the translator application connects to all open ports. The HMI shall request the user to perform the pairing procedure, on which the device will send a message to the translator application. The translator application can identify the correct port of the device.

2.4.8 Effectors

2.4.8.1 Effectors Interface Description

This view considers the Dismounted Soldier Personal Domain and the Small Tactical Unit Domain. The latter is considered as some of the effectors (e.g. Grenade Launchers) might be managed only by members of the team with specific roles (e.g. sniper). Higher-order domains (Inter-platform Domain, Joint Domain, and Coalition Domain) are neglected. The indirect relationship which might be established through the exchange of information with higher-order domains shall be addressed through the interface of the effectors with the C4I services.

In this paragraph, the different devices that provide effectors services are described together with their interfaces.

In this Figure 2-55 possible parts of a weapon are listed and it is shown how they operate together with the DSS. The following chapters further explain the relations and functions.

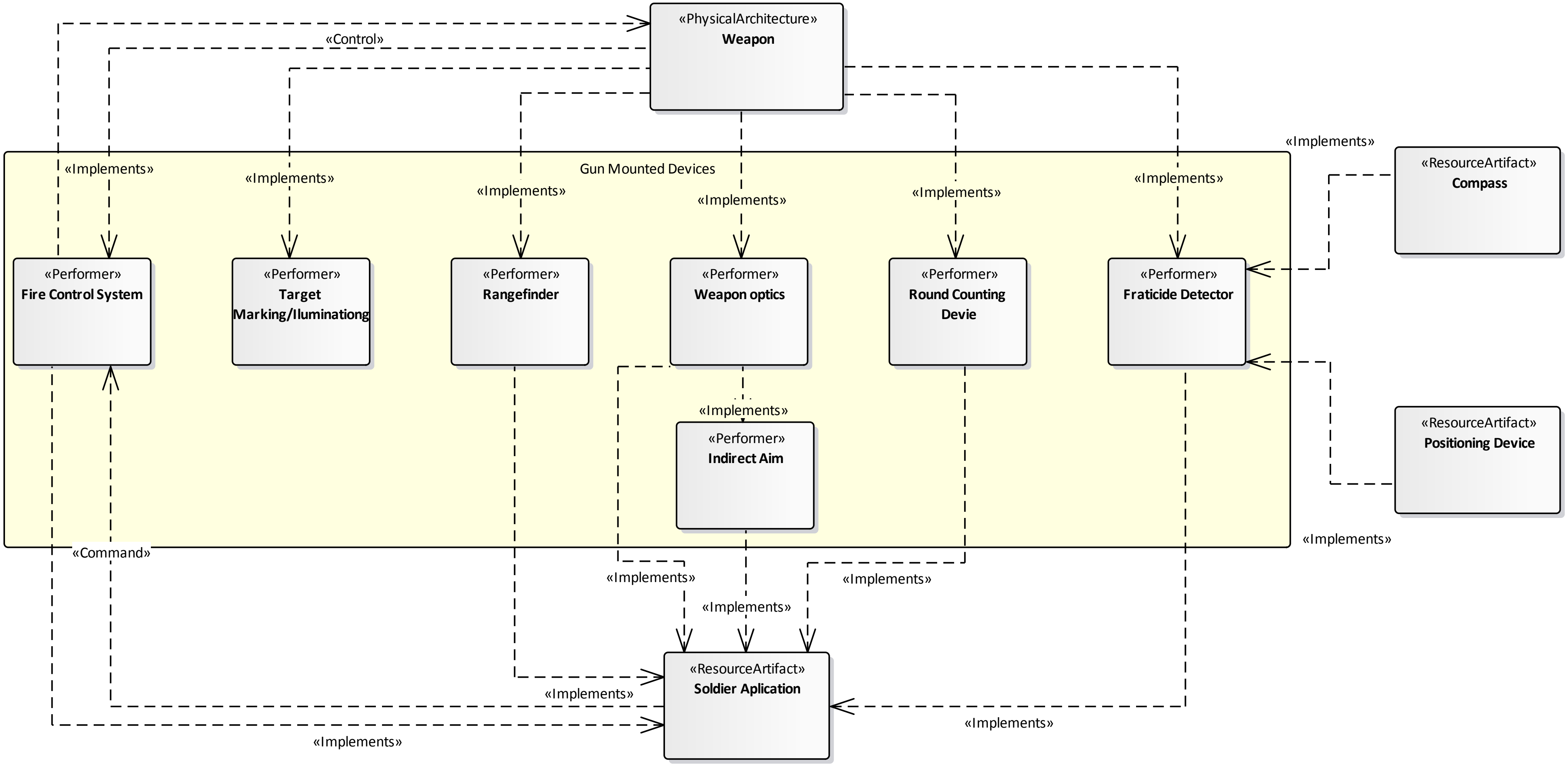


Figure 2-55 – Effectors Interface Description

2.4.8.1.1 Target Surveillance

The functional service **Target Surveillance** provides devices/tools to enhance DSS vision capabilities under all visibility conditions (day, night and poor visibility conditions). In this section, only sensors attached to the weapon are addressed. Sensors located in other places (e.g. helmet-mounted sensors) are addressed in the Sensors Interface Description.

This service is usually accomplished by a Weapon Optical Device, which comprises the following kind of sensors:

Intensified weapon sight: This is the equivalent of Night Vision Goggles, which intensifies the upcoming light in the visible wavelength range when its intensity is very low. They can only be used in night conditions. They are usually used as stand-alone equipment, due to their high resolution and good SwaP characteristics and their image are not usually digitized to be transmitted. They usually do not require control. Power is usually supplied by primary batteries (not rechargeable).

Thermal weapon camera: They detect the electromagnetic radiation in the wavelength of the infrared range. They can be used not only in night conditions but also in day conditions when the transmission of visible light may be hindered by substances like smoke. Being a camera allows them to provide images in analogue or digital form, and also to be controlled usually by an RS-232 interface. Power is usually supplied by secondary batteries (rechargeable).

Both kinds of components share a mechanical interface with the weapon.

2.4.8.1.1.1 Target Acquisition

The functional service **Target acquisition** provides devices/tools to detect, recognise and identify targets in the battlespace or to locate the identified targets and enrich them with further relevant information.

This function may be accomplished by the devices described under Target Surveillance and Range Finding.

2.4.8.1.1.2 Target Damage Assessment

The functional service **Target Damage Assessment** provides devices/tools to evaluate battle damage caused to a target after its engagement.

This function may be accomplished by the devices described under Target Surveillance and Range Finding.

2.4.8.1.2 Target Engagement

The functional service **Target engagement** provides devices/tools to engage targets with the required effect (e.g. suppression of the enemy) and to engage targets with maximum hit probability.

This service may be accomplished by following stand-alone components:

Weapon and ammunition.

Fire Control System. The soldier itself introduces in the system the parameters provided to him by services such as Range Finding or meteorological data.

The following picture displays the relationship between both components.

2.4.8.1.2.1 Handling Weapon

Typical activities of the operational service **Handling Weapon** are the preventive maintenance, preparation of ammunition and the correct use of weapons and their fire control system.

This service refers to handling effectors in general so it is not fulfilled by any concrete component of the system.

2.4.8.1.2.2 Ammunition Programming

The functional service **Ammunition Programming** provides devices/tools to set the fuze of programmable ammunition to explode at the desired point of the trajectory.

This functionality is performed on the ammunition itself, so it is an independent service.

2.4.8.1.2.3 Target Marking/Illumination

The functional service **Target marking/illumination** provides devices/tools to mark or illuminate targets to engage.

This functionality is usually performed by laser markers or illuminators in different wavelength ranges, with power supply from batteries, so the only interface to the soldier is the mechanical interface to the weapon.

2.4.8.1.2.4 Indirect Aiming

The functional service **Indirect Aiming** (also named Corner Aiming) provides devices/tools to aim the weapon at the target to be engaged without exposure or minimum exposure to enemy fire. This is usually accomplished by the transmission of the image captured by the devices employed for Target Acquisition to the Head Mounted Display.

2.4.8.1.2.5 Fratricide Alert

The functional service **Fratricide Alert** provides devices/tools to warn the soldier of potential blue fire when aiming his/her weapon towards the location of a member of his/her squad/team.

This alert gets information from the Bearing Finding service and Position/ Location Sensors and sends it to the Application HMI.

Fratricide Alert is considered only as a warning given to a combatant when another member of the same unit or net is within the aiming sector of his own weapon. This, of course relies on a wearable C4I system at a given tactical level where location of every single member of the unit connected to the same net is perfectly known by each other thanks to GNSS devices. Fratricide Alert functionality contributes to force protection by reducing the risk of fratricide taking advantage of blue force tracking capability. In no way this functionality can be taken as a CID system where more complex devices and procedures would apply with the aim of avoiding blue killing.

2.4.8.1.3 Operational Measurements

The functional service **Operational Measurements** provides devices/tools:

- to measure relevant parameters that have a direct effect on combat efficiency and force protection (fratricide alert)

2.4.8.1.3.1 Round Counting

The functional service **Round Counting** provides devices/tools to give the soldier an account of the remaining rounds in the soldier’s weapon magazine.

2.4.8.1.3.2 Range Finding

The functional service **Range Finding** provides devices/tools to measure the distance between the soldier’s weapon and the potential target.

This is accomplished by a Laser Range Finder.

2.4.8.1.3.3 Bearing Finding

The functional service **Bearing Finding** provides devices/tools to measure the azimuth and elevation angles between DSS’s weapon and a potential target.

This is accomplished by a Digital Magnetic Compass, which is usually embedded in the Laser Range Finder device (see paragraph above).

2.4.8.1.4 Data Exchange

The functional service **Data Exchange** provides devices/tools to exchange relevant data to and from DSS’s weapon and DSS’s C2I subsystems

This service is described in each of the related devices in the paragraphs above.

2.4.8.1.5 Power Management

The functional service **Power Management** provides devices/tools to feed the DSS’s weapon electronic devices directly from the DSS’s power subsystem or to recharge DSS’s weapon central battery.

This service is described in each of the related devices in the paragraphs above and is allocated in the mentioned devices.

2.4.8.1.6 System Management

The functional service **System Management** provides devices/tools:

- to configure the array of electronic devices integrated/installed on the DSS’s weapon
- to control functionalities of the electronic devices integrated/installed on the DSS’s weapon (video channel, polarity, video transmission, etc)
- to control radio voice activation from the weapon without separating hands from the DSS’s weapon

This service is described in each of the related devices in the paragraphs above and is allocated in the mentioned devices.

2.4.8.1.7 Imaging

The functional service **Imaging** provides devices/tools to capture and transmit video from the DSS’s weapon or to capture and transmit fix pictures from the DSS’s weapon

This service is described in each of the related devices in the paragraphs above and is allocated in the mentioned devices.

2.4.8.2 Effectors Port Specification

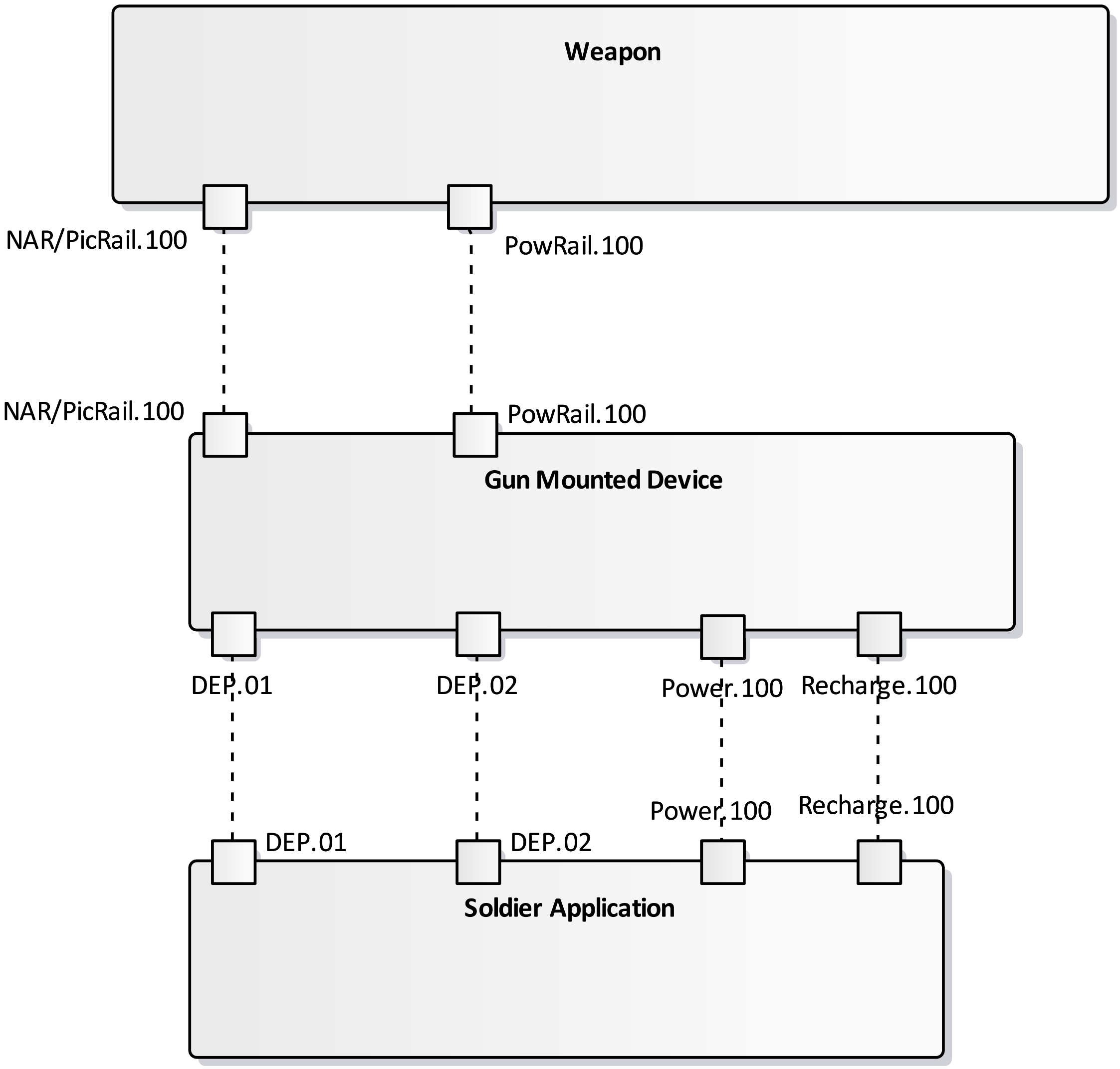


Figure 2-56 – Effectors Port Specification

2.4.8.2.1 Weapon Optical Device

The paragraphs below specify the set of ports provided by Weapon Optical Devices.
Mechanical interfaces:

- **Weapon Optical Device_NAR/PicRail.100.** This interface is a mechanical adapter to fix the device to the NATO Accessory Rail defined by STANAG 4694 or Picatinny Rail defined by MIL-STD 1913. It allows mechanical linkage to the weapon and homogenization of the line of sight.

Power interfaces:

Possible other

- **Weapon Optical Device_Power.100.** This port allows power supply to the device, and is based on the following protocols:
  - Power2wire
- **Weapon Optical Device_Recharge.100.** This port allows the charge of the secondary batteries of the device and is based on the following protocols:
  - 4wire
  - SMBUS

Mechanical and power interfaces:

- **Weapon Optical Device_PowRail.100.** This interface is an adapter to fix the device to a Powered Rail defined in STANAG 4740, which not only provides fixture to the device but also supplies power.

Data interfaces:

- **Weapon Optical Device_Wired.100.** This port allows wired communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.
- **Weapon Optical Device_Wireless.100.** This port allows wireless communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.

2.4.8.2.2 Weapon

The paragraphs below specify the set of ports provided by Weapon.

Mechanical interfaces:

- **Weapon_NAR/PicRail.100.** This interface is the NATO Accessory Rail defined by STANAG 4694 or Picatinny Rail defined by MIL-STD 1913. It allows mechanical linkage to the devices mounted on the weapon.

Mechanical and power interfaces:

- **Weapon Optical Device_PowRail.100.** This interface is an extension (STANAG 4740) of the NATO Accessory Rail defined by STANAG 4694 to allow also power supply from a stack of secondary batteries. Some versions of the rail allow a low rate of wireless transmission but this option is not considered as wireless transmission is already addressed by a dedicated port of the device.

2.4.8.2.3 Fire Control System

The paragraphs below specify the set of ports provided by the Fire Control System.

Mechanical interfaces:

- **Fire Control System_NAR/PicRail.100.** This interface is a mechanical adapter to fix the device to the NATO Accessory Rail defined by STANAG 4694 or Picatinny Rail defined by MIL-STD 1913. It allows mechanical linkage to the weapon.

Power interfaces:

- **Fire Control System_Power.100.** This port allows power supply to the device, and is based on the following protocols:
  - Power2wire
- **Fire Control System_Recharge.100.** This port allows the charge of the secondary batteries of the device, and is based on the following protocols:
  - 4wire
  - SMBUS

Mechanical and power interfaces:

- **Fire Control System_PowRail.100.** This interface is an adapter to fix the device to a Powered Rail defined in STANAG 4740, which not only provides fixture to the device but also supplies power.

Data interfaces:

- **Fire Control System_Wired.100.** This port allows wired communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.

2.4.8.2.4 Target Marking/Illumination

Target marking and illumination devices include torches, laser pointers, etc. which usually are stand-alone device with independent power supply through own batteries.

The paragraphs below specify the set of ports provided by this component.

Mechanical interfaces:

- **Target Marking Ilumination_NAR/PicRail.100.** This interface is a mechanical adapter to fix the device to the NATO Accessory Rail defined by STANAG 4694 or Picatinny Rail defined by MIL-STD 1913. It allows mechanical linkage to the weapon.

2.4.8.2.5 Fratricide Alert Device

Fratricide Alert Device is a device that gets the data from the bearing sensors and the relative positions of the soldier and the rest of the members of the STU to warn through an HMI device when aiming at blue forces. This device can also be integrated with some other electronic equipment mounted on the weapon.

The paragraphs below specify the set of ports provided by this component.

Mechanical and power interfaces:

- **Fratricide Alert Device_PowRail.100.** This interface is an adapter to fix the device to a Powered Rail defined in STANAG 4740, which not only provides fixture to the device but also supplies power.

Data interfaces:

- **Fratricide Alert Device_Wired.100.** This port allows wired communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.
- **Fratricide Alert Device_Wireless.100.** This port allows wireless communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.

2.4.8.2.6 Round counting device

Round counting device is a stand-alone device with independent power supply and HMI display. It keeps a track of the shots and warns when the cartridge is below some threshold.

The paragraphs below specify the set of ports provided by this component.

Mechanical interfaces:

- **Round Counting Device_NAR/PicRail.100.** This interface is a mechanical adapter to fix the NATO Accessory Rail defined by STANAG 4694 or Picatinny Rail defined by MIL-STD 1913. It allows mechanical linkage to the weapon.

2.4.8.2.7 Laser range finder

The paragraphs below specify the set of ports provided by this component.

Mechanical and power interfaces:

- **Laser Range Finder_PowRail.100.** This interface is an adapter to fix the device to a Powered Rail defined in STANAG 4740, which not only provides fixture to the device but also supplies power.

Data interfaces:

- **Laser Range Finder_Wired.100.** This port allows wired communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.
- **Laser Range Finder_Wireless.100.** This port allows wireless communication and control of the device, and is based on the following protocols defined in section 2.4.2.2.

2.5 STU Domain

2.5.1 Electronic Components

2.5.1.1 Electronic Components Interface Description

In this group are the external systems that exchange data with the DSS, for this exchange the system provides external interfaces, which can be wired or wireless depending on the needs.

In the case of wireless interfaces, the system in its *basic* minimum configuration has a radio that will allow this type of exchange but other possibilities are considered, such as the exchange of data with vehicles through cable, communications with another soldier in joint actions or communications inter-squad and intra-squad - data and voice.

As "Off-board" pertains to the interfaces of the DSS with STU, vehicle, platform, joint and coalition forces, the description is provided in section 2.8.4.1.

2.5.2 Data Exchange Services

2.5.2.1 Data Exchange Services Interface Description

The figure below depicts the main components and related interconnection of the Data Exchange Services, which serve a Soldier acting in the STU Domain.

The Data Exchange Protocol components allocated on different DSS Nodes or shared remote peripherals, e.g. UxV, interact to supports the data exchange among:

- The STU Commander Application Services Logic and Service Logics of the set of DSS nodes that compose the Squad.
- The Soldier Application Services Logic and the Remote Peripheral Service Logic.

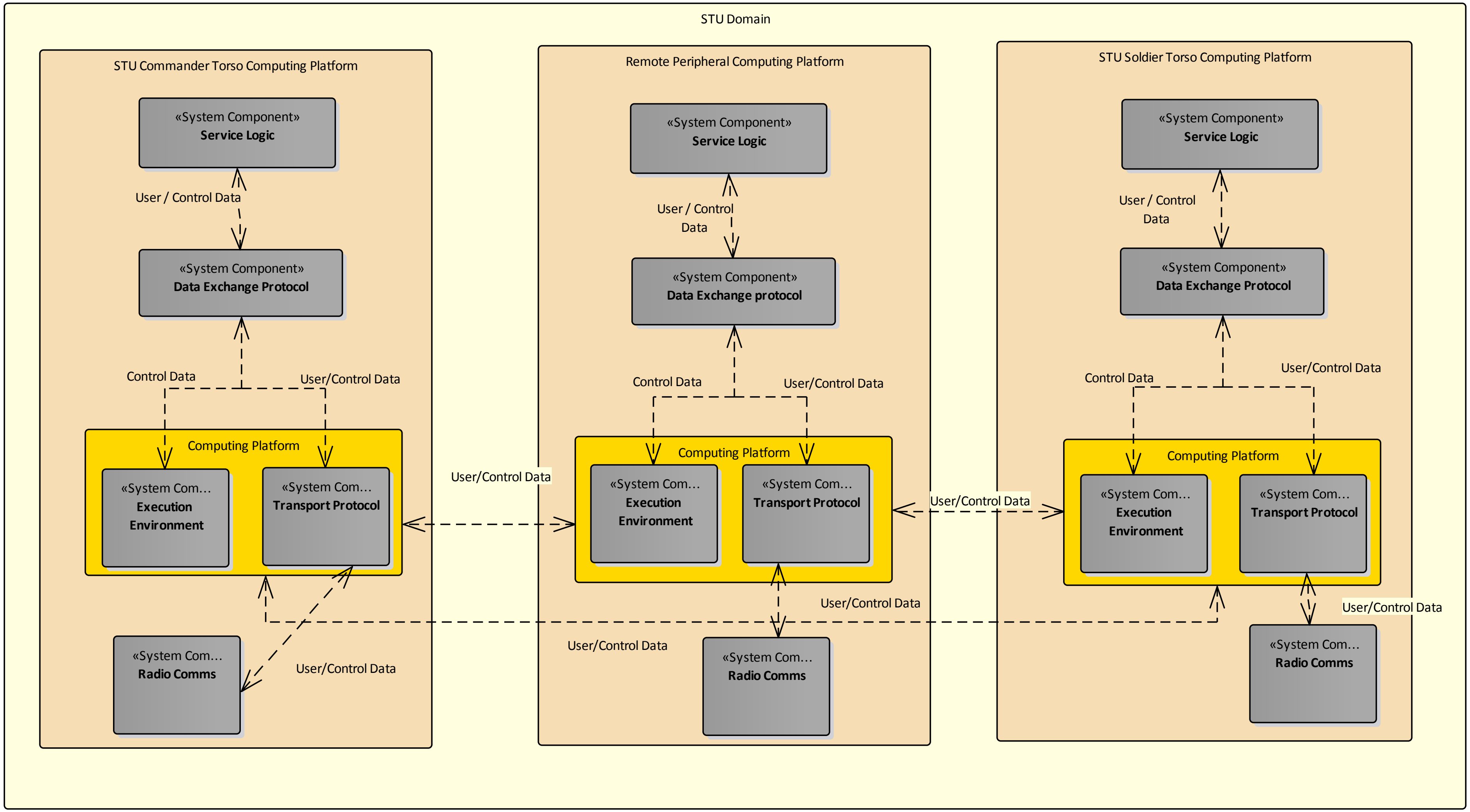


Figure 2-57 – STU Domain – Squad Data Exchange Services

2.5.2.2 Data Exchange Services Port Specification

The Data Exchange Protocol (DEP) component provides the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the STU Domain;
- Required Port, which requests services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the STU Domain are:

- Offered Ports:
    - DEP.11: STU Data Services, which provides services for exchanging data among the STU Nodes and between a DSS Node and the related shared peripherals, e.g. UxV.
    - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio, among the STU Nodes and between a DSS Node and the related shared peripherals, e.g. UxV.
    - DEP.12: Tactical Data Services, which provides for exchanging tactical data among the STU Nodes and between a DSS Node and the related shared peripherals, e.g. UxV.
    - DEP.15: File Transfer, which provides for the transmission of a file, e.g. an Image, among the STU Nodes and between a DSS Node and the related shared peripherals, e.g. UxV.
    - DEP.16: Tactical File Transfer, which provides for File Transfer service on Tactical Data Link.
- Required Ports:
    - DEP.13: Radio Services, which request for transport of data/streaming among the STU radio network endpoints.
    - DEP.14: Tactical Radio Services, which request for transport of tactical data among the STU radio network endpoints.
    - DEP.05: Execution Platform API, which requests for services supporting the execution of the DEP threads.

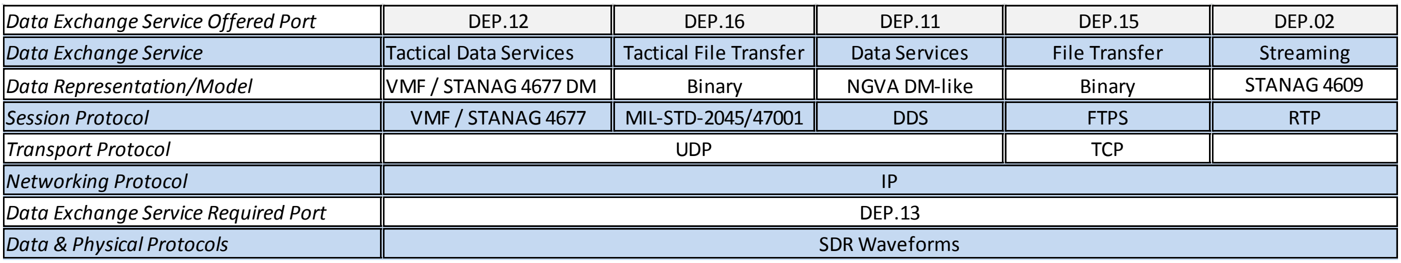
Each logical port is supported by an appropriated protocol stack as described below:

- DEP.11 provides the API for STU **Data Services** with middle to high band scenarios. The following protocols are a candidate to implement the Data Session Protocol:
    - Data Distribution Services for Real-Time Systems[/20/, /21/, /22/,/23/]
- DEP.02 provides the API for **Streaming Data Services**. The following protocols are a candidate to implement the Streaming Session Protocol:
    - Real-time Transport Protocol (RTP) [/24/].
    - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]
- DEP.12 provides the API for **Tactical Data Services** based on the protocol stack depicted in Figure 2-58 and Figure 2-59 for Narrow Band scenarios. The following protocols are a candidate to implement the Tactical Data Protocol for DEP in the STU Domain:
    - Joint Dismounted Soldier System Interoperability Network (JDSSIN) [/13/,/14/,/15/,/16/,/17/]
    - Variable Message Format [/25/]

- DEP.15 provides the API for **File Transfer Services**. The following protocols are a candidate to implement the File Transfer Services:
  - File Transfer Protocol Secure (FTPS) [/27/, /28/]
- DEP.16 provides the API for **Tactical File Transfer**. The following protocols are a candidate to implement the File Transfer Services:
  - Variable Message Format [/25/, /26/]
- DEP.13 requires for Radio Services in an STU radio area network.
- DEP.14 requires for Tactical Radio Services in an STU tactical radio area network, which does not provides for any IP networking services.
- DEP.05 requires for Execution Environment Services, it is mapped on the API of the Execution Environment provided by the hosting computer platform.

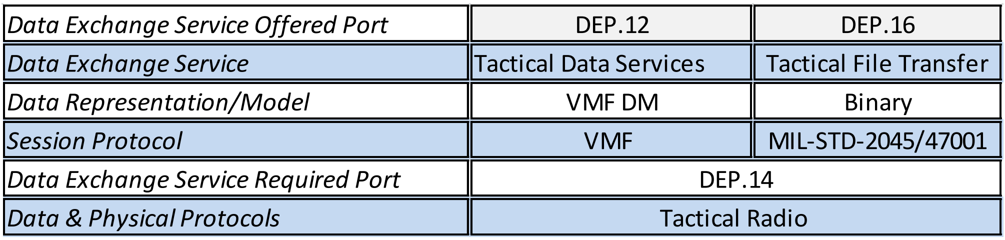
Figure 2-58 summarizes the Data Exchange Services protocol stacks in this domain.

Figure 2-59 summarizes the Data Exchange Services protocol stacks in this domain for the narrowband radio network.



Data Exchange Service Offered Port	DEP.12	DEP.16	DEP.11	DEP.15	DEP.02
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Streaming
Data Representation/Model	VMF / STANAG 4677 DM	Binary	NGVA DM-like	Binary	STANAG 4609
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	RTP
Transport Protocol	UDP			TCP	
Networking Protocol	IP				
Data Exchange Service Required Port	DEP.13				
Data & Physical Protocols	SDR Waveforms				

Figure 2-58 – NSV-2a STU Data Exchange Services Protocol Stack



Data Exchange Service Offered Port	DEP.12	DEP.16
Data Exchange Service	Tactical Data Services	Tactical File Transfer
Data Representation/Model	VMF DM	Binary
Session Protocol	VMF	MIL-STD-2045/47001
Data Exchange Service Required Port	DEP.14	
Data & Physical Protocols	Tactical Radio	

Figure 2-59 – NSV-2a STU Data Exchange Services Protocol Stack for over Tactical Protocol directly deployed on Radio Network (No IP Networking)

2.5.2.3 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component which is serving DSS Nodes, who act in the STU Domain exchange data with other DSS system nodes and Remote Peripherals as specified below.

The Data Exchange Protocol component provides services via the following logical ports:

- DEP.11, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive User Data and Service Control Data
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive User Data and Service Control Data
- DEP.12, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive Tactical Data and Service Control Data
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive Tactical Data and Service Control Data
- DEP.02, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send Streaming Data
        - Send / Receive Service Control Data
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Receive Streaming Data
        - Send / Receive Service Control Data
- DEP.15, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive files
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive files
- DEP.16, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive files on the tactical transport protocol
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive files on the tactical transport protocol

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.13, which interconnects with:
    - Radio Services serving the STU Domain, to:
        - Send / Receive User Data, Streaming Data, and Service Control Data, Files
- DEP.14, which interconnects with:
    - Tactical Radio Services serving the STU Domain, to:
        - Send / Receive Tactical Data, and Files
- DEP.05, which interconnects with:
    - Execution Environment API, to:
        - Send / Receive Service Control Data

2.5.3 Soldier Application

2.5.3.1 Soldier Application Interface Description

The figure below depicts the main components and related interconnection of a Soldier Application, which equips Specialist Soldier who acts in the STU Domain.

This diagram highlights the capability for a Specialist Application to request for Services to a Commander Application. In this interaction, the Specialist Application Service Logic acts as Consumer of Services provided by the Commander Application Service Logic.

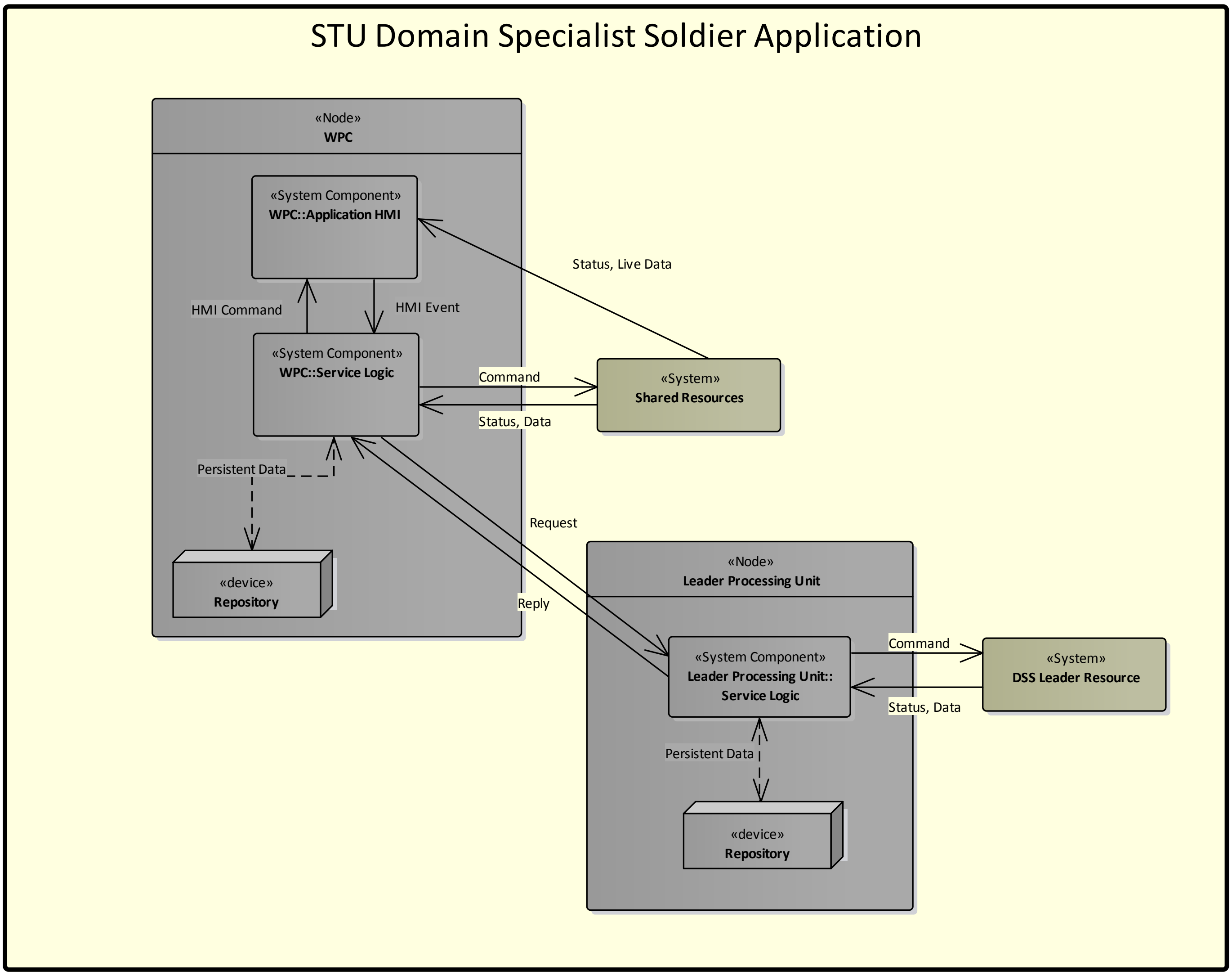


Figure 2-60 – STU Domain - Specialist Soldier Application

Unique ID	Type	Requirement Description
REQ-66	**OE**	The Commander Application should allow a Specialist Application to request for Services, which are not natively available at a Specialist computer platform.

Table 2-20 – DSS Personal Domain - Specialist Application Requirements

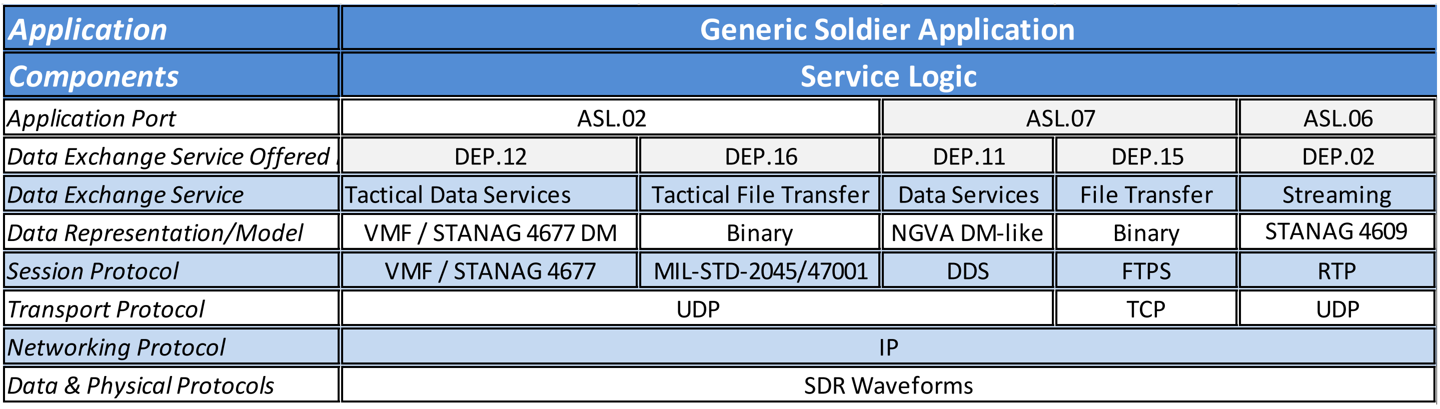
2.5.3.2 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the STU Commander Application HMI and (ii) the Application Service Logic (ASL) are listed below:

- ASL.02, which supports the Application Service Logic in the STU Domain and is mapped on:
  - STU Data Services, as described in Section 2.5.2.2
  - Tactical Data Services, as described in Section 2.5.2.2
- ASL.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in Section 2.5.2.2.
- ASL.07, which supports the File Transfer for the Application Service Logic and is mapped on:
  - File Transfer Services, as described in Section 2.5.2.2
  - Tactical File Transfer Services, as described in Section 2.5.2.2

Figure 2-61 summarizes the Soldier Application protocol stacks in this domain.



Application	Generic Soldier Application				
Components	Service Logic				
Application Port	ASL.02		ASL.07		ASL.06
Data Exchange Service Offered	DEP.12	DEP.16	DEP.11	DEP.15	DEP.02
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Streaming
Data Representation/Model	VMF / STANAG 4677 DM	Binary	NGVA DM-like	Binary	STANAG 4609
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	RTP
Transport Protocol	UDP			TCP	UDP
Networking Protocol	IP				
Data & Physical Protocols	SDR Waveforms				

Figure 2-61 – STU Domain - Soldier Application Protocol Stack

Use or disclosure of data contained on this sheet is subject to restriction on the title page of this document

2.5.3.3 Soldier Application System to System Port Connectivity

The Soldier Applications are serving a Specialist Soldier, and an STU Commander both acting in the STU Domain exchange data each as specified below.

The Specialist Soldier Application Service Logic component exchanges data via the following logical ports:

- ASL.02, which interconnects with:
    - The STU Commander Service Logic to
        - Send/Receive Tactical Data, and Tactical Files
    - A Shared Resource to
        - Send Command
        - Receive Tactical Data
- ASL.06, which interconnects with:
    - The STU Commander Service Logic to
        - Receive Commander Resource Streaming
        - Send Specialist Resource Streaming
    - A Shared Resource to
        - Receive Streaming
- ASL.07, which interconnects with:
    - The STU Commander Service Logic to
        - Send Request
        - Receive Reply, which provides for Persistent Tactical Data, Commander Resource Status/Data, Files
    - A Shared Resource to
        - Send/Receive Data
        - Send Files, e.g. Resource Configuration File.

The STU Commander Application Service Logic component exchanges data via the following logical ports:

- ASL.02, which interconnects with:
    - The Specialist Soldier Service Logic to
        - Send/Receive Tactical Data, and Tactical Files
    - A Shared Resource to
        - Send Command
        - Receive Tactical Data
- ASL.06, which interconnects with:
    - The Specialist Soldier Service Logic to
        - Send Commander Resource Streaming
        - Receive Specialist Resource Streaming
    - A Shared Resource to
        - Receive Streaming
- ASL.07, which interconnects with:
        - Send Reply which provides for Persistent Data, Commander Resource Status/Data
        - Receive Request

2.5.4 Communication Components

2.5.4.1 Communication Components Interface Description

The STUD/ID/JD/CD Domains are a combination of single communication systems that interact with each other through the Radio Services provided by the Communication Component (including one or more radios).

The peer Radio Device components are located on other entities such as other DSS (even with specific profiles) and vehicles, having the same radio capabilities and interface.

Such an interface, hence, allows communication in a networked domain of two or more nodes by means of over-the-air interconnection managed by networking and radio capabilities, namely “Waveforms”. The Networking capability may be implemented by the waveform or, in software, in the Processing Unit -the WPC- or in dedicated (small form-factor, lightweight, low power) devices.

Such capabilities can be transparent to the user, yet providing needed functionalities during the mission, such as LOS or BLOS communications, throughput, operation range, etc.).

The LOS interface provides communication capabilities for all the soldier domains, allowing for Line-of-Sight operations, within a range of tens of kilometres. Nodes using the LOS interface are typically connected among them to form a networked system where both user and radio services can be exploited.

Unique ID	Type	Requirement Description
REQ-67	**CR**	DSS radio communication system shall be able to exchange audio & data via LOS connectivity

Table 2-21 – STU Domain – DSS Radio Communication Requirements

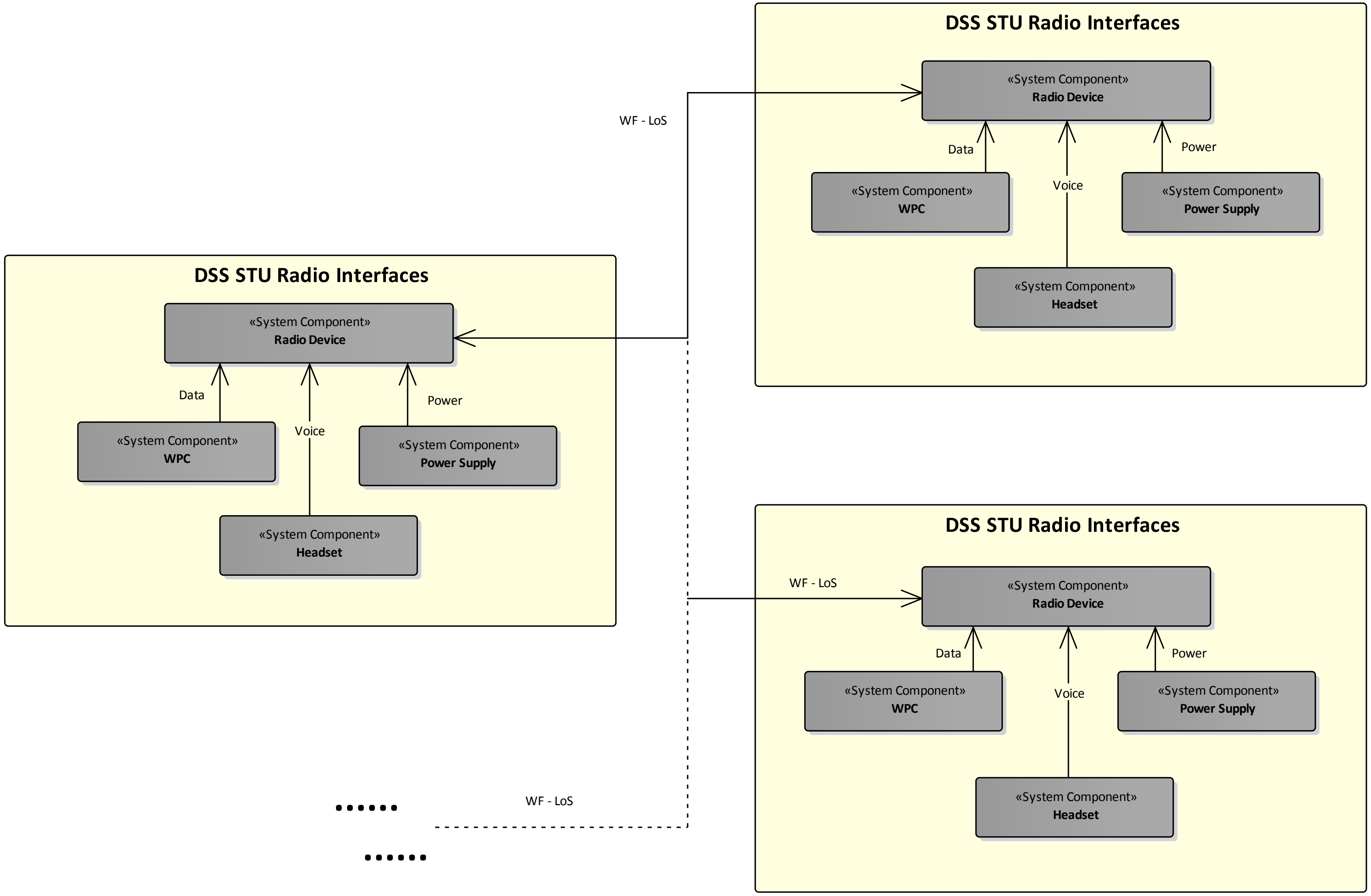


Figure 2-62 – Radio Device Interfaces via LoS WF in all system domains

2.5.4.2 Communication Components Port Specification

In the STUD/ID/JD/CD Domains, the Radio Device includes the following ports:

- RD.4: SiS LoS
- RD.5: SiS BLoS

The “SiS” (Signal in Space) interface is essential to define and allow interoperable communication means.

Component ports descriptions are provided in the next paragraphs.

2.5.4.2.1 Radio Device LoS SiS Port

Common to all DSS roles identified in the Organizational Relationship Chart, the basic communication capabilities needed to support intra-squad and inter-squad voice and data services in a restricted geographical area rely on the radio “protocols” defined through LoS SiS port.

2.5.4.3 Communication Components System to System Port Connectivity

Through the radio interface, the DSS communication system is able to interact with the other nodes in the network. Mobile Tactical Radio Networks are characterized by the capability (waveform) adopted for the specific operation, based on the identified mission requirements such as throughput, range, MANET, topology, etc.

The radio network then allows the interconnection of different DSS roles, e.g. between dismounted soldiers with their vehicle support platform or between a Leader and the command post.

In fact, the squad Commander, or a Communications Specialist, could be equipped with two radios or a two-channel radio, providing different capabilities (waveforms) for different communication links. Moreover, if size, weight and required power (and cost) of radios can be reduced further, it may become more common for basic soldiers configuration to have multi-channel radio.

When a commander or soldier is equipped with two radios or a multi-channel radio, there should be a capability to forward data traffic from one radio subnetwork to the other radio subnetwork. This may require cross-banding capability embedded into the multichannel radio or support by networking functions external to the radios (e.g. running on the Processing Unit or the WPC).

The mission-specific policy may disallow forwarding between different (e.g., coalition and national) radio networks, therefore it should be possible to disable this capability. Nevertheless, the capability should be present, in order to support more advanced networking configurations in the near future. (Even transit traffic through a radio network should be supported).

DSSs can operate in very different environments, depending on the mission location and type, so a more optimized solution should be identified that is able to adapt to changing behavioural needs.

So far, “loaned” or “procured” radio approached were simply identified as the solution to cover this delicate aspect of the mission success related to communication.

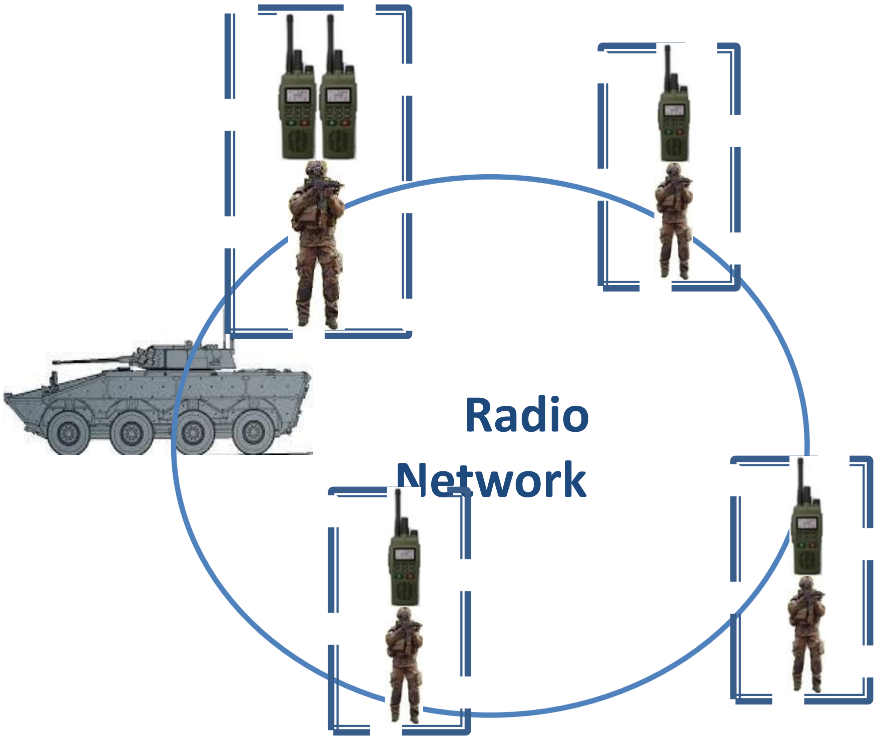


Figure 2-63 – Radio Networked Domain

A new concept (referred to as “waveform”) is now defined, which provides substantial improvements on:

- adaptability to mission environments
- interoperability
- possibility to use own radios, still guaranteeing interoperability for any of the communication solutions needed each time
- enhancement and stability of the soldier architecture (no changes to the system or easy customization, with increased flexibility)
- overall cost optimization to implement the communication solution

The new waveform paradigm is typically enabled by the SDR (Software Defined Radio) technology, however, it is focused on the definition of the standard waveforms suitable for the specific environment, performance, mission, topology, throughput, range, and services needed to be supported.

The SDR radios can be acquired by each DSS implementation in various ways, such as buying, implementing or loaning but what will allow communication interoperability, in the end, is the waveform running on top of them, chosen each time for the specific mission needs, allowing for an independent procurement of such capability.

In the mid-term, then, the DSS wireless networked communications will be focused on a basic set of SW Waveforms Applications pre-loaded on radio platforms, ready to be used in any domain application scenarios, Ground-To-Ground (GTG) or Ground-To-Air (GTA), from the DSS up to higher layer hierarchies.

The connectivity features of the radio port interface are described below.

SIS LoS Ports are connected by means of LoS waveform in any applicable domains

2.5.5 C4I Application

2.5.5.1 C4I Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equip an STU Commander who acts in the STU Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant DSS Components, the STU Commander could interact with to perform C4I Services in an STU Domain.

The HRI component is not shown because it is described in a dedicated paragraph.

The Interconnections among each C4I component with the other DSS Components is described below:

- BMS component at STU Commander Station interacts with:
  - Remote Effectors and Sensors to control them and gather the needed (Tactical) Data.
  - RAS C2 Station to control the RAS Mission and gather the relevant data
- SYS component at STU Commander Station interacts with:
  - Remote Effectors and Sensors to manage them as a system component, e.g. monitor & control, configuration, security.
  - RAS C2 Station to manage the RAS System as an external DSS component, e.g. monitor & control, configuration, security.
- SA component at STU Commander Station interacts with:
  - Remote Sensors to control them and gather the needed data and streaming, e.g. Video Streaming, Object of Interest Tracking & Position.
  - RAS C2 Station to control the RAS Mission about expected Payload usage;
  - RAS RSTA Station to gather the relevant Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

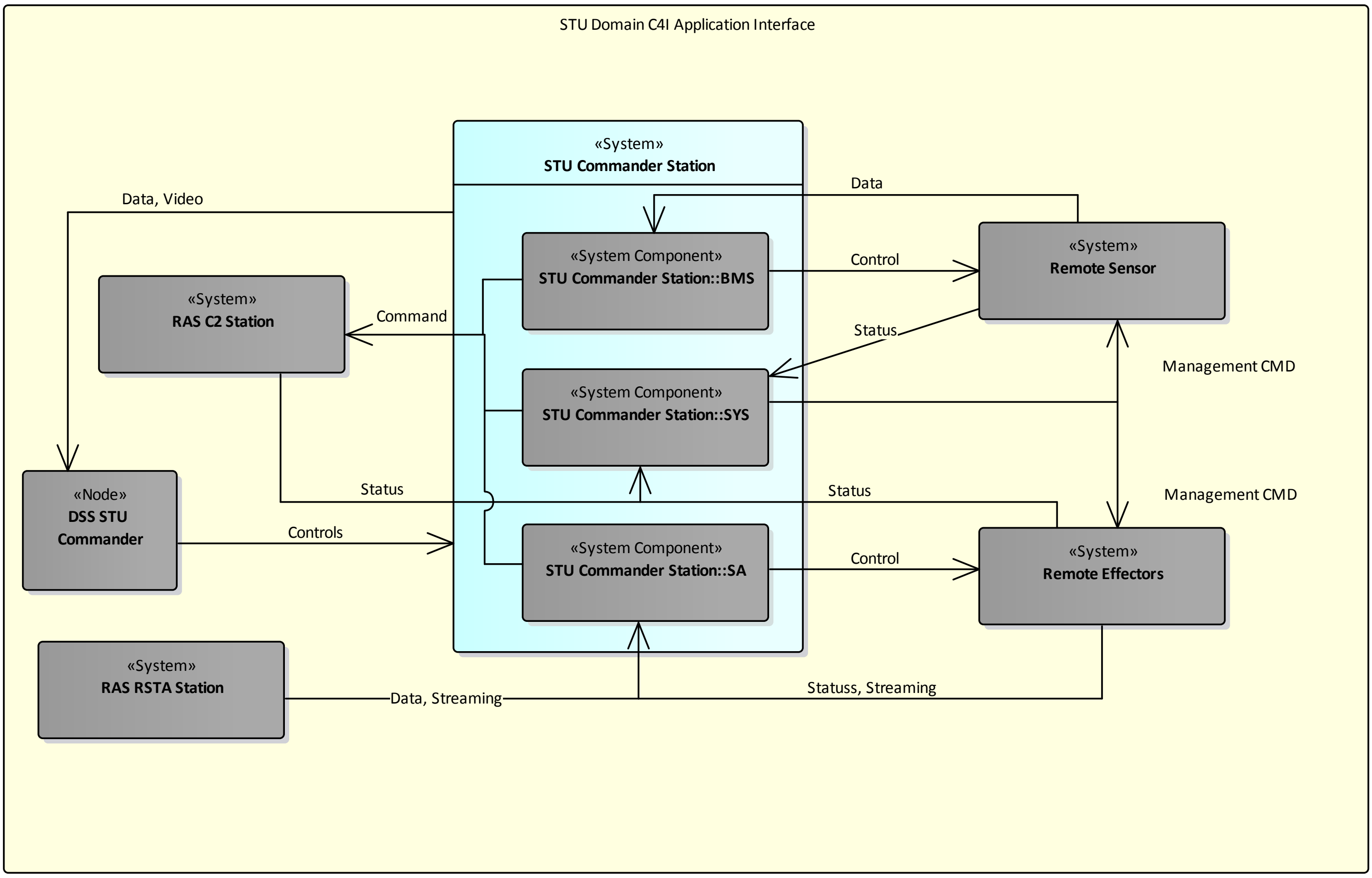


Figure 2-64 – STU Domain – STU Commander C4I Application

Unique ID	Type	Requirement Description
REQ-68	**CR**	STU Commander C4I Application shall interact with Remote Effectors and Sensors to control them and gather the needed (Tactical) Data.
REQ-69	**CR**	STU Commander C4I Application shall interact with RAS C2 Station to control the RAS Mission and gather the relevant data.
REQ-70	**CR**	STU Commander C4I Application shall interact with Remote Effectors and Sensors to manage them as a system component, e.g. monitor & control, configuration, security.
REQ-71	**CR**	STU Commander C4I Application shall interact with RAS C2 Station to manage the RAS System as an external DSS component, e.g. monitor & control, configuration, security.
REQ-72	**CR**	STU Commander C4I Application shall interact with Remote Sensors to control them and gather the needed data and streaming, e.g. Video Streaming, Object of Interest Tracking & Position.
REQ-73	**CR**	STU Commander C4I Application shall interact with RAS C2 Station to control the RAS Mission about expected Payload usage.
REQ-74	**CR**	STU Commander C4I Application shall interact with RAS RSTA Station to gather the relevant Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Table 2-22 – STU Domain – C4I Application Requirements

2.5.5.2 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components.

The set of logical ports supported respectively by (i) the BMS Service Logic and (ii) the SA Service Logic, and (iii) the SYS Service Logic are listed below.

The BMS Service Logic provides the following logical ports:

- BMS.02, which supports the BMS Services in the STU Domain and is mapped on Tactical Data Services, as described in Section 2.5.2.2
- BMS.02N, which supports the BMS Services in the STU Domain and is mapped on Tactical Data Services for Narrowband Radio, as described in Section 2.5.2.2
- BMS.08, which supports the BMS Services in the STU Domain and is mapped on Tactical File Transfer, as described in Section 2.5.2.2
- BMS.08N, which supports the BMS Services in the STU Domain and is mapped on Tactical File Transfer for Narrowband Radio, as described in Section 2.5.2.2

The SA Service Logic provides the following logical ports:

- SA.02, which supports the SA Services in the STU Domain and is mapped on STU Data Services, as described in Section 2.5.2.2
- SA.06, which supports the SA Services in the STU Domain and is mapped on STU File Transfer Services, as described in Section 2.5.2.2

- SA.04, which supports the Streaming for the SA Services and is mapped on Streaming Data Services as described in Section 2.5.2.2.

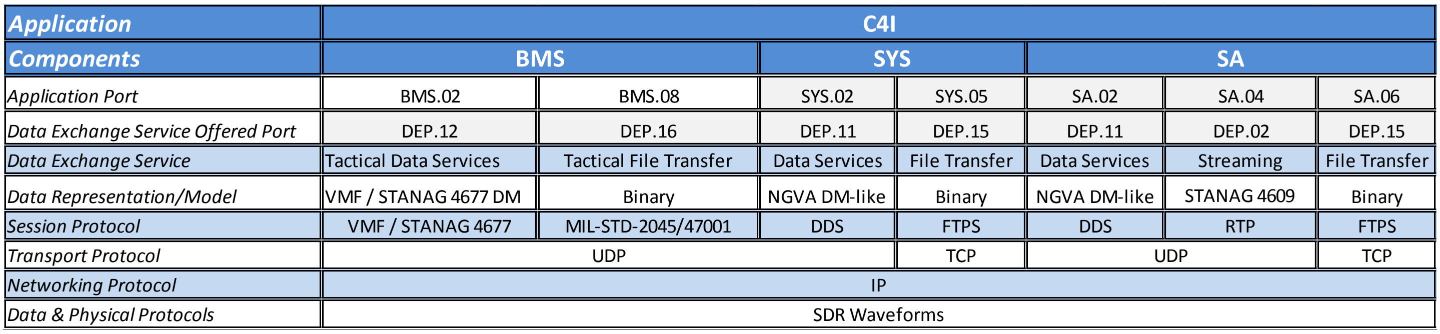
The SYS Service Logic provides the following logical ports:

- SYS.02, which supports the SYS Services in the STU Domain and is mapped on STU Data Services, as described in Section 2.5.2.2
- SYS.05, which supports the SYS Services in the STU Domain and is mapped on STU File Transfer Services, as described in Section 2.5.2.2

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.5.3.3.

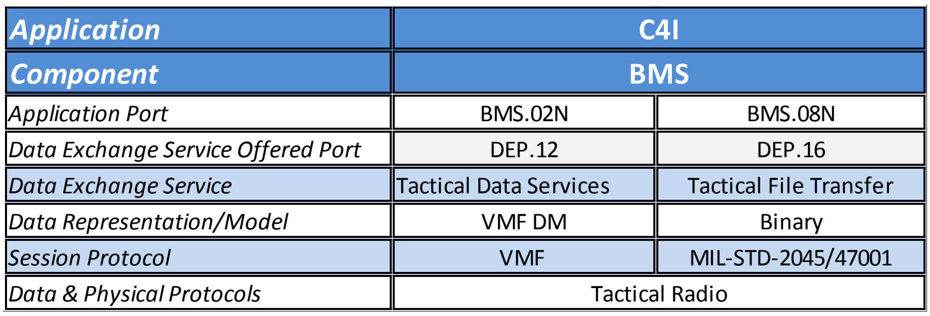
Figure 2-65 summarizes the C4I Application protocol stacks in this domain.

Figure 2-66 summarizes the C4I Application protocol stacks in this domain for the narrowband radio network.



Application	C4I						
Components	BMS		SYS		SA		
Application Port	BMS.02	BMS.08	SYS.02	SYS.05	SA.02	SA.04	SA.06
Data Exchange Service Offered Port	DEP.12	DEP.16	DEP.11	DEP.15	DEP.11	DEP.02	DEP.15
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Data Services	Streaming	File Transfer
Data Representation/Model	VMF / STANAG 4677 DM	Binary	NGVA DM-like	Binary	NGVA DM-like	STANAG 4609	Binary
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	DDS	RTP	FTPS
Transport Protocol	UDP			TCP	UDP		TCP
Networking Protocol	IP						
Data & Physical Protocols	SDR Waveforms						

Figure 2-65 – STU Domain – STU C4I Application Protocol Stacks



Application	C4I	
Component	BMS	
Application Port	BMS.02N	BMS.08N
Data Exchange Service Offered Port	DEP.12	DEP.16
Data Exchange Service	Tactical Data Services	Tactical File Transfer
Data Representation/Model	VMF DM	Binary
Session Protocol	VMF	MIL-STD-2045/47001
Data & Physical Protocols	Tactical Radio	

Figure 2-66 – STU Domain – STU C4I Application Protocol Stacks for Tactical Protocol directly deployed on Radio Network (No IP Networking)

2.5.5.3 C4I Application System to System Port Connectivity

In the STU Domain the C4I Application exchanges data with peers system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.02, which interconnects with:
    - The set of Remote Effectors to
        - Send Commands
        - Receive Tactical Data
    - The RAS Mission Control to:
        - Send Commands, Tactical Data
        - Receive Tactical Data
    - STU Soldier Application to
        - Send Commands, Tactical Data
        - Receive Tactical Data
- BMS.02N, which interconnects with:
    - The set of Remote Effectors to
        - Send Commands
        - Receive Tactical Data
    - The RAS Mission Control to:
        - Send Commands, Tactical Data
        - Receive Tactical Data
    - STU Soldier Application to
        - Send Commands, Tactical Data
        - Receive Tactical Data
- BMS.08, which interconnects with:
    - The RAS Mission Control to:
        - Send Tactical Files
        - Receive Tactical Files
    - STU Soldier Application to
        - Send / Receive Tactical Files
- BMS.08N, which interconnects with:
    - The RAS Mission Control to:
        - Send Tactical Files
        - Receive Tactical Files
    - STU Soldier Application to
        - Send / Receive Tactical Files

The SYS Service Logic component exchanges data via the following logical ports:

- SYS.02, which interconnects with:
    - The set of Remote Effectors to
        - Send Management Commands
        - Receive Data
    - The set of Remote Sensors to
        - Send Management Commands
        - Receive Data
    - The RAS C2 Station to:
        - Send Management Commands

        - Receive Data
- SYS.05, which interconnects with:
    - The set of Remote Effectors to
        - Send Files
    - The set of Remote Sensors to
        - Send Files
    - The RAS C2 Station to:
        - Send Files

The SA Service Logic component exchanges data via the following logical ports:

- SA.02, which interconnects with:
    - The set of Remote Sensors to
        - Send Sensor Control Commands
        - Receive Data
    - RAS RSTA Station to:
        - Receive Data
- SA.04, which interconnects with:
    - The set of Remote Sensors to:
        - Receive Streaming of live data, e.g. Video
    - RAS RSTA Station to:
        - Receive Streaming of live data, e.g. Video
- SA.06, which interconnects with:
    - RAS RSTA Station to:
        - Receive Files, e.g. Images

2.5.6 Human RAS Interaction

2.5.6.1 Human RAS Interaction Interface Description

The figure below depicts the main components and related interconnections of the Human RAS Interaction (HRI), which equips a RAS Control Team.

The RAS Control Team is typically composed by:

- RAS Commander, who acts as the Team Commander and is equipped by a RAS Command & Control (RAS C2) Station;
- RSTA Operator, who operates the RAS Payload and is equipped by a RAS RSTA Station.

The RAS C2 Station hosts the following SW Components:

- RAS Mission Control, which implements the RAS Mission Control Services;
- RAS Management, which implements (i) the RAS Management Services.

The RAS RSTA Station hosts the following SW Components:

- RAS Payload Control, which provides for specific controls to operate the (set of) payloads the RAS is equipped with.

The RAS Mission Control interacts with:

- The following SW components of the STU Commander Station:
  - BMS, which commands the RAS Mission Control on mission goals and related operational tasks to perform;
  - SA, which commands the RAS Mission Control about expected Payload usage.
- The following SW components of the RAS RSTA Station
  - RAS Payload Control to command this module about the requested Payload Services, e.g. Video Services.

The RAS Management interacts with:

- The following SW components of the STU Commander Station:
  - FCPS Management, which commands the RAS System Control about the system management functions, e.g. Configuration, Health Monitoring.

The RAS Payload Control interacts with:

- The following SW components of the STU Commander Station:
  - SA, to which provides for Payload outcome in accordance with the SA requests to RAS Mission Control
- The following SW components of the RAS C2 Station:
  - RAS Mission Control, which commands it on the tasks assigned to the RAS Payload(s).

Unique ID	Type	Requirement Description
REQ-75	**CR**	The RAS C2 Station shall provide the RAS Commander, or equipollent role, for RAS Mission Control and RAS Management Services.
REQ-76	**CR**	The RAS C2 Station shall interact with the STU Commander Station to receive commands and provide data about the RAS tasks.
REQ-77	**CR**	The RAS RSTA Station shall allow the DSS RSTA Operator to execute the tasks requested by Commander roles via the RAS Mission Control.

Table 2-23 – STU Domain - Human RAS Interaction Requirements

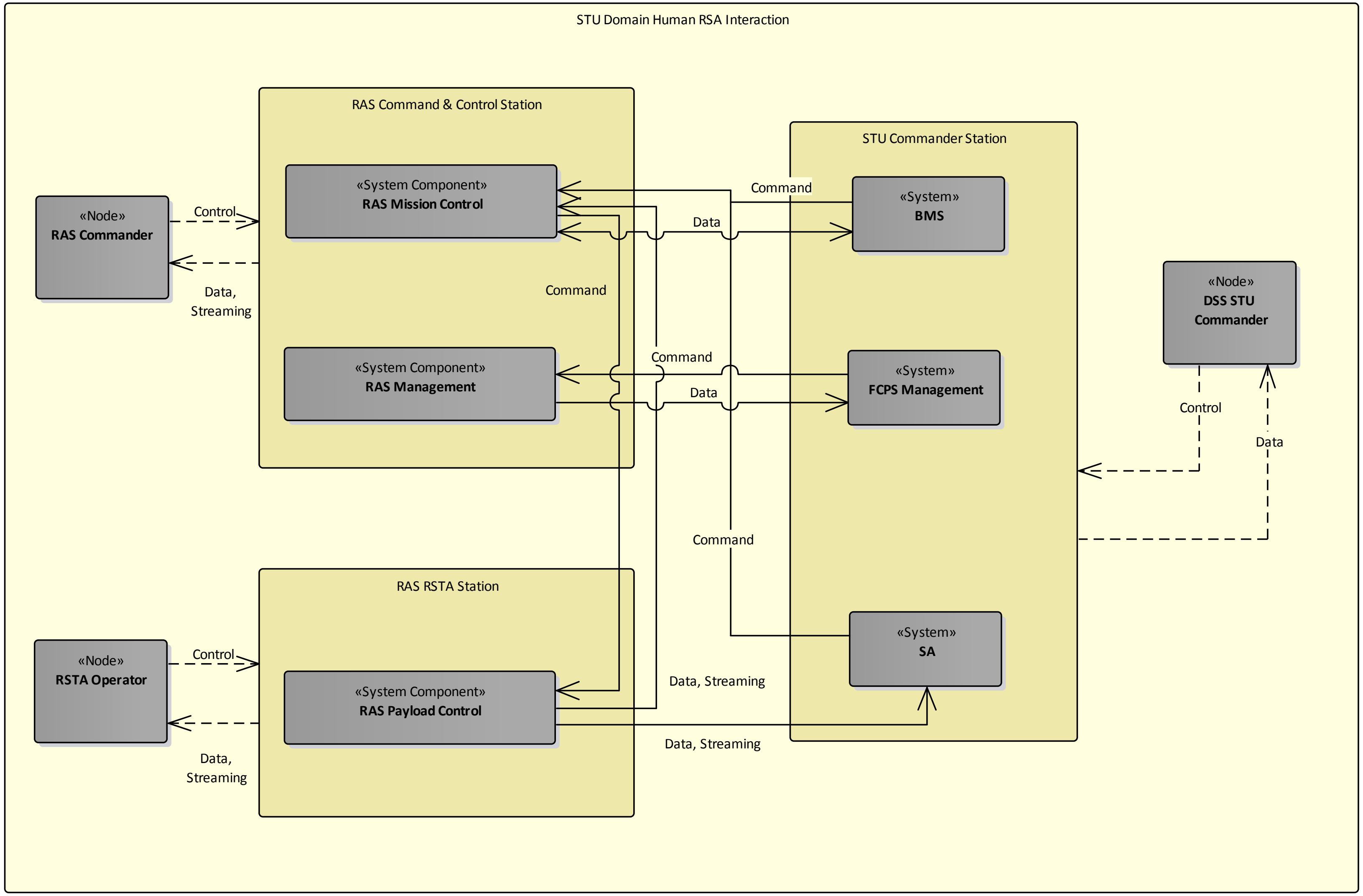


Figure 2-67 – Human RAS Interaction for STU Domain

2.5.6.2 Human RAS Interaction Port Specification

A Human RAS Interaction provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the RAS Payload Control, (ii) RAS Mission Control, and RAS Management are listed below.

The RAS Payload Control (RAS PC) provides the following logical ports:

- RAS_PC.01, which supports the RAS Payload Control Services and is mapped on STU Data Services, as described in Section 2.5.2.2
- RAS_PC.02, which supports the Streaming for the RAS Payload Control Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.

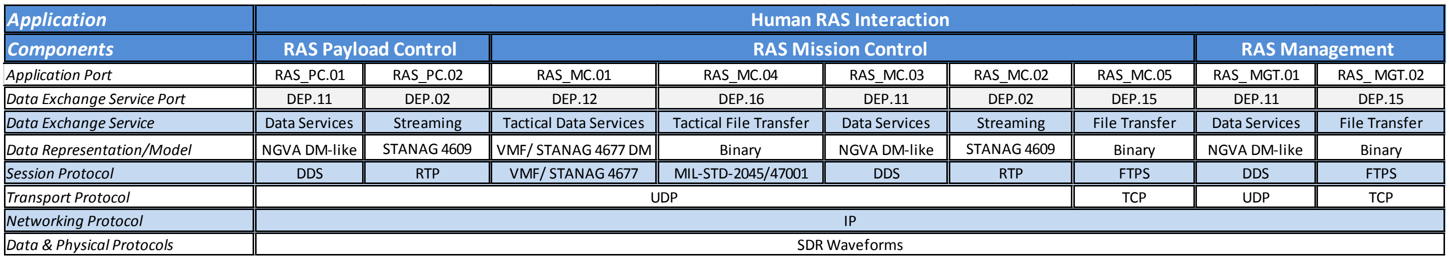
The RAS Mission Control (RAS MC) the following logical ports:

- RAS_ MC.01, which supports the RAS Mission Control Services and is mapped on Tactical Data Services, as described in Section 2.5.2.2
- RAS_ MC.02, which supports the Streaming for the RAS Mission Control Services and is mapped on Streaming Data Services as described in Section 2.5.2.2.
- RAS_ MC.03, which supports the RAS Mission Control Services and is mapped on STU Data Services, as described in Section 2.5.2.2
- RAS_ MC.04, which supports the RAS Mission Control Services and is mapped on STU Tactical File Transfer Services, as described in Section 2.5.2.2
- RAS_ MC.05, which supports the RAS Mission Control Services and is mapped on STU File Transfer Services, as described in Section 2.5.2.2

The RAS Management (RAS MGT) provides the following logical ports:

- RAS_ MGT.01, which supports the RAS Management Services in the STU Domain and is mapped on STU Data Services, as described Section 2.5.2.2
- RAS_ MGT.02, which supports the RAS Management Services in the STU Domain and is mapped on STU File Transfer Services, as described in Section 2.5.2.2

Figure 2-68 summarizes the HRI Application protocol stacks in this domain. Figure 278 summarizes the HRI Application protocol stacks in this domain.



Application	Human RAS Interaction								
Components	RAS Payload Control		RAS Mission Control					RAS Management	
Application Port	RAS_PC.01	RAS_PC.02	RAS_MC.01	RAS_MC.04	RAS_MC.03	RAS_MC.02	RAS_MC.05	RAS_ MGT.01	RAS_ MGT.02
Data Exchange Service Port	DEP.11	DEP.02	DEP.12	DEP.16	DEP.11	DEP.02	DEP.15	DEP.11	DEP.15
Data Exchange Service	Data Services	Streaming	Tactical Data Services	Tactical File Transfer	Data Services	Streaming	File Transfer	Data Services	File Transfer
Data Representation/Model	NGVA DM-like	STANAG 4609	VMF/ STANAG 4677 DM	Binary	NGVA DM-like	STANAG 4609	Binary	NGVA DM-like	Binary
Session Protocol	DDS	RTP	VMF/ STANAG 4677	MIL-STD-2045/47001	DDS	RTP	FTPS	DDS	FTPS
Transport Protocol	UDP						TCP	UDP	TCP
Networking Protocol	IP								
Data & Physical Protocols	SDR Waveforms								

Figure 2-68 – Human RAS Interaction Protocol Stacks for STU Domain

2.5.6.3 Human RAS Interaction System to System Port Connectivity

The Human RAS Interaction which is serving an STU Commander in the STU Domain exchange data each as specified below.

The RAS Mission Control (RAS MC) component exchanges data via the following logical ports:

- RAS_MC.01, which interconnects with:
  - The STU Commander BMS Component to
    - Send Tactical Data
    - Receive Command, Tactical Data
- RAS_MC.03, which interconnects with:
  - The RAS Payload Control to
    - Send/ Receive Data
- RAS_MC.04, which interconnects with:
  - The STU Commander BMS Component to
    - Receive Tactical Files, e.g. Maps
- RAS_MC.05, which interconnects with:
  - The STU Commander SA Component to
    - Send/ Receive Files, e.g. Images

The RAS Management (RAS MGT) component exchanges data via the following logical ports:

- RAS_ MGT.01, which interconnects with:
  - The STU Commander SYS Service Logic to
    - Send Data
    - Receive Management Commands
- RAS_ MGT.02, which interconnects with:
  - The STU Commander SYS Service Logic to
    - Exchange RAS System Management Files

The RAS Payload Control (RAS PC) component exchanges data via the following logical ports:

- RAS_ PC.01, which interconnects with:
  - The STU Commander SA Service Logic to
    - Send Data
  - The RAS Mission Control to
    - Send Data
    - Receive Command
- RAS_ PC.02, which interconnects with:
  - The STU Commander SA Service Logic to
    - Send Live Data Streaming, e.g. Video
  - The RAS Mission Control to
    - Send Live Data Streaming, e.g. Video

2.6 Inter-Platform Domain

2.6.1 Dismounted Soldier

2.6.1.1 Data Exchange Services

2.6.1.1.1 Data Exchange Services Interface Description

The figure below depicts the main components and related interconnections of the Data Exchange Services, which serve a Soldier acting in the Inter-Platform Domain. It applies to both Dismounted Soldier, who will typically be an STU Commander, and to Mounted Soldier.

The Data Exchange Protocol components of Soldier and a Vehicle with NGVA interact via an NGVA Gateway to supports the data exchange among the Soldier Application Services Logic and Vehicle Service Logic.

The NGVA Gateway is not necessary if the Soldier Data Exchange Services adopt the same identical protocol suite of the Vehicle.

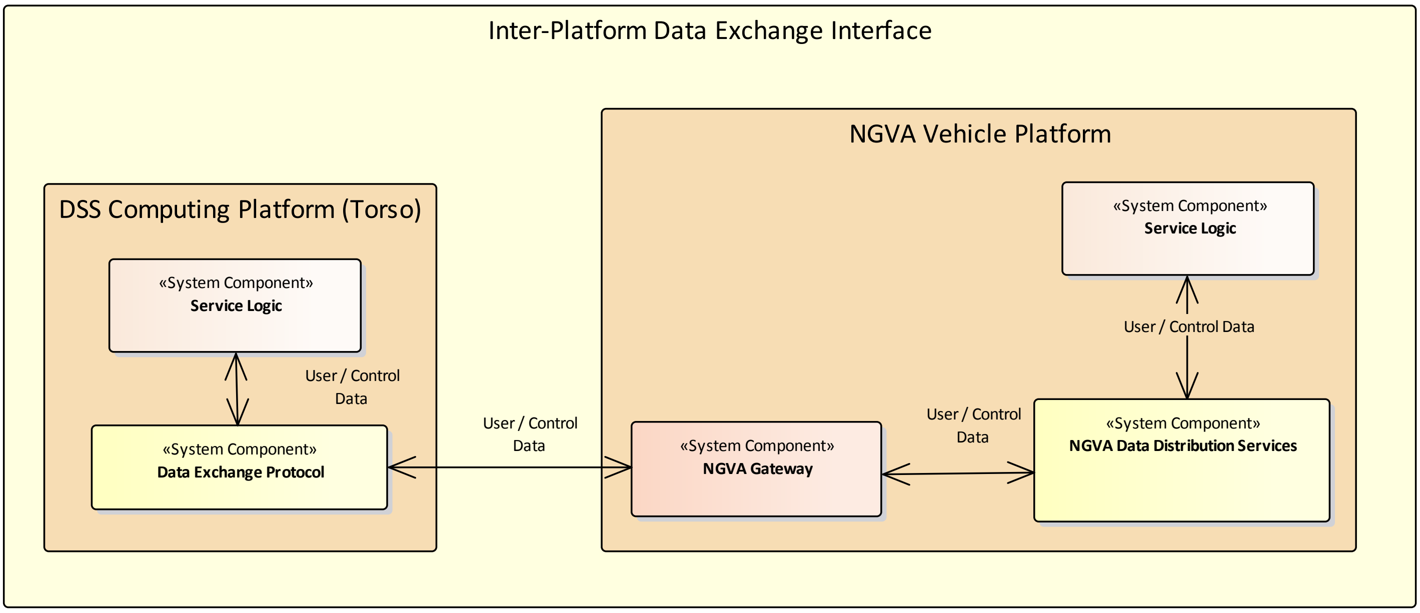


Figure 2-69 – Inter-Platform Domain – Soldier – Vehicle Data Exchange Services (with NGVA)

2.6.1.1.2 Data Exchange Services Port Specification

The Data Exchange Protocol (DEP) component provides the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Inter-Platform Domain;
- Required Port, which requests services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the Inter-Platform Domain Dismounted Soldier are:

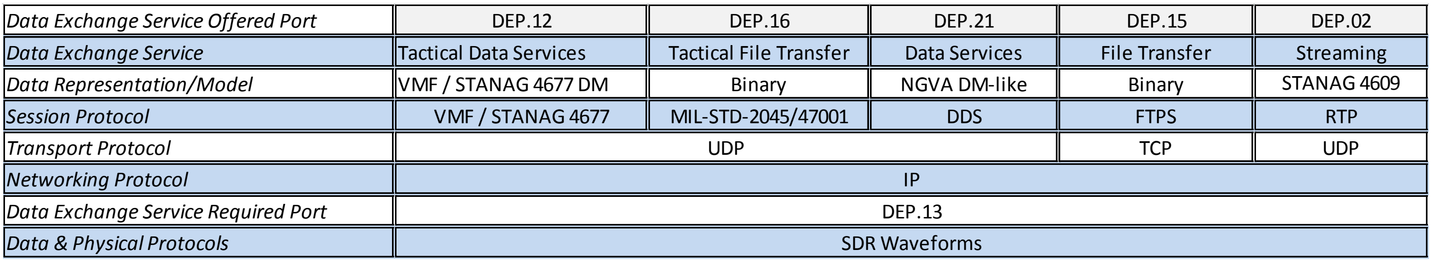
- Offered Ports:
  - DEP.21 provides the API for an Inter-Platform Data Services.
  - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio, between a Dismounted STU Commander and a commanding node, e.g. NGVA Vehicle.
  - DEP.12: Tactical Data Services, which provides for exchanging tactical data between a Dismounted STU Commander and a commanding node, e.g. NGVA Vehicle.
  - DEP.16: Tactical File Transfer, which provides for File Transfer service on Tactical Data Link.
  - DEP.15: File Transfer, which provides for the transmission of a file, e.g. an Image, between a DSS Node and the commanding node, e.g. NGVA Vehicle.
- Required Ports:
  - DEP.13: Radio Services, which request for transport of data/streaming among the Inter-Platform radio network endpoints.
  - DEP.14: Radio Tactical Services, which request for transport of tactical data among the Inter-Platform radio network endpoints.
  - DEP.05: Execution Platform API, which requests for services supporting the execution of the DEP threads.

Each logical port is supported by an appropriated protocol stack as described below:

- DEP.21 provides the API for an Inter-Platform Data Services. The following protocols are a candidate to implement the Data Session Protocol for DEP in the Inter-Platform Domain:
    - Data Distribution Services for Real-Time Systems[/20/, /21/, /22/,/23/]
- DEP.15 provides the API for File Transfer Services. The following protocols are a candidate to implement the File Transfer Services:
  - File Transfer Protocol Secure (FTPS) [/27/, /28/]
- DEP.02 provides the API for Streaming Services. The following protocols are a candidate to implement the Streaming Session Protocol:
  - Real-time Transport Protocol (RTP) [/24/].
  - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]
- DEP.12 provides the API for a Tactical Data Services. The following protocols are a candidate to implement the Tactical Data Protocol:
  - Joint Dismounted Soldier System Interoperability Network (JDSSIN) [/13/,/14/,/15/,/16/,/17/]
  - Variable Message Format [/25/]
- DEP.16 provides the API for Tactical File Transfer. The following protocols are a candidate to implement the File Transfer Services:
  - Variable Message Format [/25/, /26/]
- DEP.13 requires for Radio Services in an Inter-Platform radio area network.
- DEP.14 requires for Tactical Radio Services in an Inter-Platform radio area network.
- DEP.05 requires for Execution Environment Services, it is mapped on the API of the Execution Environment provided by the hosting computer platform.

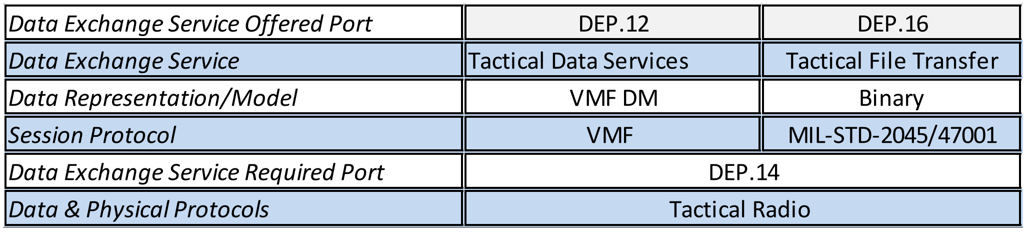
Figure 2-70 summarizes the Data Exchange Services protocol stacks in this domain.

Figure 2-71 summarizes the Data Exchange Services protocol stacks in this domain for the narrowband radio network.



Data Exchange Service Offered Port	DEP.12	DEP.16	DEP.21	DEP.15	DEP.02
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Streaming
Data Representation/Model	VMF / STANAG 4677 DM	Binary	NGVA DM-like	Binary	STANAG 4609
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	RTP
Transport Protocol	UDP			TCP	UDP
Networking Protocol	IP				
Data Exchange Service Required Port	DEP.13				
Data & Physical Protocols	SDR Waveforms				

Figure 2-70 – NSV-2a Inter-Platform Data Exchange Services Protocol Stack



Data Exchange Service Offered Port	DEP.12	DEP.16
Data Exchange Service	Tactical Data Services	Tactical File Transfer
Data Representation/Model	VMF DM	Binary
Session Protocol	VMF	MIL-STD-2045/47001
Data Exchange Service Required Port	DEP.14	
Data & Physical Protocols	Tactical Radio	

Figure 2-71 – NSV-2a Inter-Platform Data Exchange Services Protocol Stack for over Tactical Radio

2.6.1.1.3 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component(s) which is serving DSS Nodes, who act in the Inter-Platform Domain, exchange data with Vehicle components as specified below.

The Data Exchange Protocol component provides services via the following logical ports:

- DEP.21, which interconnects with:
  - The Soldier Application Service Logic, e.g. C4I Applications to:
    - Send / Receive User Data and Service Control Data
  - The Remote Peripheral(s) Service Logic, e.g. RAS to:
    - Send / Receive User Data and Service Control Data
- DEP.12, which interconnects with:
  - The Soldier Application Service Logic, e.g. C4I Applications to:
    - Send / Receive Tactical Data and Service Control Data
  - The Remote Peripheral(s) Service Logic, e.g. RAS to:
    - Send / Receive Tactical Data and Service Control Data
- DEP.02, which interconnects with:
  - The Soldier Application Service Logic, e.g. C4I Applications to:
    - Send Streaming Data
    - Send / Receive Service Control Data
  - The Remote Peripheral(s) Service Logic, e.g. RAS to:
    - Receive Streaming Data
    - Send / Receive Service Control Data
- DEP.15, which interconnects with:

    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive files
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive files
- DEP.16, which interconnects with:
    - The Soldier Application Service Logic, e.g. C4I Applications to:
        - Send / Receive files on the tactical transport protocol
    - The Remote Peripheral(s) Service Logic, e.g. RAS to:
        - Send / Receive files on the tactical transport protocol

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.13, which interconnects with:
    - Radio Services provided by the Inter-Platform radio area network, to:
        - Send / Receive User Data, Streaming Data, and Service Control Data, Files
- DEP.14, which interconnects with:
    - Tactical Radio Services provided by the Inter-Platform tactical radio area network, to:
        - Send / Receive Tactical Data, and Tactical Files
- DEP.05, which interconnects with:
    - Execution Environment API, to:
        - Send / Receive Service Control Data

2.6.1.2 Soldier Application

2.6.1.2.1 Soldier Application Interface Description

The figure below depicts the main components and related interconnection of a Soldier Application, which equips a Dismounted STU Commander who acts in the Inter-Platform Domain.

This diagram highlight the capability for a Commander Application to request Services to a Vehicle. In this interaction, the Commander Application Service Logic acts as Consumer of Services provided by the Vehicle Application Service Logic.

The relationship between Soldier Application and NGVA Application are bidirectional, i.e. the NGVA Service Logic could request a service to the Service Logic of the Commander Application.

Alternatively, following the NGVA HMI Design guidelines, the Commander Application HMI could directly interact with the Vehicle Service Logic.

It is worth noting that the NGVA Service Logic provides access to the NGVA Services, e.g. Registration Services, Arbitration Services, Resource Usage Services.

Unique ID	Type	Requirement Description
REQ-78	**OE**	A Commander Application should be able to request for Services to a Vehicle Application. In this interaction, the Commander Application Service Logic acts as Consumer of Services provided by the Vehicle Application Service Logic.
REQ-79	**OE**	A Commander Application should be able to provide for Services to a Vehicle Application. In this interaction, the Commander Application Service Logic acts as Provider of Services for the Vehicle Application Service Logic.
REQ-80	**OE**	The Commander Application HMI should be able to directly interact with the Vehicle Service Logic.

Table 2-24 – Inter-Platform Domain - Dismounted STU Commander Application Requirements

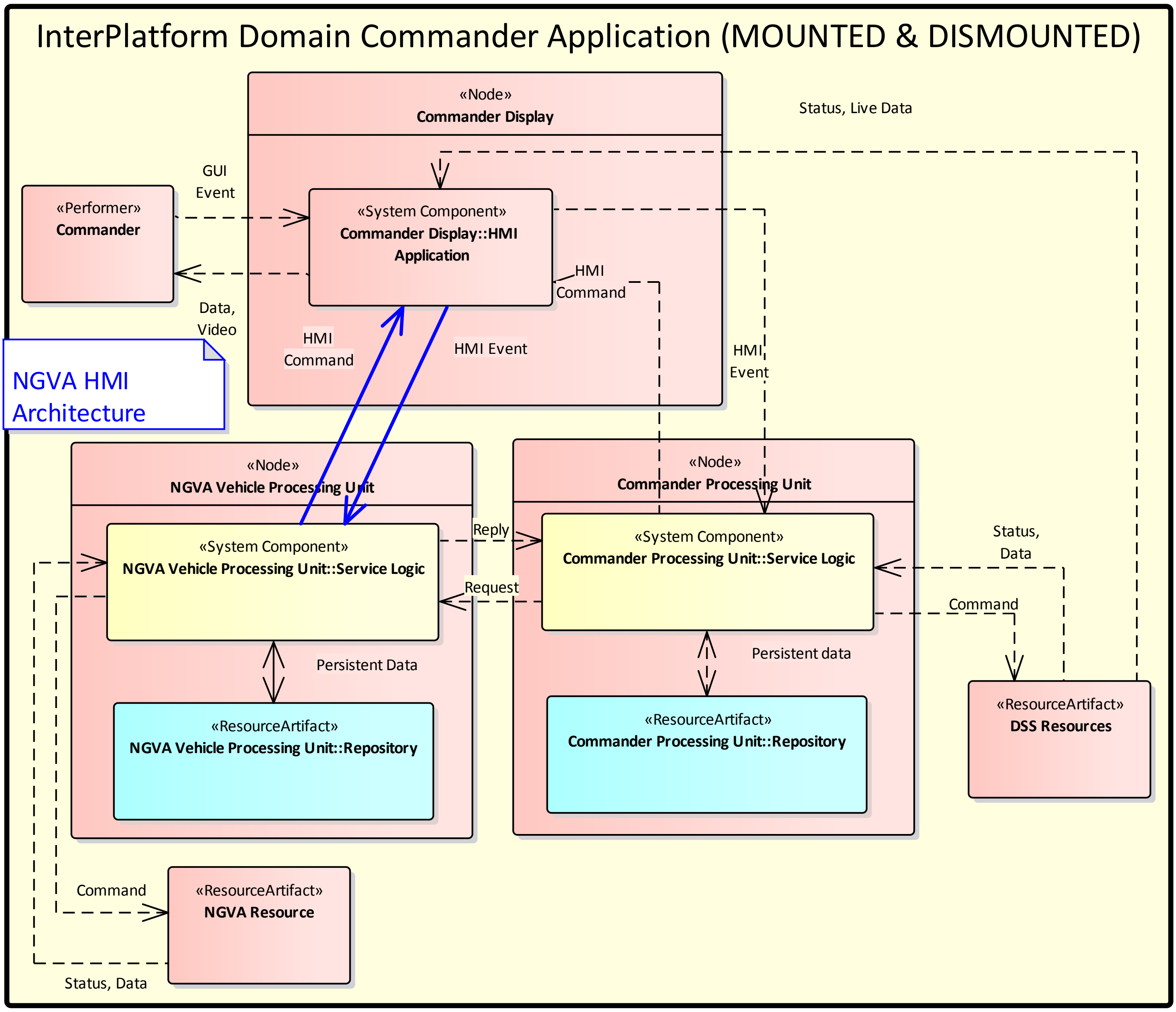


Figure 2-72 – Inter-Platform Domain – Dismounted STU Commander Application

2.6.1.2.2 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers' system components in the different domains.

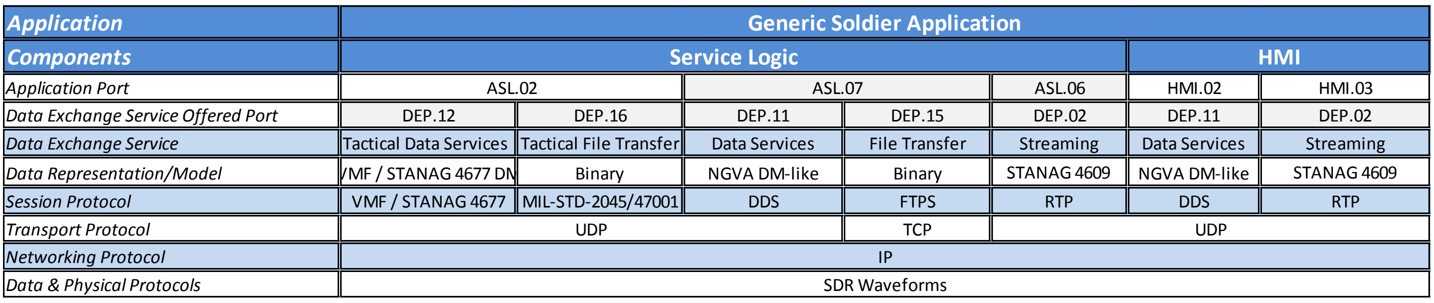
The set of logical ports supported respectively by (i) the STU Commander Application HMI and (ii) the Application Service Logic are listed below.

The STU Commander Application HMI provides the following logical ports:

- HMI.02, which supports the Application HMI Services in the Inter-Platform Domain and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- HMI.03, which supports the Streaming for the Application HMI Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs

The Application Service Logic (ASL) provides the following logical ports:

- ASL.02 which supports the Application Service Logic and is mapped on:
  - Inter-Platform Data Services, as described in Section 2.6.1.1.2
  - Tactical Data Services, as described in Section 2.6.1.1.2
- ASL.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.
- ASL.07, which supports the File Transfer for the Application Service Logic and is mapped on:
  - File Transfer Services, as described in Section 2.6.1.1.2
  - Tactical File Transfer Services, as described in Section 2.6.1.1.2



Application	Generic Soldier Application						
Components	Service Logic					HMI	
Application Port	ASL.02		ASL.07		ASL.06	HMI.02	HMI.03
Data Exchange Service Offered Port	DEP.12	DEP.16	DEP.11	DEP.15	DEP.02	DEP.11	DEP.02
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Streaming	Data Services	Streaming
Data Representation/Model	/MF / STANAG 4677 DN	Binary	NGVA DM-like	Binary	STANAG 4609	NGVA DM-like	STANAG 4609
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	RTP	DDS	RTP
Transport Protocol	UDP			TCP	UDP		
Networking Protocol	IP						
Data & Physical Protocols	SDR Waveforms						

Figure 2-73 – Inter-Platform Domain - Soldier Application Protocol Stack

2.6.1.2.3 Soldier Application System to System Port Connectivity

The Soldier Application which is serving a Dismounted STU Commander, who acts in the Inter-Platform Domain exchange data with peers system component as specified below.

The Application HMI component exchanges data via the following logical ports:

- HMI.02, which interconnects with:
  - the Vehicle Service Logic to:
    - Receive HMI Command, Data
    - Send HMI Event
- HMI.03, which interconnects with:
  - Vehicle Service Logic to:
    - Receive Streaming of live data, e.g. Video

The Application Service Logic component exchanges data via the following logical ports:

- ASL.03, which interconnects with:
  - the Vehicle Service Logic to:

    - Receive Command
    - Send / Receive Tactical Data, and Tactical File
- ASL.06, which interconnects with:
  - the Vehicle Service Logic to:
    - Send / Receive Streaming of live data, e.g. Video
- ASL.07, which interconnects with:
  - the Vehicle Service Logic to:
    - Send / Receive Data, and File

2.6.1.3 Communication Components

2.6.1.3.1 Communication Components Interface Description

In addition to the LoS interface specified in section 2.5.4.2.1, the Inter-Platform Domain (ID), Joint Domain (JD), and Coalition Domain (CD) also provide for Beyond Line of Sight (B-LOS) interface as specified below.

The B-LOS interface provides communication capabilities typically for the ID/JD/CD domains, allowing Beyond-Line-of-Sight operations, within a wide range of thousands of kilometres. Two nodes using a B-LOS interface are typically connected over a point-to-point communication link, over which user services can be exploited.

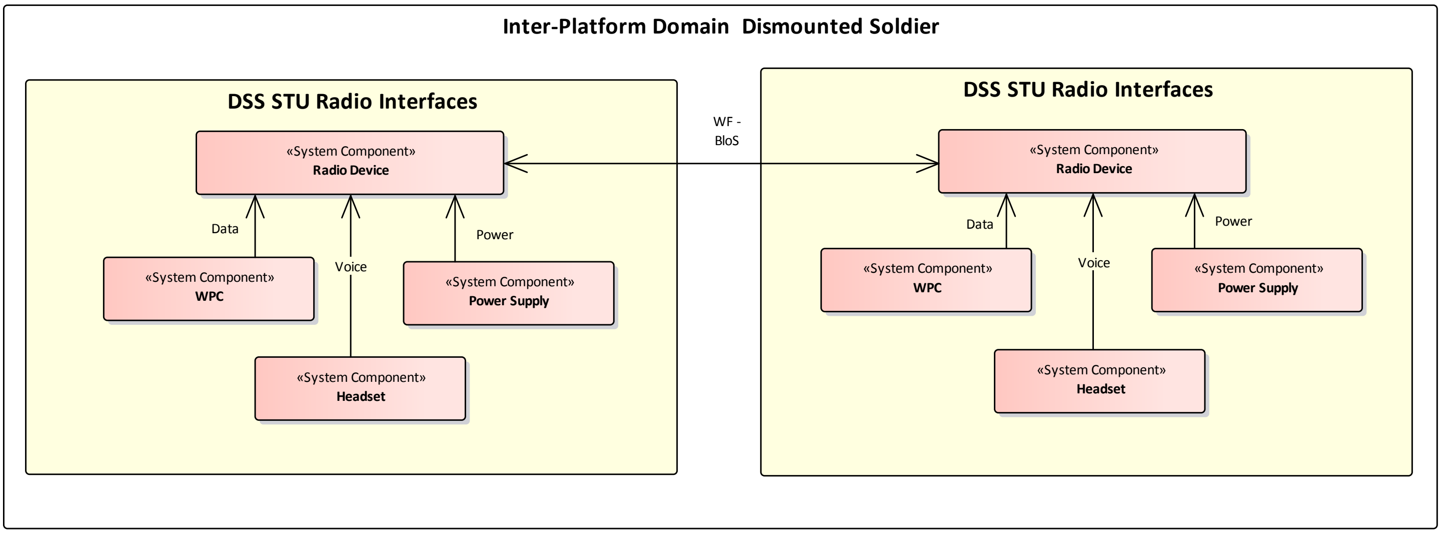


Figure 2-74 – Radio Device Interfaces in ID/JD/CD via B-LoS WF system domains

Unique ID	Type	Requirement Description
REQ-81	**CR**	DSS radio communication system shall be able to exchange audio & data via B-LOS connectivity

Table 2-25 – Inter-Platform Domain – DSS Radio Communication Requirements

2.6.1.3.2 Communication Components Port Specification

In addition to the LoS interface specified in section 2.5.4.2.1, the Inter-Platform Domain (ID), Joint Domain (JD), and Coalition Domain (CD) also provide for Beyond Line of Sight (B-LoS) interface as specified below.

For some special role DSS nodes the need for tactical SA reporting from the field or remote command exchanges to/from higher organization layer hierarchies, rely on the availability of a Beyond Line of Sight communication connectivity.

The B-LoS SiS port addresses point to point communications based mainly on HF and Satellite communications.

2.6.1.3.3 Communication Components System to System Port Connectivity

In addition to the LoS interface specified in section 2.5.4.2.1, the Inter-Platform Domain (ID), Joint Domain (JD), and Coalition Domain (CD) also provide for Beyond Line of Sight (B-LoS) interface as specified below.

SIS B-LoS Ports are connected by means of B-LoS waveform in Inter-platform, Join and Coalition domains where geographical distances do not allow LoS communications.

2.6.1.4 C4I Application

2.6.1.4.1 C4I Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equips a Dismounted STU Commander who acts in the Inter-Platform Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant Vehicle Components, STU Commander could interact with to perform C4I Services in the Inter-Platform Domain.

The HRI component is not shown because it is described in a dedicated paragraph.

The Interconnections among each C4I component with the Vehicle C4I Components is described below:

- BMS component at STU Commander Station interacts with:
    - BMS at Vehicle C2 Station to acquire Vehicle Commander commands, and exchange the needed (Tactical) Data.
- SYS component at STU Commander Station interacts with:
    - SYS at Vehicle C2 Station to manage both Resource Registration and Arbitration protocols.
- SA component at STU Commander Station interacts with:
    - SA at Vehicle C2 Station to exchange the needed Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Unique ID	Type	Requirement Description
REQ-82	**CR**	Dismounted STU Commander C4I Application shall interact with BMS at Vehicle C2 Station to acquire Vehicle Commander commands, and exchange the needed (Tactical) Data.
REQ-83	**CR**	Dismounted STU Commander C4I Application shall interact with SYS at Vehicle C2 Station to manage Resource Registration protocol.
REQ-84	**CR**	Dismounted STU Commander C4I Application shall interact with SA at Vehicle C2 Station to gather the needed Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Table 2-26 – Inter-Platform Domain – C4I Application Requirements

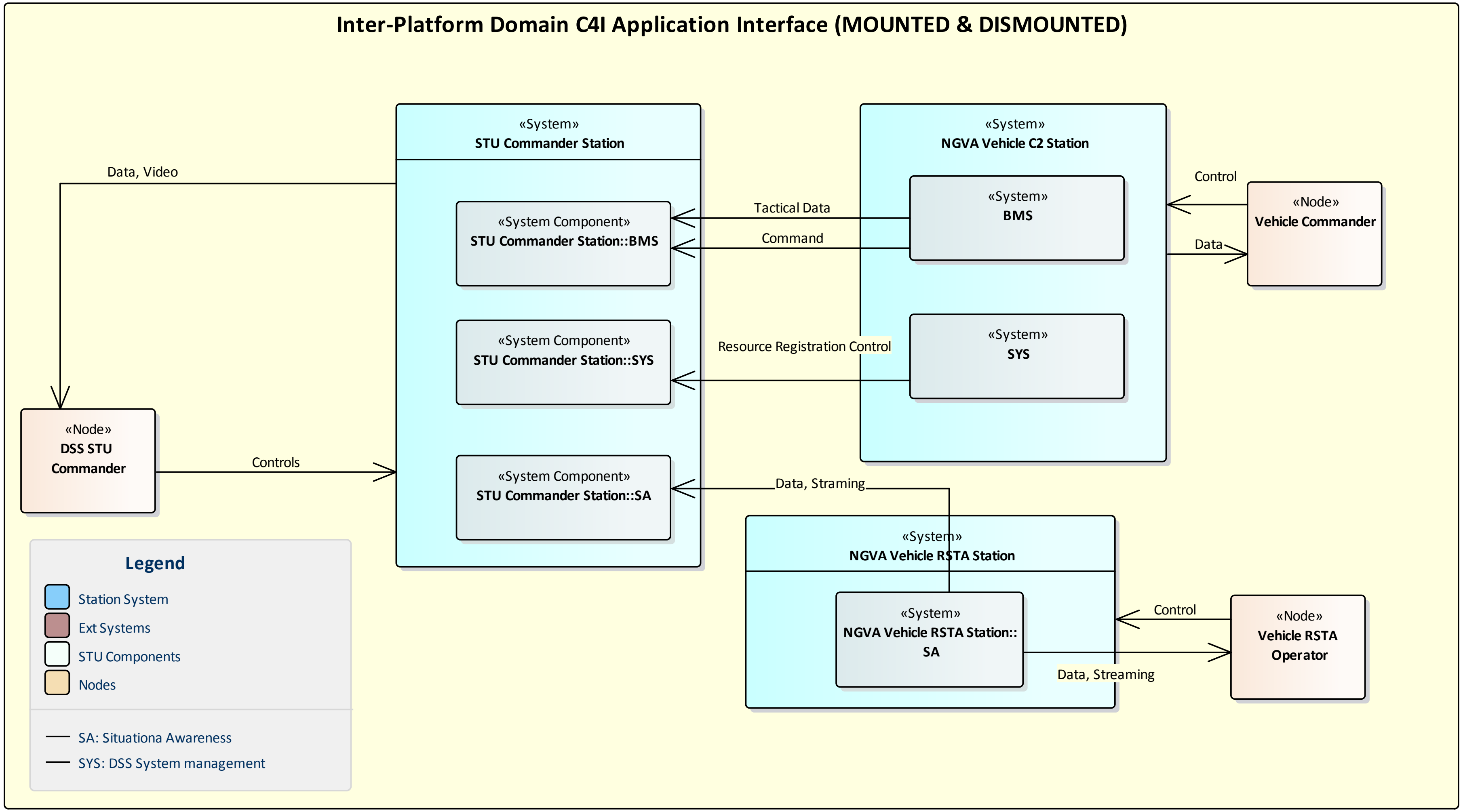


Figure 2-75 – Inter-Platform Domain – Dismounted STU Commander C4I Application

2.6.1.4.2 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the BMS Service Logic and (ii) the SA Service Logic, and (iii) the SYS Service Logic are listed below.

The BMS Service Logic provides the following logical ports:

- BMS.02, which supports the BMS Services and is mapped on Tactical Data Services, as described in Section 2.6.1.1.2
- BMS.02N, which supports the BMS Services and is mapped on Tactical Data Services for Narrowband Radio, as described in Section 2.6.1.1.2
- BMS.08, which supports the BMS Services and is mapped on Tactical File Transfer, as described in Section 2.6.1.1.2
- BMS.08N, which supports the BMS Services and is mapped on Tactical File Transfer for Narrowband Radio, as described in Section 2.6.1.1.2

The SA Service Logic provides the following logical ports:

- SA.02, which supports the SA Services and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- SA.04, which supports the Streaming for the SA Services and is mapped on Streaming Data Services as described in Section 2.6.1.1.2.
- SA.06, which supports the SA Services and is mapped on Inter-Platform File Transfer Services, as described in Section 2.6.1.1.2

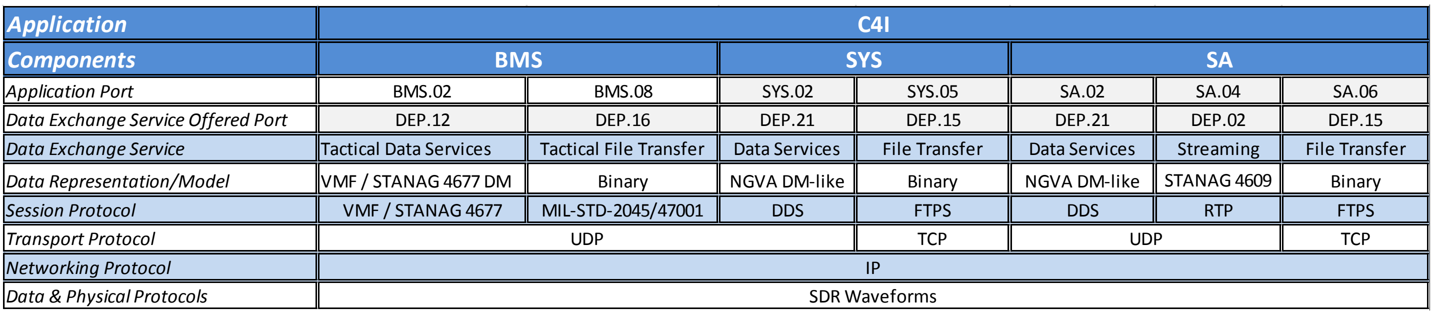
The SYS Service Logic provides the following logical ports:

- SYS.02, which supports the SYS Services and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- SYS.05, which supports the SYS Services and is mapped on Inter-Platform File Transfer Services, as described in Section 2.6.1.1.2

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.6.1.2.2.

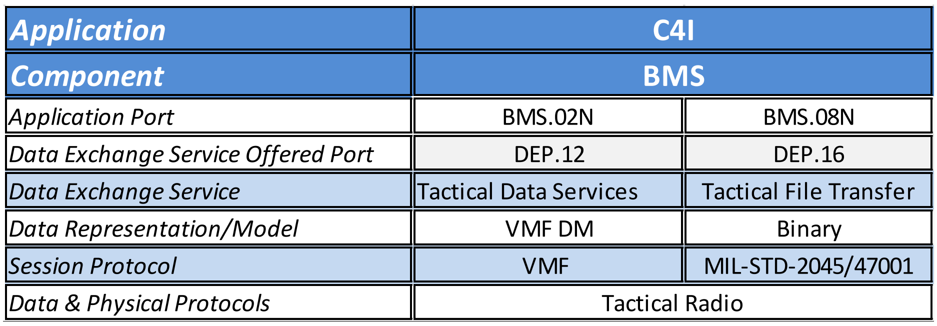
Figure 2-76 summarizes the C4I Application protocol stacks in the domain.

Figure 2-77 summarizes the C4I Application protocol stacks in the domain for the narrowband radio network.



Application	C4I						
Components	BMS		SYS		SA		
Application Port	BMS.02	BMS.08	SYS.02	SYS.05	SA.02	SA.04	SA.06
Data Exchange Service Offered Port	DEP.12	DEP.16	DEP.21	DEP.15	DEP.21	DEP.02	DEP.15
Data Exchange Service	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Data Services	Streaming	File Transfer
Data Representation/Model	VMF / STANAG 4677 DM	Binary	NGVA DM-like	Binary	NGVA DM-like	STANAG 4609	Binary
Session Protocol	VMF / STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	DDS	RTP	FTPS
Transport Protocol	UDP			TCP	UDP		TCP
Networking Protocol	IP						
Data & Physical Protocols	SDR Waveforms						

Figure 2-76 – Inter-Platform Domain – Inter-Platform C4I Application Protocol Stacks



Application	C4I	
Component	BMS	
Application Port	BMS.02N	BMS.08N
Data Exchange Service Offered Port	DEP.12	DEP.16
Data Exchange Service	Tactical Data Services	Tactical File Transfer
Data Representation/Model	VMF DM	Binary
Session Protocol	VMF	MIL-STD-2045/47001
Data & Physical Protocols	Tactical Radio	

Figure 2-77 – Inter-Platform Domain – Inter-Platform C4I Application Protocol Stacks for Tactical Protocol directly deployed on Radio Network (No IP Networking)

2.6.1.4.3 C4I Application System to System Port Connectivity

The C4I Application which is serving a Dismounted STU Commander, who acts in the Inter-Platform Domain exchange data with peers system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.02, which interconnects with:
  - Vehicle BMS to
    - Receive Commands, Tactical Data
    - Send Tactical Data
- BMS.02N, which interconnects with:
  - Vehicle BMS to
    - Receive Commands, Tactical Data
    - Send Tactical Data
- BMS.08, which interconnects with:
  - Vehicle BMS to
    - Send / Receive Tactical Files, e.g. Map
- BMS.08N, which interconnects with:
  - Vehicle BMS to
    - Send / Receive Tactical Files

The SYS Service Logic component exchanges data via the following logical ports:

- SYS.02, which interconnects with:
  - Vehicle Resource Registration Service to:
    - Publish NGVA Registration Protocol Topics
    - Subscribe NGVA Registration Protocol Topics
  - Vehicle Arbitration Service to:
    - Publish NGVA Arbitration Protocol Topics
    - Subscribe NGVA Arbitration Protocol Topics
  - Vehicle SYS to:
    - Receive Management Commands
    - Send Data
- SYS.03, which interconnects with:
  - Vehicle SYS to:
    - Send / Receive Files, e.g. DSS Configuration Files.

The SA Service Logic component exchanges data via the following logical ports:

- SA.02, which interconnects with:
  - The Vehicle SA Component to
    - Send/ Receive Data
- SA.04, which interconnects with:
  - The Vehicle SA Component to
    - Send/ Receive Streaming of live data, e.g. Video
- SA.06, which interconnects with:
  - The Vehicle SA Component to
    - Send/ Receive Files, e.g. Images

2.6.1.5 Human RAS Interaction

2.6.1.5.1 Human RAS Interaction Interface Description

The figure below depicts the main components and related interconnections of the Human RAS Interaction (HRI), which equips an RAS Control Team who operates in the Inter-Platform Domain, e.g. the RAS Team interacts with a Vehicle for the control of the RAS.

Under the hypothesis that an Vehicle is equipped with the necessary components to operate the RAS, e.g. RAS Mission Control and RAS Payload Control, Vehicle Commander coordinates with the STU Commander to acquire the control of the RAS. This coordination procedure is supported by the following components hosted at the STU Commander Station:

- Resource Registration, which provides for RAS registration as NGVA Resource to the Vehicle.
- Arbitration, which provides for coordination protocol in the sharing of the RAS as an NGVA Resource.

Both of the listed components interact with the peer components hosted at Vehicle, typically at the Vehicle C2 Station.

Resource Registration hosted at STU Commander Station provides for registration services to the RAS Management component.

Arbitration component hosted at STU Commander Station provides for RAS Coordinate Sharing to the Commander SA Function, which in turn commands the RAS Mission Control about the ownership of the RAS Control.

Unique ID	Type	Requirement Description
REQ-85	**CR**	Resource Registration shall provide for the registration of a RAS as an NGVA Resource to a Vehicle.
REQ-86	**CR**	The arbitration shall support the coordination procedure for the sharing of RAS Control between a DSS STU and a Vehicle.

Table 2-27 – Inter-Platform Domain Dismounted Soldier - Human RAS Interaction Requirements

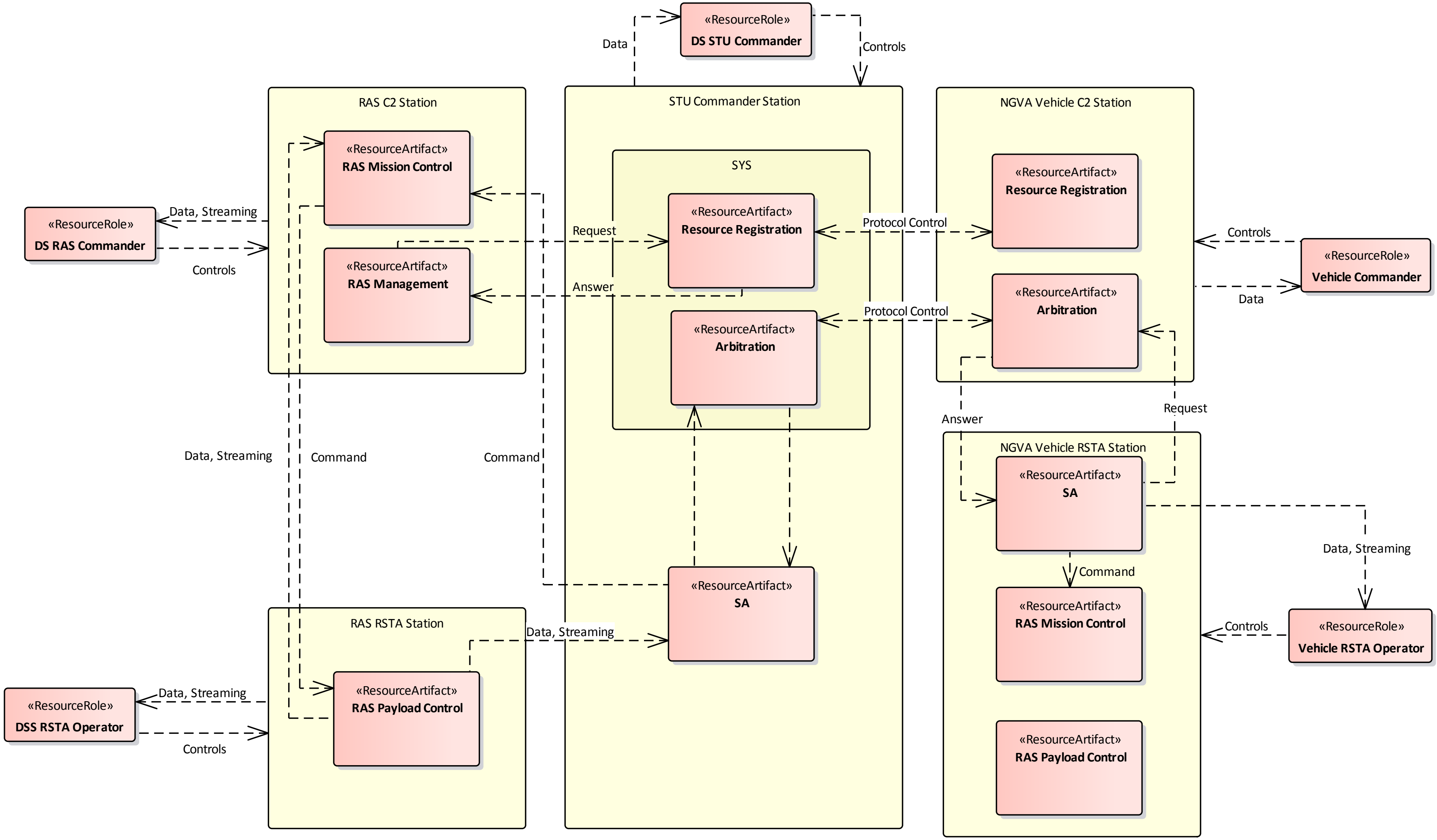


Figure 2-78 – Human RAS Interaction for Inter-Platform Domain Dismounted Soldier

2.6.1.5.2 Human RAS Interaction Port Specification

A Human RAS Interaction provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the RAS Payload Control, (ii) RAS Mission Control, and RAS Management are listed below.

The RAS Payload Control (RAS_PC) provides the following logical ports:

- RAS_PC.01, which supports the RAS Payload Control Services and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- RAS_PC.02, which supports the Streaming for the RAS Payload Control Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.

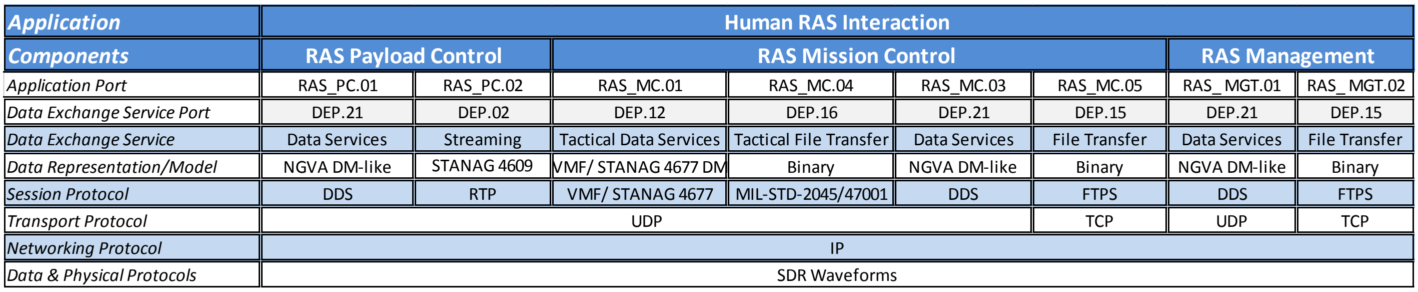
The RAS Mission Control (RAS_MC) provides the following logical ports:

- RAS_ MC.01, which supports the RAS Mission Control Services in the Inter-Platform Domain and is mapped on Tactical Data Services, as described in Section 2.6.1.1.2
- RAS_ MC.03, which supports the RAS Mission Control Services and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- RAS_ MC.04, which supports the RAS Mission Control Services and is mapped on Inter-Platform Tactical File Transfer Services, as described in Section 2.6.1.1.2
- RAS_ MC.05, which supports the RAS Mission Control Services and is mapped on Inter-Platform File Transfer Services, as described in Section 2.6.1.1.2

The RAS Management (RAS_MGT) provides the following logical ports:

- RAS_ MGT.01, which supports the RAS Management Services and is mapped on Inter-Platform Data Services, as described in Section 2.6.1.1.2
- RAS_ MGT.02, which supports the RAS Management Services and is mapped on Inter-Platform File Transfer Services, as described in Section 2.6.1.1.2

Figure 2-79 summarizes the HRI Application protocol stacks in this domain.



Application	Human RAS Interaction							
Components	RAS Payload Control		RAS Mission Control				RAS Management	
Application Port	RAS_PC.01	RAS_PC.02	RAS_MC.01	RAS_MC.04	RAS_MC.03	RAS_MC.05	RAS_ MGT.01	RAS_ MGT.02
Data Exchange Service Port	DEP.21	DEP.02	DEP.12	DEP.16	DEP.21	DEP.15	DEP.21	DEP.15
Data Exchange Service	Data Services	Streaming	Tactical Data Services	Tactical File Transfer	Data Services	File Transfer	Data Services	File Transfer
Data Representation/Model	NGVA DM-like	STANAG 4609	VMF/ STANAG 4677 DM	Binary	NGVA DM-like	Binary	NGVA DM-like	Binary
Session Protocol	DDS	RTP	VMF/ STANAG 4677	MIL-STD-2045/47001	DDS	FTPS	DDS	FTPS
Transport Protocol	UDP					TCP	UDP	TCP
Networking Protocol	IP							
Data & Physical Protocols	SDR Waveforms							

Figure 2-79 – Human RAS Interaction Protocol Stacks for Inter-Platform Domain

2.6.1.5.3 Human RAS Interaction System to System Port Connectivity

The Human RAS Interaction which is serving a Vehicle via STU Commander Control in the Inter-Platform Domain exchange data each as specified below.

The RAS Mission Control (RAS_MC) component exchanges data via the following logical ports:

- RAS_ MC.01, which interconnects with:
  - The Vehicle BMS Component to
    - Receive Command
    - Send Tactical Data
- RAS_ MC.03, which interconnects with:
  - The Vehicle SA Component to
    - Send/ Receive Data
- RAS_ MC.04, which interconnects with:
  - The Vehicle BMS Component to
    - Receive Tactical File, e.g. Maps
- RAS_ MC.05, which interconnects with:
  - The Vehicle SA Component to
    - Send/ Receive Files, e.g. Images

The RAS Management (RAS_MGT) component exchanges data via the following logical ports:

- RAS_ MGT.01, which interconnects with:
  - The Vehicle SYS Component to
    - Send NGVA Registration Request
    - Receive NGVA Registration Reply
    - Send/Receive NGVA Arbitration Protocol Data
    - Receive Management Command
    - Send Status Data
- RAS_ MGT.02, which interconnects with:
  - The Vehicle SYS Component to
    - Exchange RAS System Management Files

The RAS Payload Control (RAS_PC) component exchanges data via the following logical ports:

- RAS_ PC.01, which interconnects with:
  - The STU Commander SA Service Logic to
    - Send/Receive Data
- RAS_ PC.02, which interconnects with:
  - The STU Commander SA Service Logic to
    - Send Live Data Streaming, e.g. Video

2.6.2 Mounted Soldier

2.6.2.1 Data Exchange Services

2.6.2.1.1 Data Exchange Services Port Specification

The Data Exchange Protocol (DEP) component provides the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Vehicle Mounted Soldier Inter-Platform Domain (use of NGVA is assumed);
- Required Port, which requests services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the Vehicle Mounted Soldier Domain are:

- Offered Ports:
  - DEP.21: Inter-Platform Data Services, which provides services for exchanging data between a Mounted DSS Node and the hosting Vehicle.
  - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio, between a Mounted DSS Node and the hosting Vehicle.
  - DEP.12: Tactical Data Services, which provides for exchanging tactical data between a Mounted DSS Node and the hosting Vehicle.
- Required Ports:
  - DEP.23: NGVA Transport Services, which request for transport of (tactical) data/streaming among the Vehicles network endpoints.
  - DEP.05: Execution Platform API, which requests for services supporting the execution of the DEP threads.

Each logical port is supported by an appropriated protocol stack as described below:

- DEP.21 provides the API for an Inter-Platform Data Services based on the protocol stack described in 2.5.2.2. The following protocols are a candidate to implement the Data Session Protocol for DEP in the Inter-Platform Domain:
    - Data Distribution Services for Real-Time Systems[/20/, /21/, /22/,/23/]
- DEP.02 provides the API for an Inter-Platform Data Services based on the protocol stack described in 2.5.2.2. Next, the recommendation to implement the Streaming Session Protocol for DEP in the Inter Platform Domain:
    - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]
- DEP.12 provides the API for a Tactical Data Services based on the protocol stack described in 2.5.2.2. The following protocols are a candidate to implement the Tactical Data Protocol for DEP in the Inter-Platform Domain:
  - Joint Dismounted Soldier System Interoperability Network (JDSSIN) [/13/,/14/,/15/,/16/,/17/]
  - Variable Message Format [/25/]
- DEP.23 requires for NGVA Transport Services in the Vehicle Network. It can serve both Inter-Platform Data Services, Streaming Data Services, and Tactical Data Services. The protocol stack is described in 2.5.2.2;
- DEP.05 requires for Execution Environment Services, it is mapped on the API of the Execution Environment provided by the hosting computer platform.

	BMS Domain				
Data Exchange Service Offered Port	DEP.02	DEP.02	Undefined	DEP.02	DEP.02
Data Exchange Service	**System / Situational Awareness Data**	**BMS Data covered by NGVA**	**Proprietary-BMS-Services**	**NJDSS-based BMS**	**VMF-based BMS**
Data Representation/Model	NGVA Datamodel	NGVA Datamodel	Proprietary	NJDSS-DM (STANAG 4677) (DEP.12)	VMF-DM (DEP.12)
Session Protocol	DDS / RTPS (DEP.21)	DDS / RTPS (DEP.21)		NJDSS (STANAG 4677) (DEP.12)	NJDSS (STANAG 4677) (DEP.12)
Transport Protocol	UDP	UDP		UDP	UDP
Network	IP	IP		IP	IP
Data Link and Physical	Ethernet				

🟩 Required 🟦 Recommend 🟪 Required if physical interface is available 🟧 Undefined

Data Exchange Service Offered Port	DEP.02	DEP.02
Data Exchange Service	**Voice Communication**	**Video-Streams**
Data Representation/Model	RTP	DEF-STAN 00-082
Session Protocol	SIP	DEF-STAN 00-082
Transport Protocol	UDP	DEF-STAN 00-082
Network	IP	IP
Data Link and Physical	Ethernet	

🟩 Required 🟦 Recommend

🟪 Required if physical interface is available 🟧 Undefined

Figure 2-80 – Inter-Platform Domain – Mounted Soldier System Protocol Stack

2.6.2.1.2 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component which is serving DSS Nodes, who act as Mounted Soldier of a Vehicle, i.e. in the Inter-Platform Domain, exchange data with Vehicle components as specified below.

The Data Exchange Protocol component provides services via the following logical ports:

- DEP.21, which interconnects with:
  - The Soldier Application Service Logic to:
    - Send / Receive User Data and Service Control Data
- DEP.12, which interconnects with:
  - The Soldier Application Service Logic to:
    - Send / Receive Tactical Data and Service Control Data
  - The Remote Peripheral(s) Service Logic to:
    - Send / Receive Tactical Data and Service Control Data
- DEP.02, which interconnects with:
  - The Soldier Application Service Logic to:
    - Send Streaming Data
    - Send / Receive Service Control Data

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.23, which interconnects with:
  - NGVA Transport Services, which are the Transport Services of the NGVA Network Infrastructure, to:
    - Send / Receive User Data, Tactical Data, Streaming Data, and Service Control Data
- DEP.05, which interconnects with:
  - Execution Environment API, to:
    - Send / Receive Service Control Data

2.6.2.2 Soldier Application

2.6.2.2.1 Soldier Application Interface Description

The figure below depicts the main components and related interconnection of a Soldier Application, which equips a Specialist Soldier acting in the Inter-Platform Domain as mounted on a Vehicle.

This diagram highlight the capability for a Commander Application to request for Services to a Vehicle Application. In this interaction, the Commander Application Service Logic acts as Consumer of Services provided by the Vehicle Application Service Logic.

The relationships between Soldier Application and NGVA Application are bidirectional, i.e. the NGVA Service Logic could request a service to the Service Logic of the Commander Application.

Alternatively, following the NGVA HMI Design guidelines, the Commander Application HMI could directly interact with the Vehicle Service Logic.

It is worth noting the NGVA Service Logic provides the access to the NGVA Services, e.g. Registration Services, Arbitration Services, Resource Usage Services.

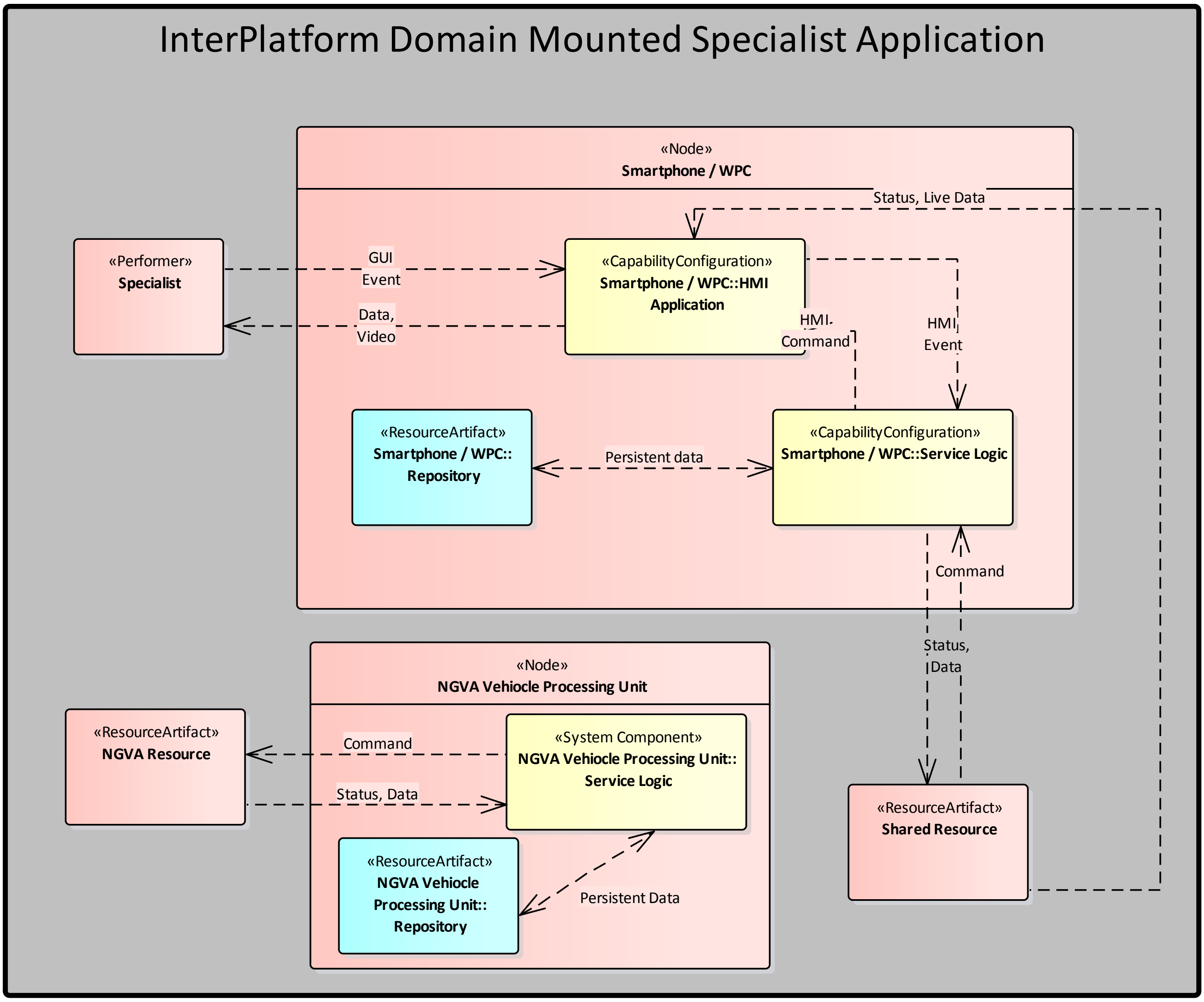


Figure 2-81 – Inter-Platform Domain – Mounted Specialist Application

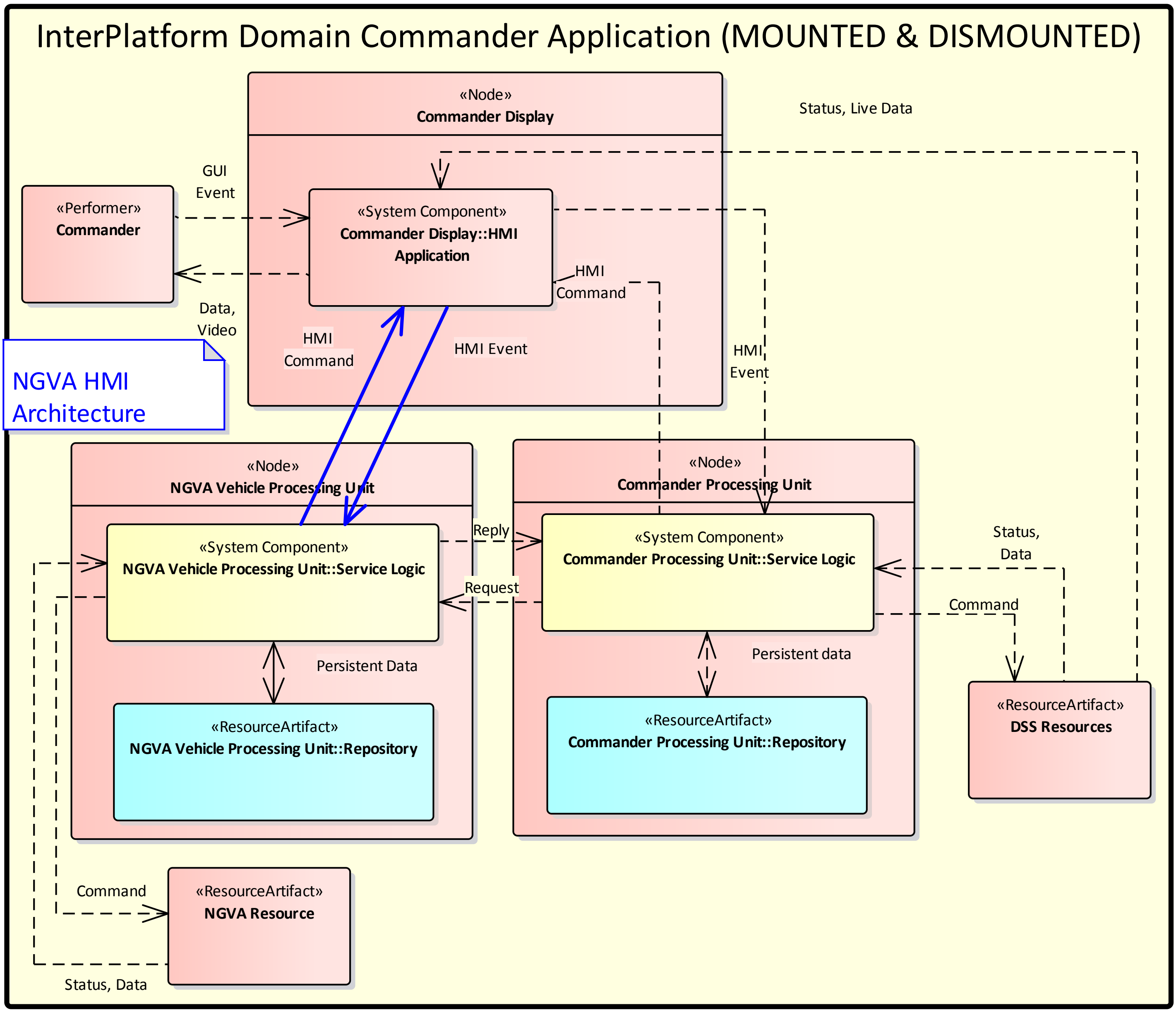

InterPlatform Domain Commander Application (MOUNTED & DISMOUNTED)
«Node» Commander Display
«Performer» Commander
GUI Event
Data, Video
«System Component» Commander Display::HMI Application
HMI Command
HMI Event
HMI Command
HMI Event
Status, Live Data
NGVA HMI Architecture
«Node» NGVA Vehicle Processing Unit
«System Component» NGVA Vehicle Processing Unit::Service Logic
Persistent Data
«ResourceArtifact» NGVA Vehicle Processing Unit::Repository
Reply
Request
«Node» Commander Processing Unit
«System Component» Commander Processing Unit::Service Logic
Persistent data
«ResourceArtifact» Commander Processing Unit::Repository
Status, Data
Command
«ResourceArtifact» DSS Resources
Command
«ResourceArtifact» NGVA Resource
Status, Data

Figure 2-82 – Inter-Platform Domain – Mounted STU Commander Application

Unique ID	Type	Requirement Description
REQ-87	**OE**	When a Specialist Soldier is mounted on-board a Vehicle (NGVA implementation is assumed), a Specialist Application should be able to request for Services to a Vehicle Application. In this interaction, the Specialist Application Service Logic acts as Consumer of Services provided by the Vehicle Application Service Logic.
REQ-88	**OE**	When a Specialist Soldier is mounted on-board a Vehicle, a Specialist Application should be able to provide for Services to a Vehicle Application. In this interaction, the Commander Application Service Logic acts as Provider of Services for the Vehicle Application Service Logic.
REQ-89	**OE**	When an STU Commander is mounted on-board a Vehicle, an STU Commander Application should be able to request for Services to a Vehicle Application. In this interaction, the STU Commander Application Service Logic acts as Consumer of Services provided by the Vehicle Application Service Logic.
REQ-90	**OE**	When an STU Commander is mounted on-board a Vehicle, an STU Commander Application should be able to provide for Services to a Vehicle Application. In this interaction, the STU Commander Application Service Logic acts as Provider of Services for the Vehicle Application Service Logic.
REQ-91	**OE**	When an STU Commander is mounted on-board a Vehicle, The STU Commander Application HMI should be able to directly interact with the Vehicle Service Logic.

Table 2-28 – Inter-Platform Domain - Mounted Specialist Application Requirements

The Diagram View and requirements for STU Commander Application are the same defined for the Inter-Platform Domain: Dismounted Soldier, see the next paragraph.

2.6.2.2.2 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the STU Commander Application HMI and (ii) the Application Service Logic are listed below.

The STU Commander Application HMI provides the following logical ports:

- HMI.03, which supports the Streaming for the Application HMI Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs
- HMI.04, which supports the Application HMI Services in the Inter-Platform Domain for Soldier Mounted on Vehicles and is mapped on Inter-Platform Data Services, as described in Section 2.6.2.1.1.

The Application Service Logic provides the following logical ports:

- ServiceLogic.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.
- ServiceLogic.07, which supports the Application Service Logic in the Inter-Platform Domain for Soldier Mounted on Vehicles and is mapped on Tactical Data Services, as described in Section 2.6.2.1.1.

2.6.2.2.3 Soldier Application System to System Port Connectivity

The Soldier Application which is serving an STU Commander, who acts as a Mounted Soldier in a Vehicle exchange data with peers system component as specified below.

The Application HMI component exchanges data via the following logical ports:

- HMI.04, which interconnects with:
  - the Vehicle Service Logic to:
    - Receive HMI Command, Data
    - Send HMI Event
- HMI.03, which interconnects with:
  - Vehicle Service Logic to:
    - Receive Streaming of live data, e.g. Video

The Application Service Logic component exchanges data via the following logical ports:

- ServiceLogic.07, which interconnects with:
  - the Vehicle Service Logic to:
    - Send Data
    - Receive Data
- ServiceLogic.06, which interconnects with:
  - the Vehicle Service Logic to:
    - Send Streaming of live data, e.g. Video
    - Receive Streaming of live data, e.g. Video

2.6.2.3 Communication Components

The Communication component is the same as the one for STU Domain, which is described in section 2.5.4.

2.6.2.4 C4I Application

2.6.2.4.1 C4I Application Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equips a Mounted STU Commander who acts in the Inter-Platform Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant Vehicle Components, STU Commander could interact with to perform C4I Services in the Inter-Platform Domain.

The HRI component is not shown because it is described in a dedicated paragraph.

The Interconnections among each C4I component with the Vehicle C4I Components is described below:

- BMS component at STU Commander Station interacts with:
  - BMS at Vehicle C2 Station to acquire Vehicle Commander commands, and exchange the needed (Tactical) Data.
- SYS component at STU Commander Station interacts with:
  - SYS at Vehicle C2 Station to manage Resource Registration protocol.
- SA component at STU Commander Station interacts with:
  - SA at Vehicle C2 Station to gather the needed Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

• Unique ID	Type	Requirement Description
REQ-92	**CR**	Mounted STU Commander C4I Application shall interact with BMS at Vehicle C2 Station to acquire Vehicle Commander commands, and exchange the needed (Tactical) Data.
REQ-93	**CR**	Mounted STU Commander C4I Application shall interact with SYS at Vehicle C2 Station to manage Resource Registration protocol.
REQ-94	**CR**	Mounted STU Commander C4I Application shall interact with SA at Vehicle C2 Station to gather the needed Data and Streaming, e.g. Video Streaming, Object of Interest Tracking & Position.

Table 2-29 – Inter-Platform Domain – Mounted STU Commander C4I Application Requirements

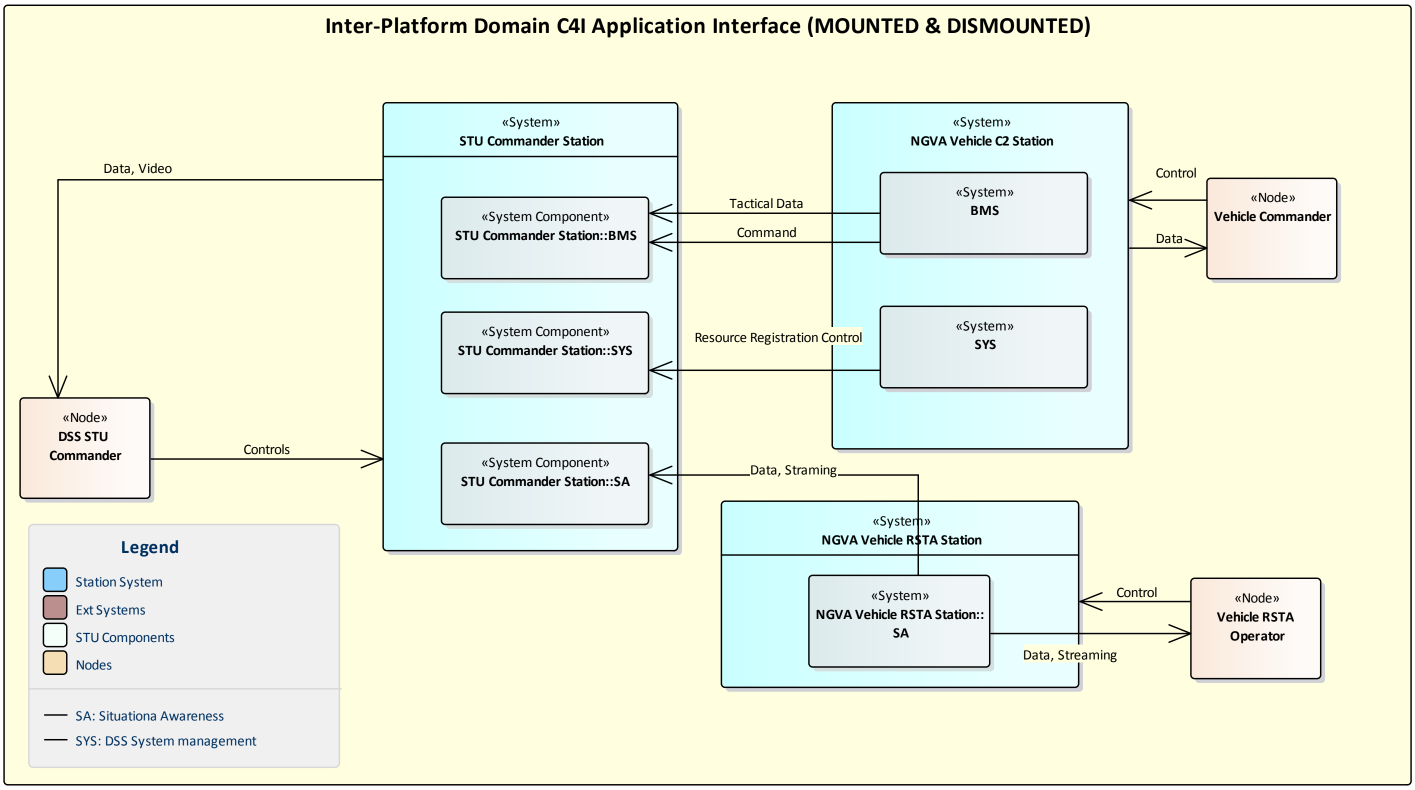


Figure 2-83 – Inter-Platform Domain – Mounted STU Commander C4I Application

2.6.2.4.2 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the BMS Service Logic and (ii) the SA Service Logic, and (iii) the SYS Service Logic are listed below.

The BMS Service Logic provides the following logical ports:

- BMS.06, which supports the Streaming for the BMS Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.
- BMS.07, which supports the BMS Services in the Inter-Platform Domain for Soldier Mounted on Vehicles and is mapped on Tactical Data Services, as described in Section 2.6.2.1.1.

The SA Service Logic provides the following logical ports:

- SA.04, which supports the Streaming for the SA Services and is mapped on Streaming Data Services as described in relevant Data Exchange Domain paragraphs.
- SA.05, which supports the SA Services in the Inter-Platform Domain for Soldier Mounted on Vehicles and is mapped on Inter-Platform Data Services, as described in Section 2.6.2.1.1.

The SYS Service Logic provides the following logical ports:

- SYS.04, which supports the SYS Services in the Inter-Platform Domain for Soldier Mounted on Vehicles and is mapped on Inter-Platform Data Services, as described in Section 2.6.2.1.1.

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.6.2.2.2.

2.6.2.4.3 C4I Application System to System Port Connectivity

The C4I Application which is serving an STU Commander, who acts in the Inter-Platform Domain as Mounted Soldier of a Vehicle, exchange data with peers' system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.07, which interconnects with:
  - The Vehicle BMS Component to
    - Send Tactical Data
    - Receive Commands, Tactical Data
- BMS.06, which interconnects with:
  - The Vehicle SA Component to
    - Receive Streaming of live data, e.g. Video

The SYS Service Logic component exchanges data via the following logical ports:

- SYS.04, which interconnects with:
  - Vehicle Resource Registration Service to:
    - Publish NGVA Registration Protocol Topics
    - Subscribe NGVA Registration Protocol Topics
  - Vehicle Arbitration Service to:
    - Publish NGVA Arbitration Protocol Topics
    - Subscribe NGVA Arbitration Protocol Topics

The SA Service Logic component exchanges data via the following logical ports:

- SA.05, which interconnects with:
  - The Vehicle SA Component to
    - Send Data
    - Receive Data
- SA.04, which interconnects with:
  - The Vehicle SA Component to
    - Receive Streaming of live data, e.g. Video
    - Send Streaming of live data, e.g. Video

2.7 Joint Domain

2.7.1 Data Exchange Services

2.7.1.1 Data Exchange Services Interface Description

The figure below depicts the main components and related interconnections of the Data Exchange Services, which serve an STU Commander acting in the Joint Forces Domain.

The Data Exchange Protocol components of STU Commander and a Joint Forces peer node interact via a Joint Force Gateway, which executes the necessary processing and control on data, which are moving between different stakeholders domains.

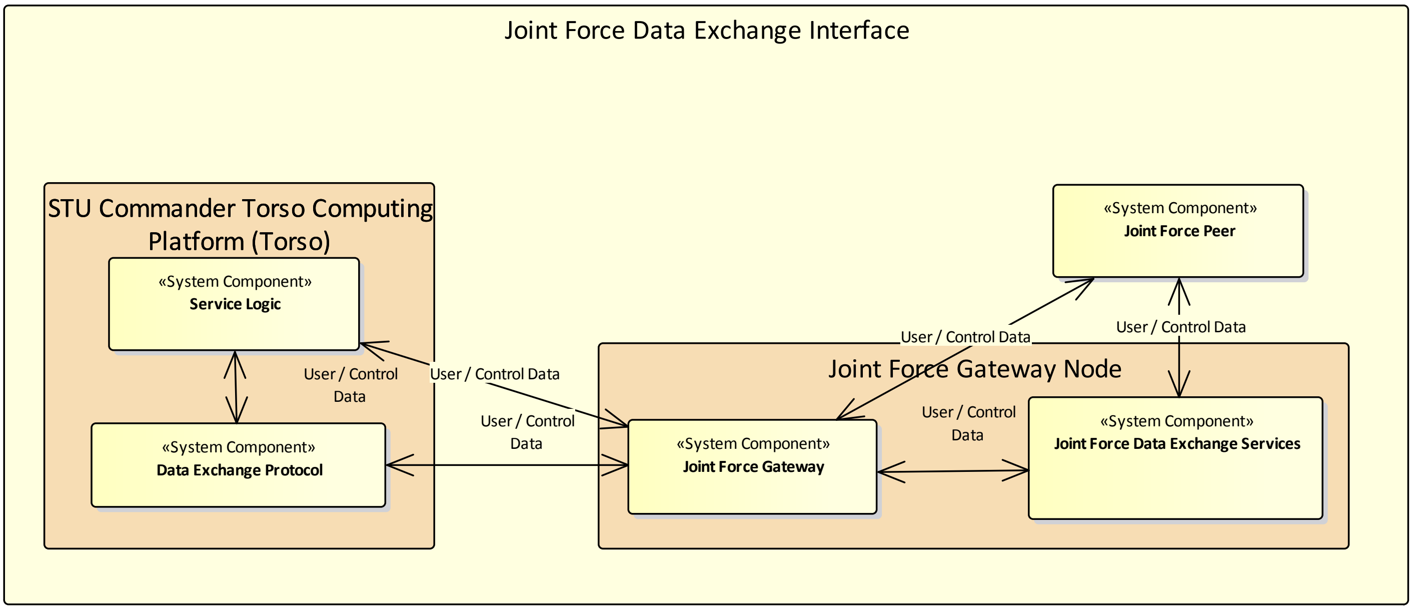

Joint Force Data Exchange Interface
STU Commander Torso Computing Platform (Torso)
«System Component» Service Logic
«System Component» Data Exchange Protocol
User / Control Data
User / Control Data
User / Control Data
Joint Force Gateway Node
«System Component» Joint Force Gateway
User / Control Data
«System Component» Joint Force Data Exchange Services
User / Control Data
User / Control Data
«System Component» Joint Force Peer

Figure 2-84 – Joint Forces Domain – STU Commander Data Exchange Services

2.7.1.2 Data Exchange Services Port Specification

The Data Exchange Protocol (DEP) component provides the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Joint Forces Domain;
- Required Port, which requests services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the STU Domain are:

- Offered Ports:
  - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio.
  - DEP.12: Tactical Data Services, which provides for exchanging tactical data between an STU Commander and a Joint Force peers via the Joint Force Gateway, as described in Section 2.7.1.1.

- Required Ports:
    - DEP.13: Radio Transport Services, which request for transport of data/streaming among the Joint Forces radio network endpoints.
    - DEP.14: Radio Tactical Transport Services, which request for transport of tactical data among the Joint Forces radio network endpoints.
    - DEP.05: Execution Platform API, which request for services supporting the execution of the DEP threads.

Each logical port is supported by an appropriated protocol stack as described below:

- DEP.02 provides the API for Streaming Data Services based on the protocol stack described in 2.5.2.2. Next, the recommendation to implement the Streaming Session Protocol for DEP in the Personal Domain:
        - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]
- DEP.12 provides the API for a Tactical Data Services based on the protocol stack described in 2.5.2.2. The following protocols are a candidate to implement the Tactical Data Protocol for DEP in the Joint Forces Domain:
    - Joint Dismounted Soldier System Interoperability Network (JDSSIN) [/13/,/14/,/15/,/16/,/17/]
    - Variable Message Format [/25/]
- DEP.13 requires for Radio Transport Services in a Joint Forces radio area network. It serves Tactical Data Services. The protocol stack is described in section 2.5.2.2 ;
- DEP.14 requires for Tactical Radio Transport Services in a Joint Forces radio area network. It serves Tactical Data Services. The protocol stack is described in section 2.5.2.2;
- DEP.05 requires for Execution Environment Services, it is mapped on the API of the Execution Environment provided by the hosting computer platform.

2.7.1.3 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component which is serving an STU Commander DSS Node, who acts in the Joint Forces Domain, exchange data with Joint Forces peer node(s) as specified below.

The Data Exchange Protocol component provides services via the following logical ports:

- DEP.02, which interconnects with:
    - The Soldier Application Service Logic to:
        - Send Streaming Data
        - Send / Receive Service Control Data
- DEP.12, which interconnects with:
    - The Soldier Application Service Logic to:
        - Send / Receive Tactical Data and Service Control Data

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.13, which interconnects with:
    - Radio Transport Services, which are the Transport Services of the Radio Network serving the Joint Forces Domain, to:
        - Send / Receive User Data, Streaming Data, and Service Control Data

- DEP.14, which interconnects with:
  - Tactical Radio Transport Services, which are the Transport Services of the Tactical Radio Network serving the Joint Forces Domain, to:
    - Send / Receive Tactical Data, and Service Control Data
- DEP.05, which interconnects with:
  - Execution Environment API, to:
    - Send / Receive Service Control Data

2.7.2 Soldier Application

2.7.2.1 Soldier Application Interface Description

The figure below depicts the main components and related interconnections of a Soldier Application, which equips an STU Commander who acts in the Joint Forces Domain.

This diagram highlight the capability for a Commander Application to request for Services to a Joint Node, e.g. an Airforce UAV. In this interaction, the Commander Application Service Logic acts as Consumer of Joint Node Service.

The data exchange between the STU Commander Application and Joint Forces Peer Node could be bidirectional.

Each Data Exchange is mediated via a Joint Force Gateway, which executes the necessary processing and control on data, which are moving between different stakeholders domains.

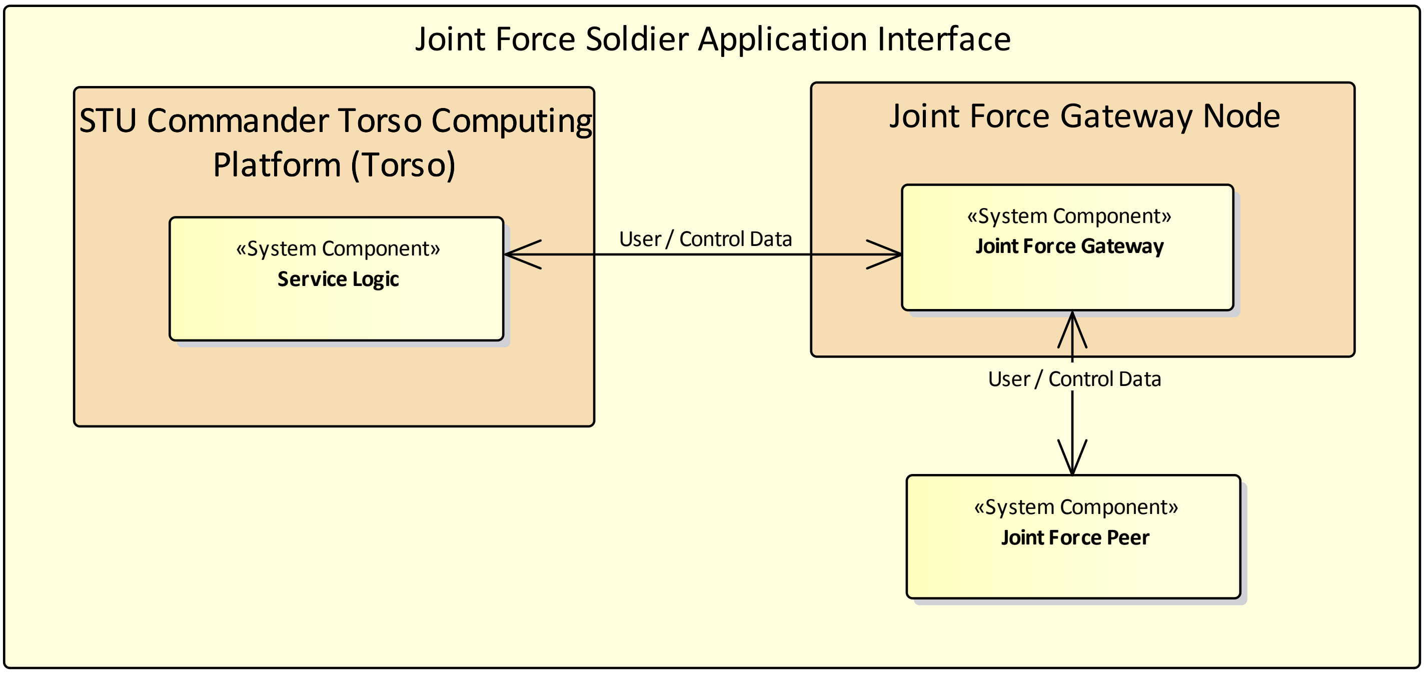


Figure 2-85 – Joint Forces Domain – STU Commander Application

Unique ID	Type	Requirement Description
REQ-95	**OE**	A Commander Application should be able to request for Services to a Joint Force Node via an appropriate Joint Gateway. In this interaction, the Commander Application Service Logic acts as Consumer of Joint Node Services.
REQ-96	**OE**	A Commander Application should be able to provide for Services to a Joint Node Application via an appropriate Joint Gateway. In this interaction, the Commander Application Service Logic acts as Provider of Services for the Joint Node.

Table 2-30 – Joint Forces Domain - STU Commander Application Requirements

2.7.2.2 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the STU Commander Application HMI and (ii) the Application Service Logic are listed below:

- ServiceLogic.04, which supports the Application Service Logic in the Joint Force Domain and is mapped on Tactical Data Services, as described in Section 2.7.1.2
- ServiceLogic.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in Section 2.7.1.2

2.7.2.3 DSS Application System to System Port Connectivity

The Soldier Application which is serving an STU Commander, who acts in the Joint Forces Domain exchange data with peers system component as specified below.

The Application Service Logic component exchanges data via the following logical ports:

- ServiceLogic.04, which interconnects with:
  - The Joint Force Gateway to
    - Send Data
    - Receive Data

2.7.3 Communication Components

The Communication component is the same as the one for STU Domain, which is described in section 2.5.4.

2.7.4 C4I Application

2.7.4.1 C4I Application Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equips an STU Commander who acts in the Joint Forces Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant C4I Components of a Joint Forces Node.

The Interconnections among each C4I component with the Vehicle C4I Components is described below:

- BMS component at STU Commander Station interacts with:
    - BMS at Joint Forces Node C4I Station to exchange the needed (Tactical) Data via the Joint Forces Gateway.

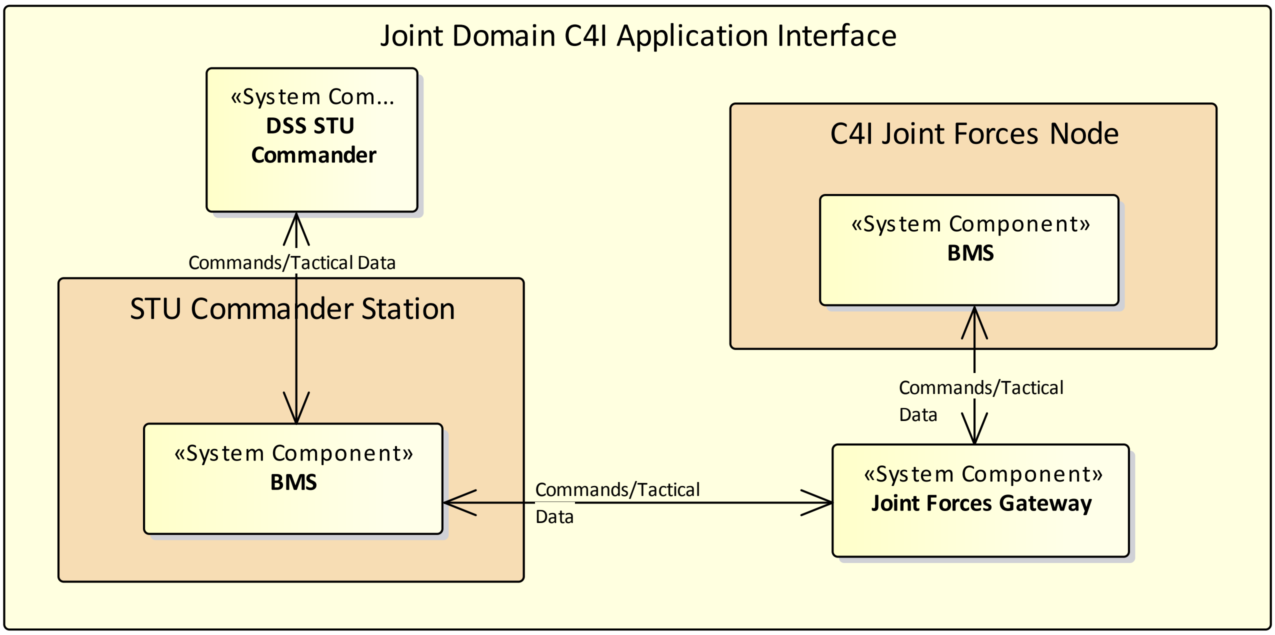


Figure 2-86 – Joint Forces Domain –STU Commander C4I Application

Unique ID	Type	Requirement Description
REQ-97	**CR**	STU Commander C4I Application shall interact with BMS at Joint Forces Node C4I Station to exchange the needed (Tactical) Data via the Joint Forces Gateway.

Table 2-31 – Joint Forces Domain – C4I Application Requirements

2.7.4.2 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the BMS Service Logic and (ii) the SA Service Logic, and (iii) the SYS Service Logic are listed below.

The BMS Service Logic provides the following logical ports:

- BMS.04, which supports the BMS Services Tactical Data in the Joint Force Domain and is mapped on Tactical Data Services, as described in Section 2.7.1.2
- BMS.06, which supports the Streaming for the BMS Services and is mapped on Streaming Data Services as described in Section 2.7.1.2

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.7.2.2.

2.7.4.3 C4I Application System to System Port Connectivity

The C4I Application which is serving an STU Commander, who acts in the Joint Forces Domain exchange data with peers system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.04, which interconnects with:
    - The Joint Force Gateway to
        - Send Tactical Data
        - Receive Tactical Data

2.8 Coalition Domain

2.8.1 Data Exchange Services

2.8.1.1 Data Exchange Services Interface Description

The figure below depicts the main components and related interconnections of the Data Exchange Services, which serve an STU Commander acting in the Coalition Domain.

The Data Exchange Protocol components of STU Commander and a Coalition peer node interact via a Coalition Gateway, which executes the necessary processing and control on data, which are moving between different stakeholders domains.

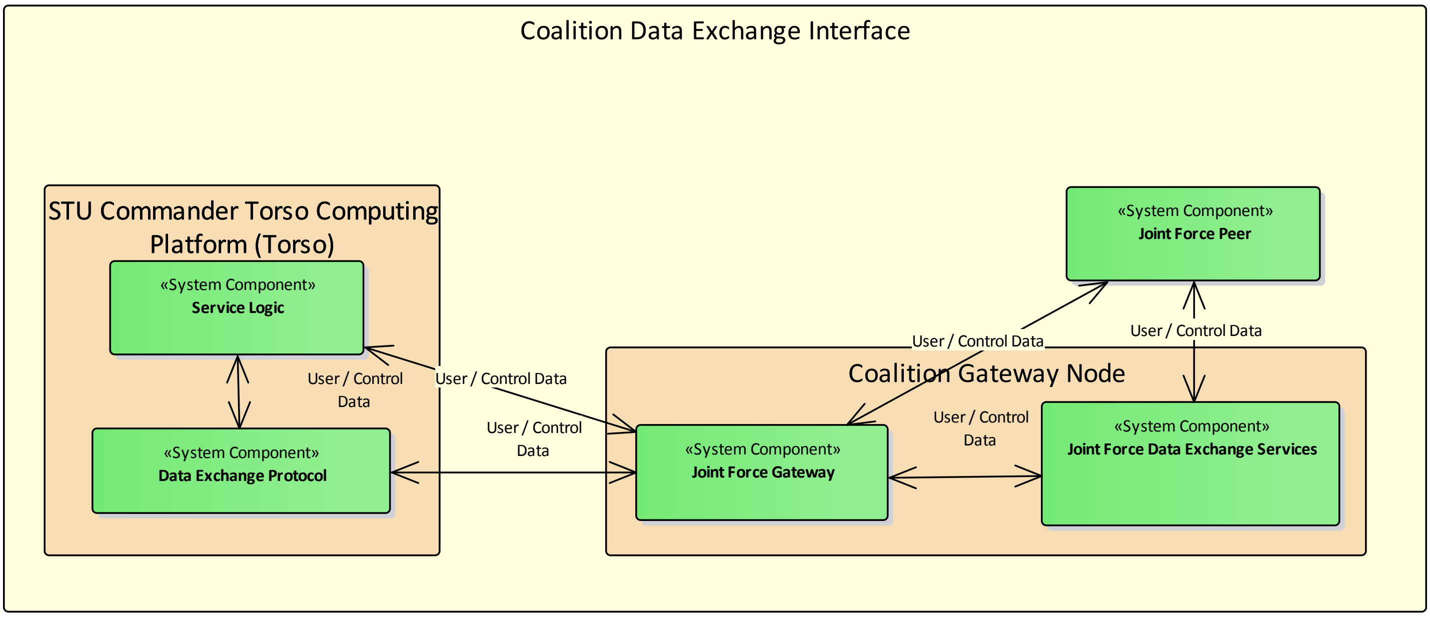


Figure 2-87 – Coalition Domain – STU Commander Data Exchange Services

2.8.1.2 Data Exchange Services Port Specification

The Data Exchange Protocol (DEP) component provides the following kinds of logical ports:

- Offered Port, which provides Data Exchange Services in the Coalition Domain;
- Required Port, which request services to underlying layers, namely Transport Services and Execution Environment.

The set of logical ports in the STU Domain are:

- Offered Ports:
  - DEP.02: Streaming Data Services, which provides services for distributing streaming of data, e.g. Video, Audio.
  - DEP.12: Tactical Data Services, which provides for exchanging tactical data between an STU Commander and a Coalition peers via the Coalition Gateway, as described in Section 2.8.1.1.
- Required Ports:
  - DEP.13: Radio Transport Services, which request for transport of data/streaming among the Coalition radio network endpoints.
  - DEP.14: Radio Tactical Transport Services, which request for transport of tactical data among the Coalition radio network endpoints.
  - DEP.05: Execution Platform API, which request for services supporting the execution of the DEP threads.

Each logical port is supported by an appropriated protocol stack as described below:

- DEP.02 provides the API for Streaming Data Services based on the protocol stack described in 2.5.2.2. Next, the recommendation to implement the Streaming Session Protocol for DEP in the Personal Domain:
  - STANAG 4609 AEDP-8 (Edition 4) for Video Streaming [/34/]
- DEP.12 provides the API for a Tactical Data Services based on the protocol stack described in 2.5.2.2. The following protocols are a candidate to implement the Tactical Data Protocol for DEP in the Coalition Domain:
  - STANAG 4677, Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability)) (JDSSIN) [/13/,/14/,/15/,/16/,/17/]
  - Variable Message Format [/25/]
- DEP.13 requires for Radio Transport Services in a Coalition radio area network. It serves data/streaming Services. The protocol stack is described in 2.5.2.2.
- DEP.14 requires for Tactical Radio Transport Services in a Coalition radio area network. It serves Tactical Data Services. The protocol stack is described in 2.5.2.2;
- DEP.05 requires for Execution Environment Services, it is mapped on the API of the Execution Environment provided by the hosting computer platform.

2.8.1.3 Data Exchange Services System to System Port Connectivity

The Data Exchange Protocol component which is serving an STU Commander DSS Node, who acts in the Coalition Domain, exchange data with Coalition peer node(s) as specified below.

The Data Exchange Protocol component provides services via the following logical ports:

- DEP.02, which interconnects with:
  - The Soldier Application Service Logic to:
    - Send Streaming Data
    - Send / Receive Service Control Data
- DEP.12, which interconnects with:
  - The Soldier Application Service Logic to:
    - Send / Receive Tactical Data and Service Control Data

The Data Exchange Protocol component requires services to underlying layers namely, Execution Environment Services and Transport Services, via the following logical ports:

- DEP.13, which interconnects with:
  - Radio Transport Services, which are the Transport Services of the Radio Network serving the Coalition Domain, to:
    - Send / Receive User Data, Streaming Data, and Service Control Data
- DEP.14, which interconnects with:
  - Tactical Radio Transport Services, which are the Transport Services of the Tactical Radio Network serving the Coalition Domain, to:
    - Send / Receive Tactical Data, and Service Control Data
- DEP.05, which interconnects with:
  - Execution Environment API, to:
    - Send / Receive Service Control Data

2.8.2 Soldier Application

2.8.2.1 Soldier Application Interface Description

The figure below depicts the main components and related interconnection of a Soldier Application, which equips a Dismounted STU Commander who acts in the Coalition Domain.

The Application Service Logic exchanges data directly via the Data Exchange Services agreed by the Allied Nations, e.g. STANAG 4677 (DSS C4 Interoperability) (/16/)

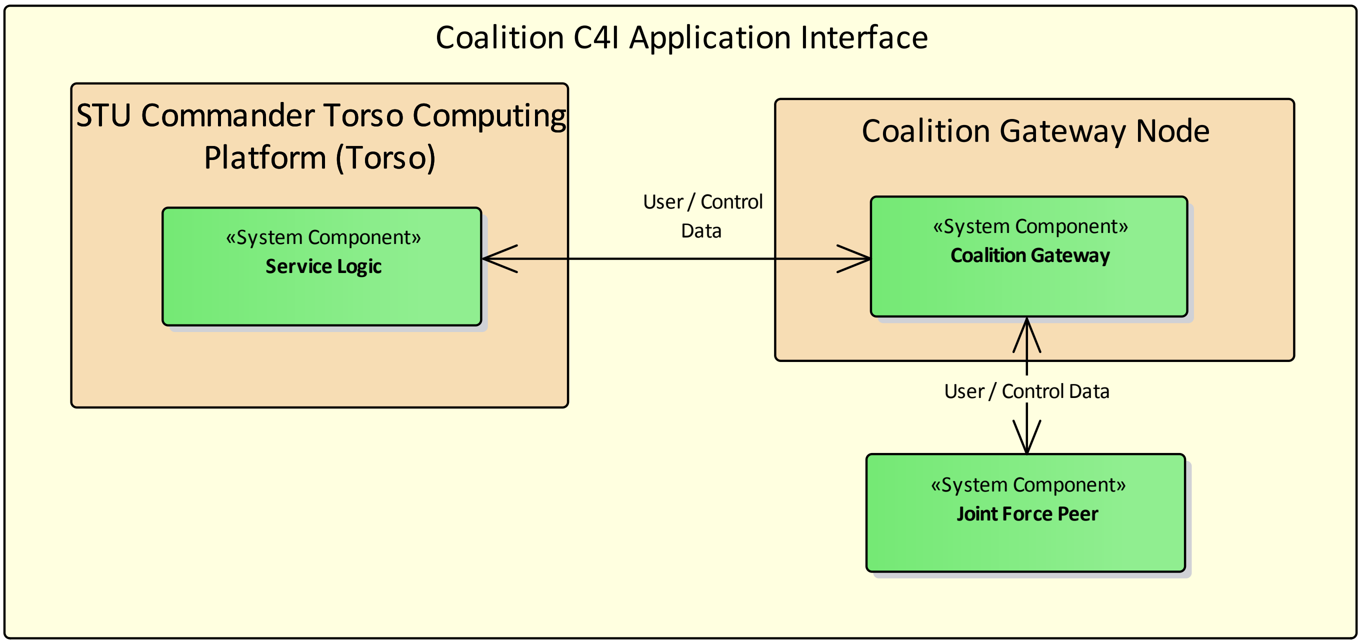


Figure 2-88 – Coalition Domain – STU Commander Application

Unique ID	Type	Requirement Description
REQ-98	**OE**	A Commander Application should be able to access the Data Exchange Services for the Coalition Domain to exchange information with an Allied Node via an appropriate Squad-to-Squad Coalition Interoperability Gateway.
REQ-99	**CR**	A Commander Application should be able to integrate/fuse the received Coalition Data with the National Situational Awareness data already present in the application.
REQ-100	**CR**	A Commander Application should be able to exchange the received Coalition Data with the Soldier with the other members in his squad (Soldier Applications)
REQ-101	**CR**	A Commander Application should be able (automatically or manually) to select the relevant information items to be exchanged with coalition partners.

Table 2-32 – Coalition Forces Domain - STU Commander Application Requirements

2.8.2.2 Soldier Application Port Specification

A Soldier Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The set of logical ports supported respectively by (i) the STU Commander Application HMI and (ii) the Application Service Logic are listed below:

- ServiceLogic.05, which supports the Application Service Logic in the Coalition Domain and is mapped on Tactical Data Services, as described in Section 2.8.1.2
- ServiceLogic.06, which supports the Streaming for the Application Service Logic and is mapped on Streaming Data Services as described in Section 2.8.1.2.

2.8.2.3 Soldier Application System to System Port Connectivity

The Soldier Application which is serving an STU Commander, who acts in the Coalition Domain exchange data with peers system component as specified below.

The Application Service Logic component exchanges data via the following logical ports:

- ServiceLogic.05, which interconnects with:
  - The Coalition Gateway to
    - Send Data
    - Receive Data

2.8.3 Communication Components

The Communication component is the same as the one for STU Domain, which is described in section 2.5.4.

2.8.4 C4I Application

2.8.4.1 C4I Application Interface Description

The figure below depicts the main components and related interconnection of a C4I Application, which equips an STU Commander who acts in the Coalition Domain.

This diagram specifies the interconnections of the C4I System Components with the relevant C4I Components of an Allied Forces Node.

The Interconnections among each C4I component with the Vehicle C4I Components is described below:

- BMS component at STU Commander Station interacts with:
  - BMS at Allied Forces Node C4I Station to exchange the needed (Tactical) Data and Commands via the Squad-to-Squad Coalition Interoperability Gateway.

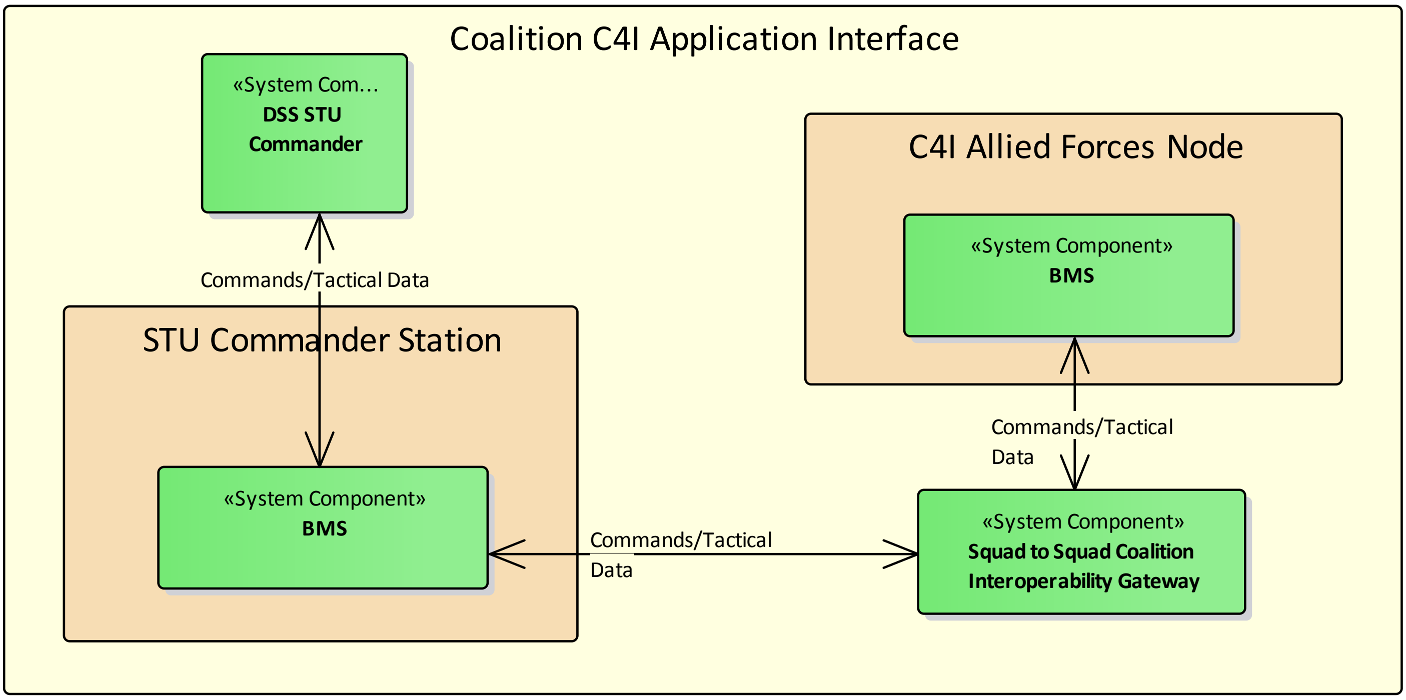


Figure 2-89 – Coalition Domain –STU Commander C4I Application

Unique ID	Type	Requirement Description
REQ-102	**CR**	STU Commander C4I Application shall interact with BMS at Allied Forces Node C4I Station to exchange the needed (Tactical) Data and Commands via the Squad-to-Squad Coalition Interoperability Gateway.

Table 2-33 – Coalition Domain – C4I Application Requirements

2.8.4.2 C4I Application Port Specification

A C4I Application provides a set of logical ports to exchange data with peers' system components in the different domains.

The figure below summarizes the set of logical ports supported respectively by (i) the BMS Service Logic and (ii) the SA Service Logic, and (iii) the SYS Service Logic.

The BMS Service Logic provides the following logical ports:

- BMS.05, which supports the BMS Services in the Coalition Domain and is mapped on Tactical Data Services as described in Section 2.8.1.2
- BMS.06, which supports the Streaming for the BMS Services and is mapped on Streaming Data Services as described in Section 2.8.1.2.

The C4I Application is a specialization of the Soldier Application, then the C4I HMI provides the same set of logical ports as the STU Commander Application HMI as specified in Section 2.8.2.2.

2.8.4.3 C4I Application System to System Port Connectivity

The C4I Application which is serving an STU Commander, who acts in the Coalition Domain exchange data with peers system component as specified below.

The BMS Service Logic component exchanges data via the following logical ports:

- BMS.05, which interconnects with:
    - The Coalition Gateway to
        - Send Tactical Data
        - Receive Tactical Data

2.9 System Evolution (NSV-8)

2.9.1 Maintain State of the Art Soldier Systems

GOSSRA endeavours to provide an architectural framework that will enable the soldier system to remain *'State of the Art'*. This means that the technological design and features of the soldier system, based on the GOSSRA architecture, should be comparable with the latest technologies prevalent in the world market at any particular time. This is a tall order and requires an understanding of the management of the research and innovation process required to achieve it. In order to keep the soldier system state of the art it is necessary to understand two major aspects.

Firstly, the evolution of a soldier system over time in terms of current technologies and methodologies will happen through a *dual process of modern technology and current operational needs* driving the innovation cycle of research, development, prototyping, and production. This is compounded by the lengthy military procurement process, which invariably results in the procurement of systems already nearing obsolescence. This implies that any development and production agency should have a lead time that will cater for the time required for these stages of technology readiness and procurement process to synchronize. This, in turn, necessitates the fact that there needs to be in place a long-term commitment between the procurement agency and the industry.

Secondly, it is necessary to have a process in place that allows innovation that is not too costly to integrate, given the need to integrate the different innovation cycles of mechanical (8-10 years), electronic hardware (4 - 6 years), and software (1-2 years) components/sub-systems for a soldier system. In terms of a soldier system, where both sensor and software development fall in the category of fast innovation cycles, it is important to introduce interfaces between different innovation cycles such that parts are able to innovate independently from each other and the rest of the system. Automatic rollout and distribution of software, including anti-virus updates and regular component upgrades is here a key issue.

Mere 'Obsolescence Management' or developing an 'Obsolescence Management Strategy' enables only the life cycle management of equipment from advent to discard, but does not ensure that forces have a state-of-the-art system at all times.

2.9.1.1 Concept of Maintaining a State-of-the-Art Soldier System

Figure 2-90 below illustrates the outline process of converting existing soldier systems into a GOSSRA compatible interoperable soldier system and then keeping the newer versions as State-of-the-Art.

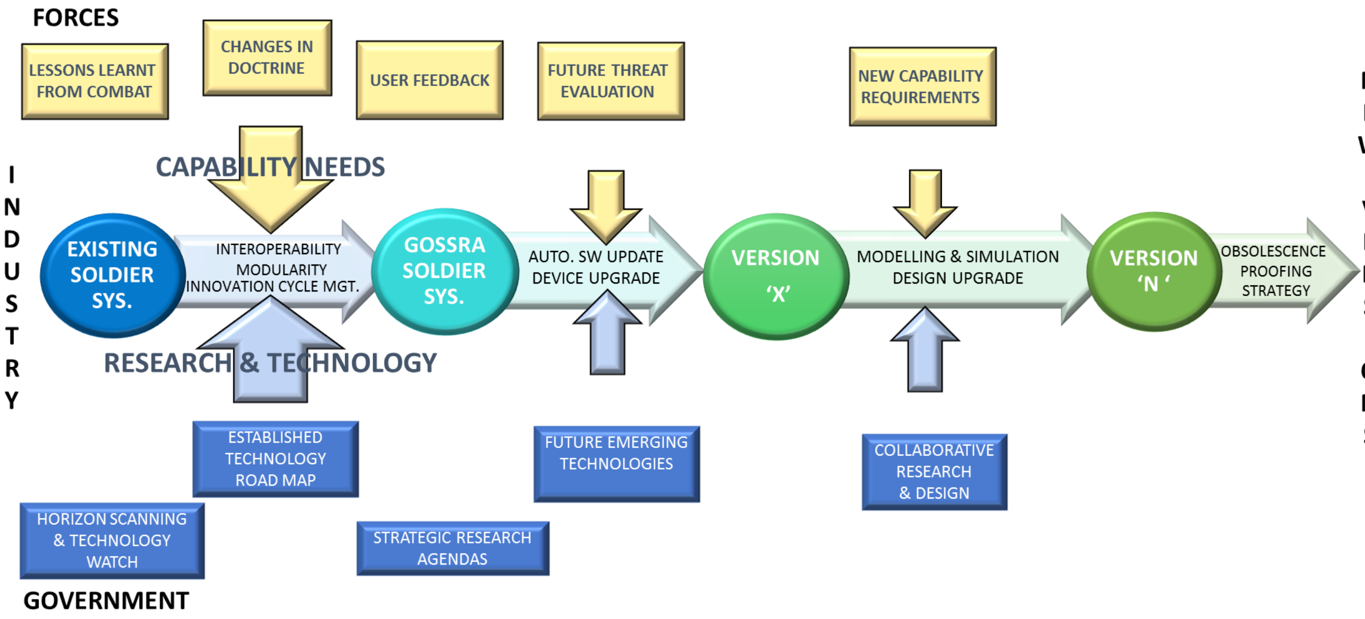

FORCES
LESSONS LEARNT FROM COMBAT
CHANGES IN DOCTRINE
USER FEEDBACK
FUTURE THREAT EVALUATION
NEW CAPABILITY REQUIREMENTS
CAPABILITY NEEDS
INDUSTRY
EXISTING SOLDIER SYS.
INTEROPERABILITY MODULARITY INNOVATION CYCLE MGT.
GOSSRA SOLDIER SYS.
AUTO. SW UPDATE DEVICE UPGRADE
VERSION 'X'
MODELLING & SIMULATION DESIGN UPGRADE
VERSION 'N '
OBSOLESCENCE PROOFING STRATEGY
NEW VERSIONS
RESEARCH & TECHNOLOGY
ESTABLISHED TECHNOLOGY ROAD MAP
FUTURE EMERGING TECHNOLOGIES
COLLABORATIVE RESEARCH & DESIGN
HORIZON SCANNING & TECHNOLOGY WATCH
STRATEGIC RESEARCH AGENDAS
GOVERNMENT

Figure 2-90 – Transition to GOSSRA and Creation of further Versions of Soldier System

In yellow, are the operational inputs or requirements generated by the ***Forces*** or Customers of soldier systems in terms of ***Capability Needs*** translated into general service qualitative requirements based on factors like *Changes in Doctrine, Lessons Learnt During Actual Combat, User Feedback, Anticipated Threat Evaluation* and *New Capability Requirements* identified through EDA/National/Institutional commissioned studies.

In blue, the ***Research and Technology Road Map*** can be found, evolved by the Government through its institutional arrangements of a *Horizon Scanning and Technology Watch*, *Prioritised Technology Areas* based on *Strategic Research Agendas*, identified *Key Enabling Technologies (KET)* and *Future Emerging Technologies (FET).* This would be augmented by the Industry's own R&D covering both civilian and military technological areas.

In green, the ***Industry*** using the GOSSRA framework to develop and produce state-of-the-art soldier systems can be found, which are *interoperable, modular in design,* and have a fast and *cyclic innovation management process* of co-development and co-production. Both, regular *modular device upgrade* and *automated software update* should be a part of the overall system design to ensure *state of the art* happens as a routine and regular process, without having to call back the product to the Base or Factory. The development of new models or periodic *design upgrade* should be expedited through the use of *modelling and simulation* to validate new designs.

Coordinated project management for the synchronised development of different components and parts ensures that the upgrades and updates are rolled out in time. Figure 2-91 illustrates the methodology of bridging the gaps in time of different innovation cycles in a system through the use of interfaces. Synchronizing the development of mechanical, electronic and software (including embedded software) innovation cycles in a cost-effective manner is the need of the hour for the industry.

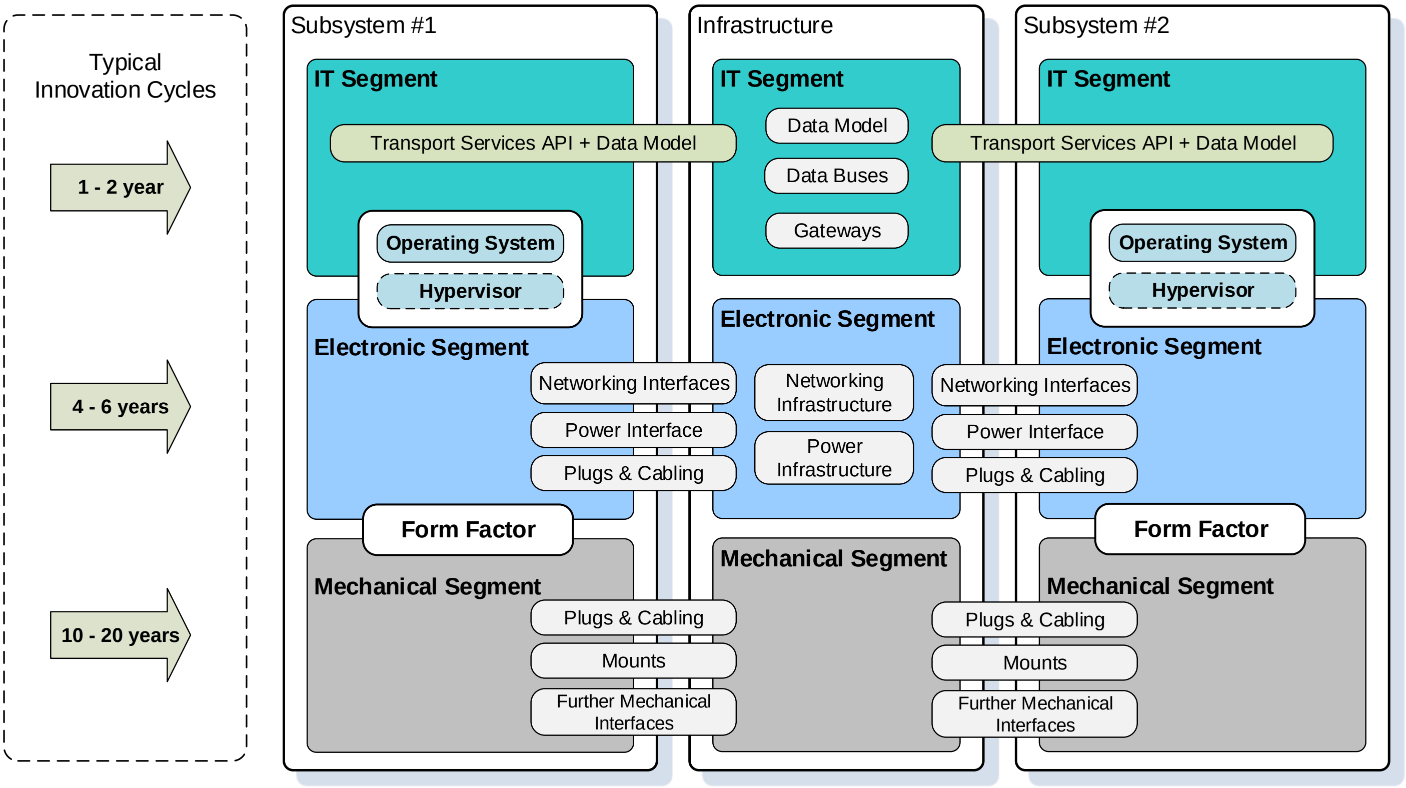


Figure 2-91 – Using Interfaces to Bridge Different Innovation Cycles of Sub-Systems

In order to provide ownership and bring about integration amongst all stakeholders, a ***strategic partnership model*** should be adopted by the government /procurement agency, wherein each stakeholder plays an important role in the overall process of maintaining a state-of-the-art soldier system. Based on the *technological road map* provided by institutional mechanisms of the Government, as well as, project-based *collaborative research and development* by a consortium of industry, academia; and a *capability road map* provided by the force development authorities, military users and acquisition agencies; the research, development and acquisition cycles have to become cyclic and attain a speed that makes it difficult for adversaries to match. Implementation of such a process would require detailed stakeholder identification, public-private partnership, requisite institutional arrangements, steady project funding, assured orders to the industry consortium and a dynamic system of policy review and implementation. Also, industry, through strategic partnership, should be empowered with the capability to look into and monitor future technologies and operational trends, as well as, develop the capability to translate such trends into adopted technologies and operational capability features.

This is the essence of the concept of maintaining a state-of-the-art or cutting-edge technology soldier system.

To enable this concept of maintaining the state of the art to fructify it is important that nations/governments have in place institutional arrangements which help in evolving a capability-based force development plan and an implementation plan, which is funded. An open soldier system architecture to this end will help Governments to adopt a common standard, instead of planning for and investing in such systems on a national basis.

Practical realisation of this conceptual model of maintaining a state-of-the-art soldier system would, therefore, necessitate the evolution of a strategy to not only provide soldiers with a technological edge over their adversaries but also obviate relative obsolescence at any given time, while keeping the costs affordable by alliance member states. A strategy to obviate obsolescence should encompass both a *technology and innovation management strategy* as well as an *obsolescence management strategy.* A *technology and innovation strategy* will ensure the timely injection of new technologies through the evolution of a dynamic technology road map, which drives both future operational capability concepts and meets projected capability needs. An *obsolescence management strategy* ensures optimal performance of the system through its life cycle through timely predictive notices for activities related to the life-time purchase of spares / critical components, discontinuance of procurement, discard and adoption of new versions of soldier systems.

2.9.1.2 Technology and Innovation Management Strategy

The purpose of all defence-related technology and innovation is to be able to meet the operational capability needs of the force. Most nations promote a capability-based approach to force and capability planning, which includes coherent integration of new and emergent technologies into military capability. However, in order to maintain a state-of-the-art soldier system, it is important to be able to accurately assess the future capability requirements and establish a technology and innovation management system for soldier systems.

A Rand Europe study in 2018 on *Exploring Europe’s Capability Requirements for 2035 and Beyond*[4]*,* assesses the long-term requirements and suggests a number of high-level requirements, not specifically related to soldier systems, but will have a significant impact on future soldier systems. These requirements are appended below: -

- **Information Sharing.** Efficient information sharing with joint multinational forces and other actors is an underlying requirement in all six Generic Military Tasks List (GMTL) of Command, Inform, Engage, Protect, Deploy and Sustain. Some measures to build this capability include, using interoperable communication systems; data-sharing systems; training forces on communication with non-military actors, using common technical standards for military and commercial satellite communications, etc.

- **Decision Making.** There is a need to ensure effective and rapid decision making at all levels, supported by enhanced situational awareness in complex, congested battlefields. Some measures to build this capability include, enhancing the surveillance capabilities of individual soldiers through better ISTAR capabilities, AI systems for faster data processing, improved communications, threat recognition, and human cognitive capabilities.

- **Civil-Military Cooperation.** Civil-military cooperation will be necessary to ensure the fulfilment of mission mandates and leverage deeper and common understanding between the armed forces and civilian actors.

- **Mobility.** Mobility is key to allow Member States’ forces to engage in more flexible, agile deployments and operate in complex, contested and hazardous environments. Measures

[4] Kepe, Black, Melling & Plumridge (Rand Europe) - *Insights from the 2018 update of the long-term strand of the Capability Development Plan* (European Defence Agency June 2018)

include reduced logistics, lightweight modular and easily transportable materials and equipment and more independent and self-sustainable deployments.

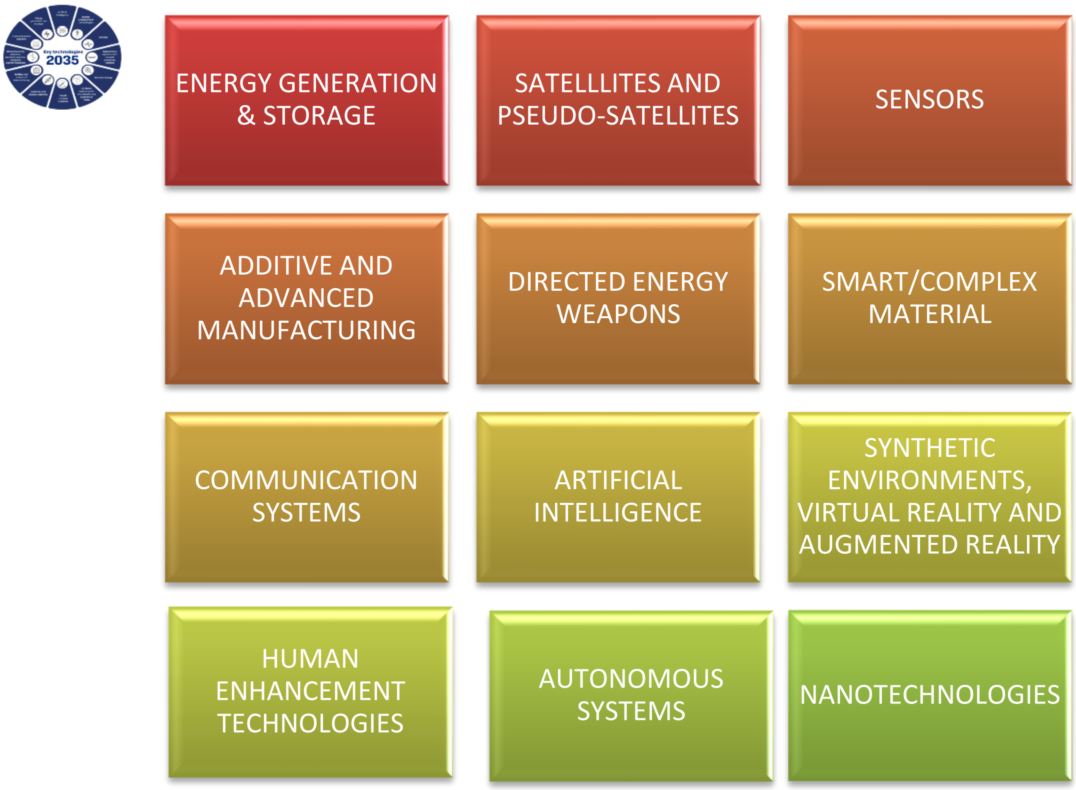
- **Cyber Operations.** Member States' forces need the ability to conduct defensive and offensive cyber operations at the strategic, operational and tactical level, including the ability to disrupt and take control of the adversary's manned and unmanned systems as remotely piloted and autonomous vehicles become more prevalent on the future battlefield.

- **Deploying a Flexible Range of Non-Lethal and Non-Kinetic Effects.** Deploying a flexible range of non-lethal and non-kinetic effects will allow forces to minimise collateral damage while disrupting the adversary's capabilities, such as microwave and sonic-based weapons.

- **Enhancing Individual Soldiers.** Enhancing individual soldiers will empower them with improved information gathering, mobility and resilience to operate in complex, contested environments. Measures may include protection against CBRN threat, DEW and swarm UAVs.

2.9.1.2.1 Technology Research and Industrial Enablers for Future Military Capabilities (2035 and beyond)

Based on this requirement analysis, EDA in June 2018 has identified 12 key technologies, research in which may enable future military capabilities. These key technologies which will impact the development of a state of the art soldier system are depicted in Figure 2-92 below:



ENERGY GENERATION & STORAGE

SATELLLITES AND PSEUDO-SATELLITES

SENSORS

ADDITIVE AND ADVANCED MANUFACTURING

DIRECTED ENERGY WEAPONS

SMART/COMPLEX MATERIAL

COMMUNICATION SYSTEMS

ARTIFICIAL INTELLIGENCE

SYNTHETIC ENVIRONMENTS, VIRTUAL REALITY AND AUGMENTED REALITY

HUMAN ENHANCEMENT TECHNOLOGIES

AUTONOMOUS SYSTEMS

NANOTECHNOLOGIES

Figure 2-92 – Key Technologies Enabling Future Military Capabilities in 2035 + (Source: Rand Europe 2018)

2.9.1.2.2 Research Base & Defence Industry Issues

An important part of the strategy is to be able to mobilise all possible resources (civilian and defence) into the process of research, technology and innovation management. It is important to create project-based consortiums of the industry and academia by more than one member-state / company in their selected areas of technological expertise for effecting collaborative research. Also, an open innovation system comprising SMEs, provided with institutionalised incubation support the moment they achieve a TRL of 5 or 6, would help build a vibrant research and technology innovation eco-system. The last but not least important issue is of focussed and effective funding, which should be 80% by the Government and 20% by Companies till TRL 6 and thereafter on successful production, companies should be reimbursed their 20% expenditure as well and given assured orders. This strategic partnership approach would need to be carefully structured and funded through government financial mechanisms.

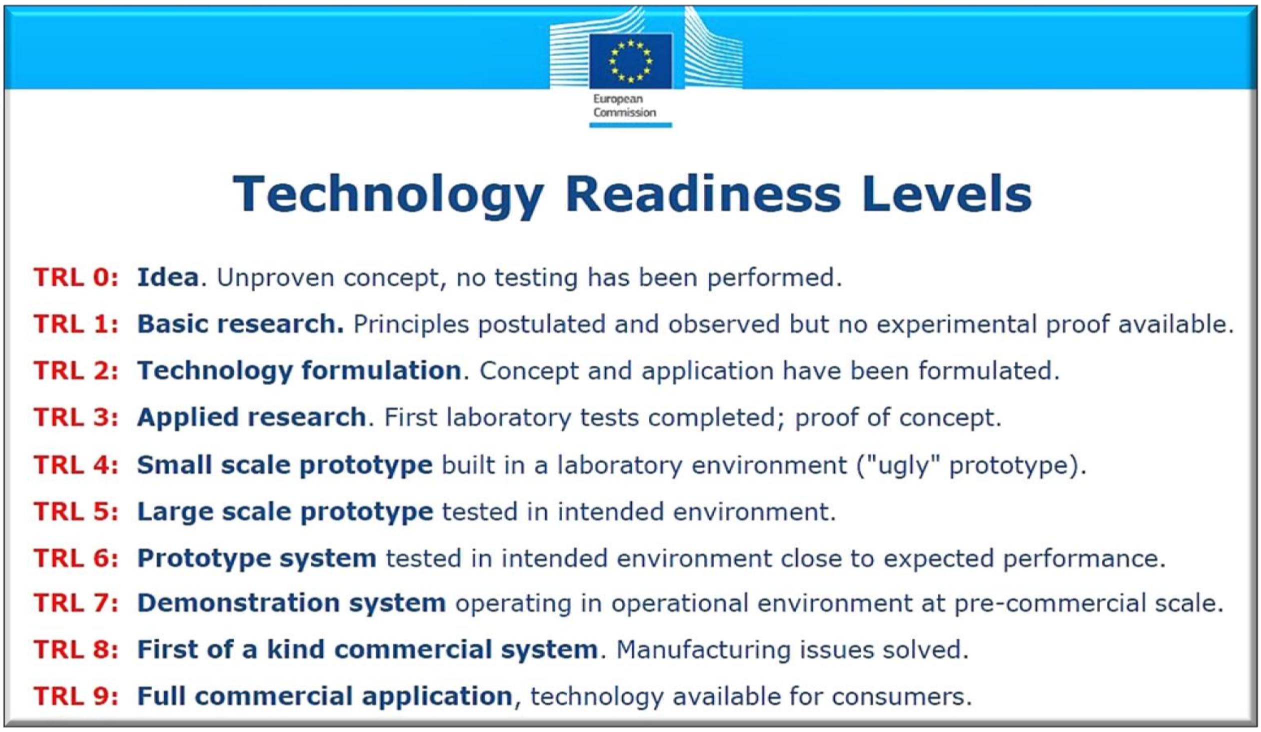
2.9.1.2.3 Horizon Technology Research Funding

Development of a soldier system merely to meet a particular forces' projected capability needs, carries the risk of getting outdated or being disrupted unless a mechanism for long term funding for research and innovation into new areas are institutionalised. This funding should be committed by all alliance nations towards long- term research into future or horizon technologies. Such a decision would obviate national conflicts of interest in terms of large-scale defence expenditures versus more pressing demands on national budgets. In short, while no single country may be able to fund large scale projects, collectively funded joint project-based research programmes may fructify the goal of maintaining a state-of-the-art solder system, which as per the swarm concept of operations, in an evolved and effective Net Centric Operations (NCO) scenario, will act as a system of systems in enhancing military capability.

2.9.1.3 Technology Readiness for Maintaining State of the Art

2.9.1.3.1 Technology Readiness Levels (TRL) and Technology Readiness Assessment (TRA)

The concept of Technology Readiness Levels first instituted on a scale of 7 by NASA in 1974 and then expanded to 9 levels over a period of time is a measure of the level of technology achieved in a particular product or service. The scale of nine has been adopted by most countries and a variety of institutions around the world like the USA, Canada, Australia, EU, OECD, etc. The nine levels of technology readiness or maturity are shown in Figure 2-93 below.



European Commission

Technology Readiness Levels

TRL 0: **Idea**. Unproven concept, no testing has been performed.

TRL 1: **Basic research.** Principles postulated and observed but no experimental proof available.

TRL 2: **Technology formulation**. Concept and application have been formulated.

TRL 3: **Applied research**. First laboratory tests completed; proof of concept.

TRL 4: **Small scale prototype** built in a laboratory environment ("ugly" prototype).

TRL 5: **Large scale prototype** tested in intended environment.

TRL 6: **Prototype system** tested in intended environment close to expected performance.

TRL 7: **Demonstration system** operating in operational environment at pre-commercial scale.

TRL 8: **First of a kind commercial system**. Manufacturing issues solved.

TRL 9: **Full commercial application**, technology available for consumers.

Figure 2-93 – EC Technology Readiness Levels

The maturity level of 6, i.e. when a prototype of the technology has been developed and tested in a relevant environment, is when investors are ready to invest and commit to a large-scale commercial project.

While TRLs have proven to be useful in evaluating a technology’s performance, as demonstrated in the laboratory or in a test environment, they do not inform one whether or not the technology product can actually be produced in an affordable manner. The concept of manufacturing readiness levels (MRL) has been incorporated to expand the TRL idea so that it can incorporate producibility concerns. The MRL approach addresses questions such as the level of technology reproducibility, the cost of production, and technology manufacturing production environment early in the development phase (GAO 2003, DoD 2011).

Another maturity aspect is the readiness of the market for the product or *Market Readiness Level (MRL)*. TRL and MRL are often plotted together to ensure that production and marketing are in sync with each other (See Figure 2-94 below). TRL – Technology Readiness Level – expresses the degree of technology to be used safely by intended and educated users in the envisaged user environment. MRL measures the maturity of a given need in the market considering the potential obstacles. Concurrent, step-by-step market and technology development places the right product into the right market window at the right time.

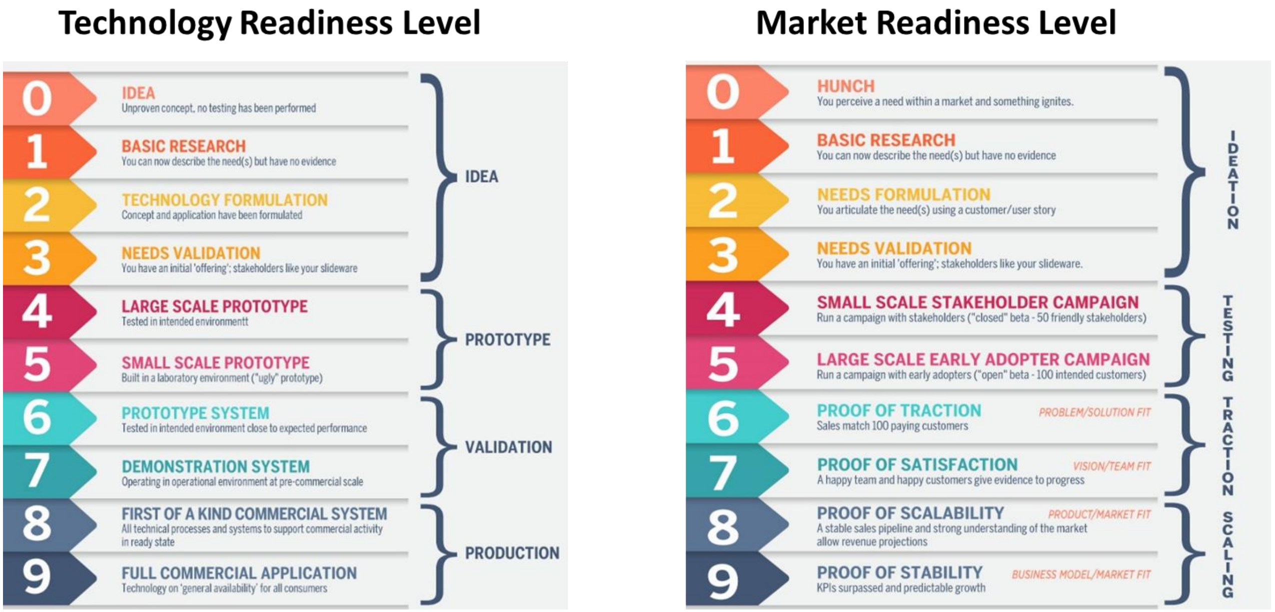

Technology Readiness Level
0
IDEA
Unproven concept, no testing has been performed
1
BASIC RESEARCH
You can now describe the need(s) but have no evidence
2
TECHNOLOGY FORMULATION
Concept and application have been formulated
3
NEEDS VALIDATION
You have an initial 'offering'; stakeholders like your slideware
4
LARGE SCALE PROTOTYPE
Tested in intended environmentt
5
SMALL SCALE PROTOTYPE
Built in a laboratory environment ("ugly" prototype)
6
PROTOTYPE SYSTEM
Tested in intended environment close to expected performance
7
DEMONSTRATION SYSTEM
Operating in operational environment at pre-commercial scale
8
FIRST OF A KIND COMMERCIAL SYSTEM
All technical processes and systems to support commercial activity in ready state
9
FULL COMMERCIAL APPLICATION
Technology on 'general availability' for all consumers
IDEA
PROTOTYPE
VALIDATION
PRODUCTION
Market Readiness Level
0
HUNCH
You perceive a need within a market and something ignites.
1
BASIC RESEARCH
You can now describe the need(s) but have no evidence
2
NEEDS FORMULATION
You articulate the need(s) using a customer/user story
3
NEEDS VALIDATION
You have an initial 'offering'; stakeholders like your slideware.
4
SMALL SCALE STAKEHOLDER CAMPAIGN
Run a campaign with stakeholders ("closed" beta - 50 friendly stakeholders)
5
LARGE SCALE EARLY ADOPTER CAMPAIGN
Run a campaign with early adopters ("open" beta - 100 intended customers)
6
PROOF OF TRACTION
PROBLEM/SOLUTION FIT
Sales match 100 paying customers
7
PROOF OF SATISFACTION
VISION/TEAM FIT
A happy team and happy customers give evidence to progress
8
PROOF OF SCALABILITY
PRODUCT/MARKET FIT
A stable sales pipeline and strong understanding of the market allow revenue projections
9
PROOF OF STABILITY
BUSINESS MODEL/MARKET FIT
KPIs surpassed and predictable growth
IDEATION
TESTING
TRACTION
SCALING

Figure 2-94 – Matching TRL and MRL

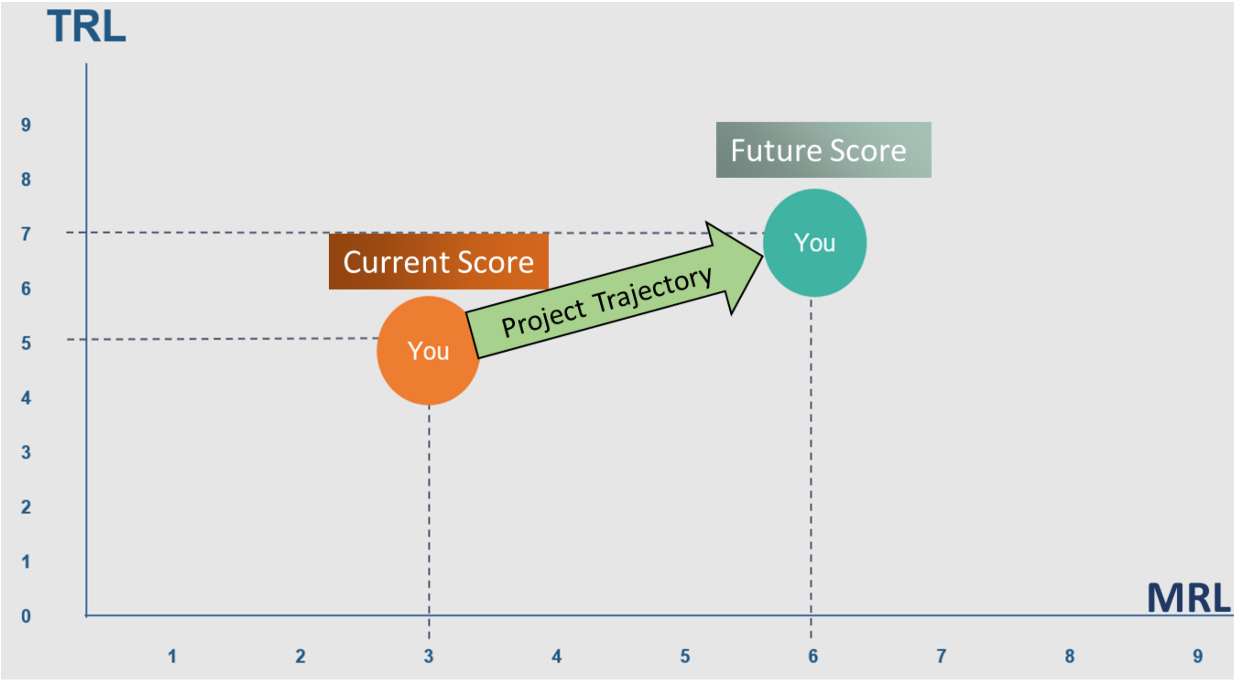


Figure 2-95 – Plotting Project Milestones
(Source: cloudwatchhub.eu)

Plotting of Technology Readiness Level against Market Readiness Level (See Figure 2-95) enables system development milestones to be planned proactively instead of a benchmark approach in each individual scale. It also enables more comprehensive visualisation of the project's trajectory and whether timelines in a project will be achieved.

Yet another aspect is the provisioning of products that are readily available and referred to as commercial off-the-shelf (COTS). Such products, be they hardware, software, or a mixture of both, have hopefully achieved the degree of maturity so that those acquiring them can rely upon their operational properties and that the documentation of the COTS products is sufficient to provide the proper guidance in their use.

The product systems engineer should realize that the TRL assessment for COTS changes dramatically if the operational environment or other requirements are imposed that exceed the design limits of the COTS product (e.g., operations at very high or very cold temperatures, high shock, or vibration levels). GOSSRA should evolve a common Technology Readiness Assessment (TRA) Methodology based on parameters suited to individual projects, level of ambition and operational needs.

2.9.1.4 **Concept of Systems Readiness Levels (SRL)**

Readiness levels are an active research area within academia and government agencies with regard to the integration of technology components into complex systems (integration readiness levels (IRLs)) to address interface maturity among existing and maturing technology developments. TRLs apply to the critical enabling technologies, which are usually embodied at the subsystem, assembly level, or system component level. Systems readiness levels (SRL) are used when going from individual technologies to the whole system. The SRL model is a function of the individual TRLs in a system and their subsequent integration points with other technologies and scales (Sauser 2006).

By adopting a systems' approach for a new soldier system, the correct integration points can be selected for each of the different readiness level (RL) scales - TRL, Manufacturing RL, Integration RL, and Market RL. This will help in the correct selection of milestones to be reached by each scale at any given point of time and enable achievement of realistic project completion timelines.

Yet another aspect is the timing of the acquisition cycle of the soldier system, particularly in the context of defence procurement. Figure 2-96 below depicts the relationship of the three levels of readiness TRL, MRL and System Acquisition Milestones of a system depicted as A, B C below: -

A – Finalisation of Board Drawings (TRL 4) and Manufacturing Processes in the Lab (MRL 4) allows finalisation of Concept & Start of Technology Development.

B – Completion of testing of a prototype in a representative environment (TRL 6) and Finalisation of the Manufacturing process in a representative manufacturing environment (MRL 6) enables System Development for Demonstration and Trials to commence.

C – Finalisation of Prototype in an Operational Environment (TRL 7) and Manufacturing Process in Place for Low-Rate Initial Production - LRIP (MRL 8) allows production and deployment to commence.

FRP – Adopting modern manufacturing processes (like Lean and Industry 4.0) and ongoing technology refinement after mission proving the system allows Full Rate Production (FRP).

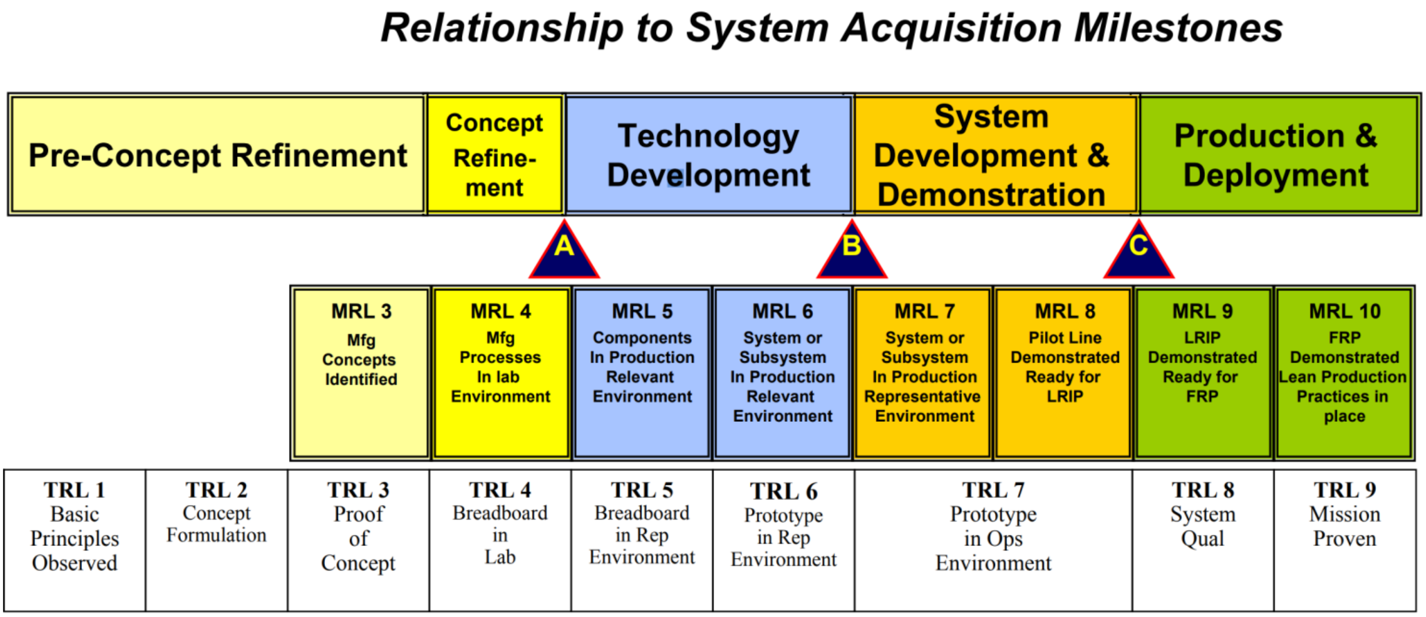

Relationship to System Acquisition Milestones
Pre-Concept Refinement
Concept Refine-ment
Technology Development
System Development & Demonstration
Production & Deployment
A
B
C
MRL 3 Mfg Concepts Identified
MRL 4 Mfg Processes In lab Environment
MRL 5 Components In Production Relevant Environment
MRL 6 System or Subsystem In Production Relevant Environment
MRL 7 System or Subsystem In Production Representative Environment
MRL 8 Pilot Line Demonstrated Ready for LRIP
MRL 9 LRIP Demonstrated Ready for FRP
MRL 10 FRP Demonstrated Lean Production Practices in place
TRL 1 Basic Principles Observed
TRL 2 Concept Formulation
TRL 3 Proof of Concept
TRL 4 Breadboard in Lab
TRL 5 Breadboard in Rep Environment
TRL 6 Prototype in Rep Environment
TRL 7 Prototype in Ops Environment
TRL 8 System Qual
TRL 9 Mission Proven

Figure 2-96 – Relationship of TRL, MRL and Market RL / Acquisition Milestones (Source: Morgan 2008 /Released by Manufacturing Technology Division of the US Air Force)

A system approach will also help ensure that technology improvement benefits can be prospectively quantified to plan R&D allocation and meet the capability expectations of the users in time.

2.9.2 Obsolescence and Innovation Management

Obsolescence management is a more complex process compared to project-based research and innovation of specific products, due to the proliferation of stakeholders during the life cycle of the product, who manage the system – production (main and sub-contractors), procurement, financial, and maintenance agencies as well as the users. As commercially driven technologies used in soldier systems (software, electronics, hardware/mechanical, advanced materials, etc.) change at a rapid, different and unpredictable pace, keeping the soldier system state of the art becomes a compounded problem. Prediction of how long the system will remain state of the art, therefore, becomes difficult as does the planning of research and technology projects to develop new systems.

2.9.2.1 Product Life Cycle Activities and Predictive Notices

The aim of obsolescence management is to schedule actions which, while ensuring availability, minimising the impact of the loss of operational efficacy and cost. This calls for an efficient and pro-active obsolescence management strategy depicts the obsolescence management activities in relation to the product life cycle of an existing product (in blue) and an upgraded or a new product (in green).

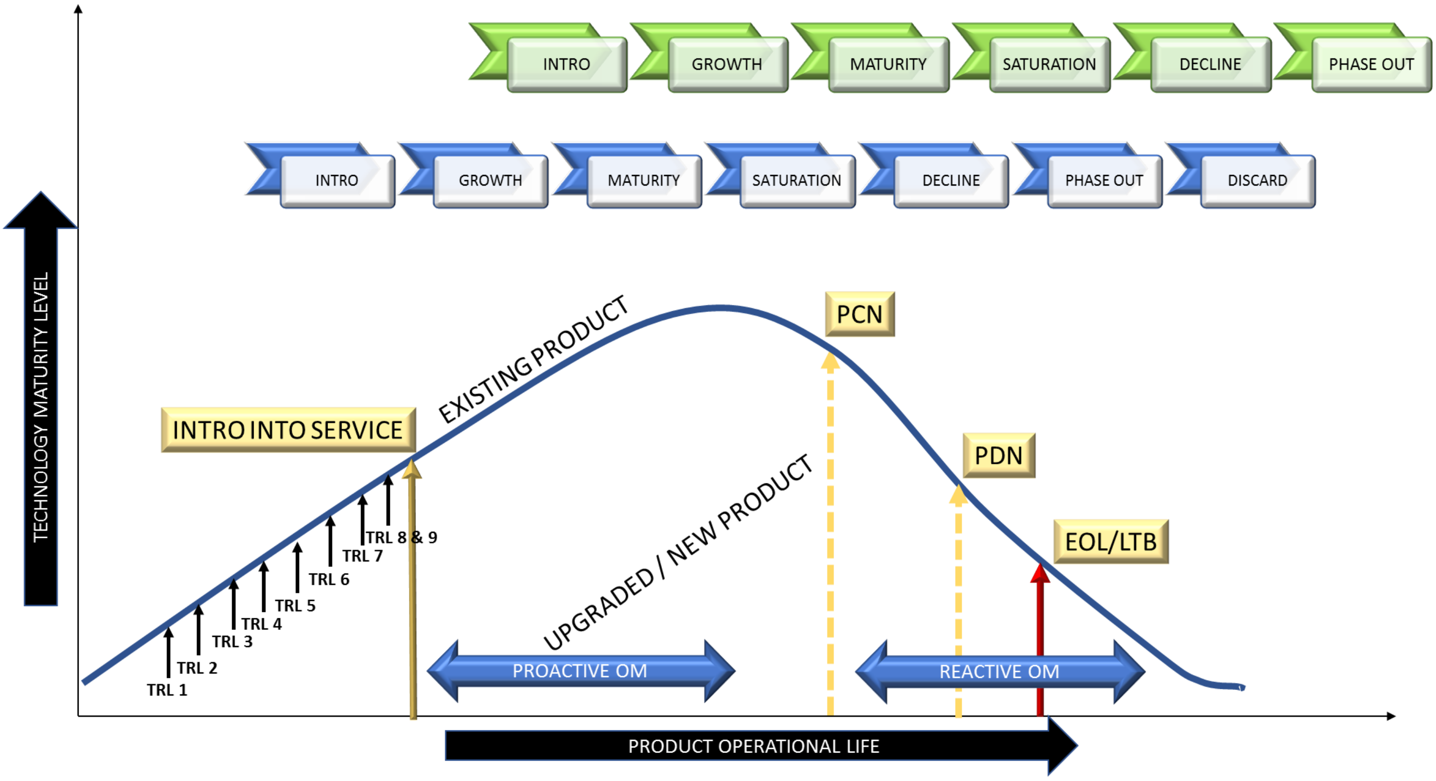


Figure 2-97 – Matching Product Life Cycle Phases and Technology Changes

Optimum utilisation of a product’s operational life can be enhanced by early adoption (introduction into service) of the current state of the art technology product, without prolonged development and procurement processes making it near obsolescent at delivery.

Similarly, A pro-active obsolescence management (OM) strategy and plan at the beginning of a product’s life enables timely insertion of new technologies through software updates/ component upgrades as well notices for scheduled activities like periodic maintenance; Product Change Notice (PCN) - upgrade/update notices; Product Discontinuance Notice (PDN); and; End of Life (EOL) / Life Time Buy (LTB) notices to the users, suppliers, and other relevant stakeholders.

2.9.2.2 Planning Updates and Upgrades

One way of addressing the issue of obsolescence management is to make component designs modular, which are amenable to easy replacements by upgraded components/sub-systems. The system can be kept state of the art for some time through such software updates and component upgrades. However, whenever a disruptive technology comes along, it sometimes becomes easier to build a new system from scratch. Maintaining the balance between producing updates/upgraded versions, say ever one to two years, and substantially investing in R&D for developing a new product every 8-10 years is key to obsolescence management. The different durations of the innovation cycles of software, sensors, electronics and mechanical components of sub-systems, of course, have to remain in synchrony through the use of interfaces and efficient project management.

2.9.2.3 Evolving a Continuous Process of Innovation

Given the fact that it is difficult to accurately predict or plan the commencement and end of new technology development cycles in relation to the obsolescence of the product life cycle of the soldier system, it may be a better idea to have in place a continuous process of innovation. Figure 2-98 depicts the drivers of such a continuous innovation process.

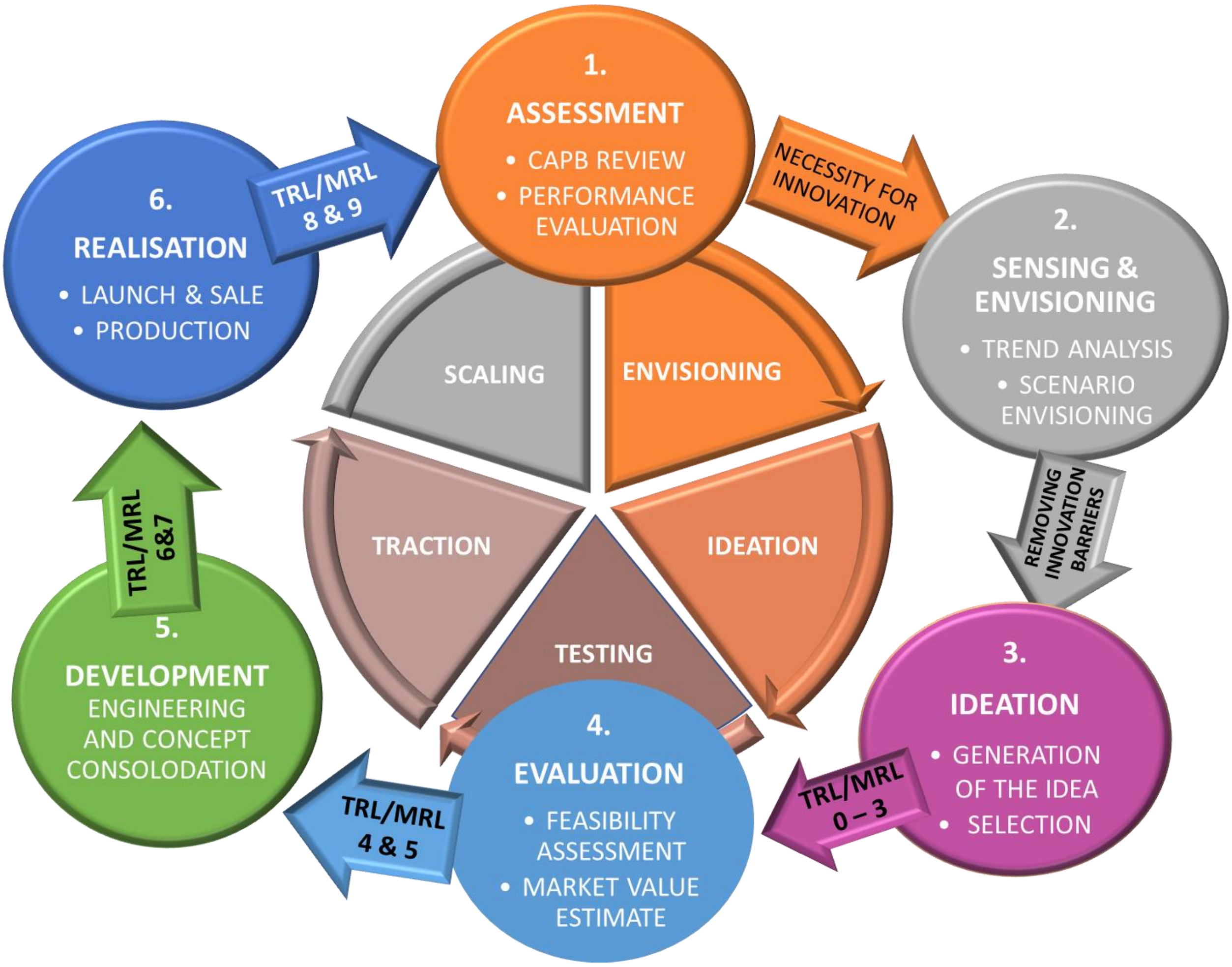


Figure 2-98 – Continuous Innovation Cycle Process

The critical aspect is synchronising the timing of completion of TRL and MRL (Manufacturing Readiness Level) stages for all individual components with that of the main system – ensuring economical, staged and continuous innovation.

2.9.2.4 Product System Engineering Special Activities

Every production agency should, apart from the activities listed above, carry out the following product system engineering activities to ensure timely and quality production:

- **Readiness Level Assessments**. Carry out a coordinated assessment in terms of TRL, MRL, IRL, SRL of all components and sub-systems including the assessment of COTS items.

- **Product Certification**. Ensure compliance management (in relation to human, health, safety and government regulations) and product certification, preferably by a third-party.

- **Technology Planning and Insertion.** Programme system engineers should align activities with technology developers to ensure that technology insertion happens as per the enterprise programme.

- **Product Road Mapping and Release.** Ensure that the internal product road map and the external release plan/road map are in synchrony.

- **IPR Management.** Proprietary information, patents, trademarks and copyrights of collaborators / sub-contractors should be respected.

3 Integrated Dictionary

3.1 Abbreviations and Acronyms

AEP	Allied Engineering Publication
ANR	Active Noise Reduction
API	Application Programming Interface
ASL	Application Service Logic
AI	Artificial Intelligence
AR	Augmented Reality
BMS	Battery Management System
BLOS	Beyond Line Of Sight
BFT	Blue Force Tracking
BC	Bulk Charger
CASEVACREQ	Casualty Evacuation Request
CRB	Central Rechargeable Battery
CBRN	Chemical, Biological, Radiological, and Nuclear
CD	Coalition Domain
CXP	Collection and Exploitation Plan
CRL	Collection Requirements List
CTL	Collection Task List
CEDS FSP	Combat Equipment for Dismounted Soldier - Feasibility Study Programme
CID	Combat Identification
COTS	Commercial off-the-shelf
CDC	Communication Device Class
CR	Compulsory Requirement
DDS	Data Distribution Services
DEP	Date Exchange Protocols
DNV GL	Det Norske Veritas Germanischer Lloyd (NLD)
DEU	Deutschland (Germany)
DEW	Directed Energy Weapon
DSS	Dismounted Soldier System
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
EO	Earth Observation
ET	Ejercito de Tierra
EMC	Electromagnetic Compatibility
ECM	Electronic Counter Measures
EOL	End of Life
EUD	End User Device
EDR	Enhanced Data Rate (see Bluetooth)
EC	European Comission
EDA	European Defence Agency
ESSOR	European Secure SDR

EU	European Union
XML	Extensible Marcup Language
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
FRP	Full Rate Production
FET	Future Emerging Technologies
GVA	General Vehicle Architecture
GMTL	Generic Military Tasks List
GOSSRA	Generic Open Soldier System Reference Architecture
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GDM	GOSSRA Data Model
GUI	Graphic User Interface
GND	Ground
GMTI	Ground Moving Target Indicator
GTA	Ground-To-Air
GTG	Ground-To-Ground
HDD	Head Down Display
HMD	Head Mounted Display
HUD	Head Up Display
HSP	HeadSet Profile
HDR	High Data Rate
HF	High Frecuency
HPC	High Power Consumers
HID	Human Interface Device
HRI	Human RAS Integration
HMI	Human-Machine Interface
ID	Identification
IED	Improvised Explosive Device
IR	Infrared
IRL	Innovation Readiness Level
IEEE	Institute of Electrical and Electronic Engineers
IPR	Intellectual Property Rights
ICP	Intelligence Collection Plan
ISR	Intelligence Surveillance and Reconaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconaissance
IDL	Interface Definition Language
IP	Internet Protocol
ITA	Italy
JDSS	Joint Dismounted Soldier System
JDSSDM	Joint Dismounted Soldier System Data Model
JDSSIEM	Joint Dismounted Soldier System Information Exchange Mechanism
JD	Joint Domain
JNN	Joint Network Node
JPEG	Joint Photographic Experts Group
KET	Key Enabling Technologies

LCG-DSS	Land Capability Group – Dismounted Soldier Systems
LDM	Land Data Model
LRF	Laser Range Finder
LTB	Life Time Buy
LOS	Line Of Sight
LRU	Line replaceable unit
LEP	Link Exchange Protocols
LAN	Local Area Network
LLCP	Logical Link Control Protocol
LPC	Low Power Consumers
LRIP	Low-Rate Initial Production
MGT	Management
MRL	Manufacturing Readiness Level
MPC	Medium Power Consumers
MQTT	Message Queue Telemetry Transport
MEMS	MicroElectroMechanical Systems
MIL	Militar
MOTS	Military off-the-shelf
MDE	Ministerio de Defensa de España
MC	Mission Control
MANET	Mobile Ad hoc Network
MOLLE	Modular Lightweight Load-carrying Equipment
MUMSIS	Multi-Modal Soldier Interface System
NBWF	Narrowband Waveform
NASA	National Aeronautics and Space Administration
NAR	NATO Accessory Rail
NAV	NATO All View
NCV	NATO Capability View
NGVA	NATO Generic Vehicle Architecture (STANAG 4754)
NOV	NATO Operational View
NSOV	NATO Service Oriented View
NSV	NATO System View
NTV	NATO Technical View
NFC	Near Field Communication
NLD	Netherlands
NCO	Network Centric Operations
NEC	Network Enabled Capability
NDEF	NFC Data Exchange Format
NVG	Night Vision Goggles
NGV	Night Vision Goggles
NATO	North Atlantic Treaty Organization
NBC	Nuclear Biological Chemical
OM	Obsolescence Management
OTG	On The Go
OE	Operational Enhancement
OS	Operative System

OECD	Organisation for Economic Co-operation and Development
PC	Payload Control
PAN	Personal Area Network
PIM	Platform Independent Model
PSM	Platform Specific Model
POL	Poland
PRT	Portugal
PDD	Power and Data Distribution
PCU	Power Control Unit
PADR	Preparatory Action on Defence Research
PCN	Product Change Notice
PDN	Product Discontinuance Notice
PU	Public
PRS	Public Regulated Service
PTT	Push-to-talk
RD	Radio Device
RFCOMM	Radio Frecuency Communication
RL	Readiness Level
RTP	Real-Time Transport Protocol
RSTA	Reconnaissance, Surveillance, and Target Acquisition
RNDIS	Remote Network Driver Interface Specification
ROVER	Remotely Operated Video Enhanced Receiver
RFI	Request For Information
RE	Required if operational enhancement is available
REQ	Requirement
RAS	Robotic & Autonomous System
SAR	Search and Rescue
COMSEC	Secure Communications
SN	Sensor Network
SA	Situational Awareness
STU	Small Tactical Unit
SW	Software
SDR	Software Defined Radio
SPD	Soldier Personal Domain
SDCI	Soldier Power Distribution, Control and Information
SPS	Soldier Power System
ESP	Spain
SOF	Special Operations Forces
STANAG	Standardisation Agreement (NATO)
STASS	Standardized Architecture for Soldier System
STUD	STU Domain
SWE	Sweden
SMBus	System Management Bus
SRL	System Readiness Level
TRA	Technology Readiness Assessment
TRL	Technology Readiness Levels

UCS	UA Control System
UHF	Ultra-High Frequency
UGS	Unattended Ground Sensors
UML	Unified Modelling Language
US	United States
USA	United States of America
USB	Universal Serial Bus
UAS	Unmaned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UA	Unmanned Aircraft
UGV	Unmanned Ground Vehicle
VHF	Very High Frequency
VDP	Video Distribution Profile
VR	Virtual Reality
VDC	Volts Direct Current
WF	Wave Form
WPC	Wearable Portable Computer
WPC	Wireless Power Consortium
WP	Work Package
WG	Working Group
XSD	XML Schema Documentation

3.2 Referenced Documents

3.2.1 GOSSRA Documents' references

/1/ GOSSRA Architecture for Standardisation – Volume 1 – All View (NAV) and Summary, PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/2/ GOSSRA Architecture for Standardisation – Volume 2 – Capability View (NCV), PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/3/ GOSSRA Architecture for Standardisation – Volume 3 – Operational View (NOV), PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/4/ GOSSRA Architecture for Standardisation – Volume 4 – Service Oriented View (NSOV), PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/5/ GOSSRA Architecture for Standardisation – Volume 5 – System View (NSV), PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/6/ GOSSRA Architecture for Standardisation – Volume 6 –Technical View (NTV), PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A033 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/7/ GOSSRA Architecture for Standardisation – Volume 7 – Security View, PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.5), V1.0, 30-04-2020

/8/ GOSSRA Architecture Formal File for Standardisation, PADR-FPSS-01-2017: GA 800783 GOSSRA (Generic Open Soldier System Reference Architecture), BL8464A037 REP, (GOSSRA Deliverable D8.4), V1.0, 30-04-2020

3.2.2 Document related references

/9/ STASS II Design Document v3.1, GMV 21407/17 V3/17, 01-02-2018

/10/ STASS Design Document v3.02, BL 8387 T244 REP, 30-10-2016

/11/ NATO Information Exchange Mechanism for Dismounted Soldier Systems, Dr. Norbert Härle (Rheinmetall Electronics), Issue 1.1, 05-11-2008

/12/ MUMSIS (Multimodal Soldier Interface System) Executive Summary, Issue 1.1, 02-03-2016

/13/ NATO AEP-76, VOL. 1 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security (STANAG 4677) Edition A

/14/ NATO AEP-76, VOL.2 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) Data Model (STANAG 4677) Edition A

/15/ NATO AEP-76, VOL.3 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Loaned Radio (STANAG 4677) Edition A

/16/ NATO AEP-76, VOL.4 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism (STANAG 4677) Edition A

/17/ NATO AEP-76, VOL.5 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access (STANAG 4677) Edition A

/18/ NATO STANAG AEP-4695, Electrical Connectivity Standards Between NATO Power Sources And Dismounted Soldier Systems (DSS), Edition A, Version 1, Jun 2016

/19/ NATO STANAG 4677, Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability Standardisation Agreement (DSS C4 Interoperability STANAG), Edition 1, November 2012.

/20/ Object Management Group (2015), “Real-Time Data Distribution Services”, Issue 1.4, 04/ 2015

/21/ OMG, “The Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification – version 2.2” , 11/2014

/22/ Extensible and Dynamic Topic Types for DDS Specification, Version .1.2, September 2017

/23/ Interface Definition Language, Version 4.2, March 2018

/24/ Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson,"RTP: a transport protocol for real-time applications", RFC 1889, January 1996.

/25/ MIL-STD-6017 – Variable Message Format

/26/ MIL-STD-2045/47001 - Connectionless Data Transfer Application Layer Standard, Rev. D_Change1, 23 JUN 2008.

/27/ J.Postel, J. Reynolds, “File Transfer Protocol”, RFC 959,October 1985

/28/ P. Ford-Hutchinson, “Securing FTP with TLS”, RFC 4217, October 2005

/29/ IBM, A. Stanford-Clark , H.L. Truong, “MQTT for Sensor Network”, V 1.2 , November 2013

/30/ Audio Codec ‘97 Specification (Intel), Revision 2.3, 2002

/31/ High Definition Audio Specification (Intel), Revision 1.0a, 2010

/32/ USB Device Class Definition for Basic Audio Functions, release 3.0, 2016

/33/ Nett Warrior Interconnect Architecture White Paper (NWPAN-WP-01112013), Version 6, 2017

/34/ STANAG 4609 / AEDP-8 - NATO Digital Motion Imagery Standard Edition 4

/35/ STANAG 4559 – NATO Standard ISR Library Interfaces and Services Edition 4

/36/ STANAG 4586 - STANDARD INTERFACES OF UA CONTROL SYSTEM (UCS) FOR NATO UA INTEROPERABILITY

/37/ STANAG 4695 - SOLDIER POWER CONNECTOR - ELECTRICAL CONNECTIVITY STANDARDS BETWEEN NATO POWER SOURCES AND DISMOUNTED SOLDIER SYSTEMS (DSS)

/38/ STANREC 4851 - SOLDIER DATA AND POWER CONNECTOR - ELECTRICAL AND DATA CONNECTIVITY STANDARDS BETWEEN NATO SOLDIER ANCILLARY DEVICES AND DISMOUNTED SOLDIER SYSTEMS (DSS)