

GOSSRA

Generic Open Soldier System Reference Architecture



Collaborative Project

PADR_FPSS_A_2017_800783

GOSSRA Architecture for Standardisation - Vol. 1

All View (NAV)

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.

This document is disclosed outside the GOSSRA Consortium and specifically targeted to the dismounted soldier system community. It shall not be used – in whole or in part – for any purpose other than for architectural work (e.g. reference architecture standardisation, derivation of target architectures, or extracting recommendation for soldier system definition, specification, design, and development), unless otherwise expressly authorised by the GOSSRA Consortium.

This project as well as any other results and rights obtained in performing the GOSSRA Grant Agreement, including copyright and other intellectual or industrial property rights, shall be owned solely by the GOSSRA Consortium, which may use, publish, assign or transfer them as it sees fit, without geographical or other limitation, except where industrial or intellectual property rights exist prior to the contract being entered into.



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 2.1.1

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 Figure 1-1 Final Release |

Table of Contents

| | | |
|----------|---|-----------|
| 1 | EXECUTIVESUMMARY | 5 |
| 2 | ALL VIEW | 10 |
| 2.1 | NAV-1 OVERVIEW AND SUMMARY INFORMATION..... | 10 |
| 2.1.1 | <i>Identification.....</i> | 12 |
| 2.1.2 | <i>Scope.....</i> | 14 |
| 2.1.2.1 | Architectural Scope..... | 14 |
| 2.1.2.2 | Architectural Framework..... | 14 |
| 2.1.2.3 | Views and Sub- Views | 14 |
| 2.1.2.4 | Reference Architecture and Target Architectures..... | 15 |
| 2.1.3 | <i>Contextual Background.....</i> | 17 |
| 2.1.3.1 | Technical Challenges in the Soldier Systems Domain..... | 17 |
| 2.1.3.2 | Challenges in Development, Procurement and Interoperability..... | 17 |
| 2.1.3.3 | Generic architectures and their Benefits | 17 |
| 2.1.3.4 | Potential Impact for Federated Mission Networking (FMN) and the TES (Tactical Edge Syndicate) Initiatives..... | 18 |
| 2.1.4 | <i>Aim and Purpose.....</i> | 19 |
| 2.1.4.1 | Aim | 19 |
| 2.1.4.2 | Purpose..... | 19 |
| 2.1.4.3 | Decision Support Needs for Soldier System Procurement | 20 |
| 2.1.5 | <i>Tools and File Formats.....</i> | 20 |
| 2.2 | FINDINGS | 21 |
| 2.2.1 | <i>Capability View (NCV, Vol. 2).....</i> | 22 |
| 2.2.2 | <i>Operational View (NOV, Vol. 3).....</i> | 24 |
| 2.2.3 | <i>Service Oriented View (NSOV, Vol. 4).....</i> | 27 |
| 2.2.4 | <i>System View (NSV, Vol. 5).....</i> | 29 |
| 2.2.5 | <i>Technical View (NTV, Vol. 6).....</i> | 33 |
| 2.2.6 | <i>Security View (Vol. 7).....</i> | 34 |
| 2.3 | NAV-2 INTEGRATED DICTIONARY | 35 |
| 2.3.1 | <i>Abbreviations and Acronyms.....</i> | 35 |
| 2.3.2 | <i>Referenced Documents.....</i> | 37 |
| 2.3.2.1 | GOSSRA Documents' references..... | 37 |
| 2.3.2.2 | Document related references..... | 37 |

Table of Figures

| | |
|--|----|
| Figure 1-1 – Reference Architecture interfaces in a common DSS | 8 |
| Figure 2-1 – GOSSRA Document Structure..... | 10 |
| Figure 2-2 – Way from Overarching to Target Architecture..... | 15 |
| Figure 2-3 – GOSSRA Views and Domains | 16 |
| Figure 2-4 – Categories for the Capability Vision | 23 |
| Figure 2-5 – High Level Operational Concept Description..... | 24 |
| Figure 2-6 – Organisational Relationship Chart..... | 26 |
| Figure 2-7 – DSS Services..... | 28 |
| Figure 2-8 – Example of Equipment needed for all Different Roles | 29 |
| Figure 2-9 – Personal Domain Standards | 32 |
| Figure 2-10 – STU, Coalition and Joint Domain Standards | 32 |
| Figure 2-11 – Risk Management Framework..... | 34 |

1 Executive Summary

Project and Funding

Under the Preparatory Action on Defence Research (PADR), the grant for the Research Action call on the topic of ‘Force protection and advanced soldier systems beyond current programmes’, subtopic ‘Generic Open Soldier Systems Architecture (GOSSRA)’, was awarded in 2018. The project with a duration of 23 months received an EU grant of roughly €1.5 million. The GOSSRA consortium led by Rheinmetall Electronics (Germany) encompassed GMV (Spain), iTTi (Poland), Tekever-ASDS (Portugal), Larimart (Italy), Leonardo (Italy), SAAB (Sweden), Indra (Spain) and TNO (The Netherlands).

Open Reference Architecture for Dismounted Soldier Systems (DSS)

The aim of GOSSRA is the development of an openly available Reference Architecture for modern Soldier Systems to be proposed for standardisation. The architecture, not implying any protected intellectual property, is intended to be used on EU-/NATO-Level as “best practice” reference for deriving Target Architectures for specific Soldier Systems to be procured at country-level and shall

- make the complex soldier systems manageable and realizable,
- increase operational effectiveness by complete networking of all systems,
- reduce integration effort through standardisation,
- allow innovation by upgrading easily integrated sub-systems,
- enhance competition for sub-systems by making them interchangeable,
- reduce technical risks by using sub-systems and integration approaches with higher Technology Readiness Levels (TRL),
- reduce logistic and maintenance efforts by lowering the variety of different sub-system, and
- increase the number of suppliers and by using a common technical approach.

Thus, Soldier Systems to be procured are easier to develop, include all necessary aspects, and use specific common standards enabling interoperability.

Main parts of the architecture have been validated and demonstrated to the Soldier System community during the GOSSRA project.

Architectural Views

The Reference Architecture, formulated according to NAF v3.1, focuses on the domain of software, electronics, voice and data communication, sensors, effectors, human interface devices, and C4I. It consists of the views as follows.

All View (NAV)

The All View states administrative and meta-data about the architecture. It contains the aim and purpose, the names of the architecture developers, which views are chosen, and also a summary about the findings.

Capability View (NCV)

The Capability View describes the capability of Dismounted Soldiers and Small Tactical Units (STUs) which also considers related mobile platforms.

The **Capability Vision (NCV-1)** describes the following Capability Goals:

- **Command, Control, Communication, Computing (C4).** A DSS shall provide support to address the core questions for an infantry soldier (“What is my task?”, “Where am I?”, “Where are my comrades?”, “Where is the enemy?”, “What is my environment?”)

- **Intelligence, Surveillance, Target Acquisition, Reconnaissance (ISTAR).** A DSS shall provide ISTAR capabilities mainly to improve the situational awareness, target acquisition and designation, and decision making of a soldier.
- **Effective Engagement.** A DSS shall improve the coordination and support for a soldier to engage a target during day, night and all-weather conditions.
- **Mobility.** A DSS shall enable a soldier to move either mounted or dismounted in an unhindered manner in all types of terrain and environmental conditions, and in special configuration cases, augment mobility in difficult and 'no-go' terrain.
- **Protection and Survivability.** A DSS shall help the soldier to endure the physical and psychological stresses of a battle space or operational area, through adaptive camouflage, concealment from sensors, and protection against hostile fire, splinters, stabbing weapons and the din of battle.
- **Sustainability and Logistics.** A DSS shall enable the soldier to configure its equipment in accordance to the needs of the mission; in advance and during mission. Sustainability reflects that the soldier is able to operate the DSS for a longer period of time.
- **Education and Training.** A DSS shall enable a soldier to train the system by the use of operational equipment. The DSS shall support training with minimum effort in time and cost.
- **Multi-National Interoperability (including CIMIC).** This Capability Goal focusses on addressing the specific gaps in interoperability in terms of Tactical, Technical and Logistic Interoperability with the aim to achieve comprehensive interoperability in a multi-national environment

A **Capability Taxonomy (NCV-2)** is defined based for the Capability Goals previously introduced, which defines the vocabulary for the capabilities used throughout the architecture.

Dependencies between capabilities are illustrated in **Capability Dependencies (NCV-4)**.

Finally, in **Capabilities to Activity Mapping (NCV-6)**, the Capability Goals are related to the Operational Activities of the Operational View (NOV).

Operational View (NOV)

The **High-Level Operational Concept Description (NOV-1)** is defined considering the typical scenarios and situations where a soldier equipped with a DSS operates in various military branches other than regular infantry, namely, Armoured Corps, Corps of Engineers, Mountain Infantry, Marines, Paratroopers, Special Operation Forces, etc.

The underlying concepts of military operations are also defined and a new concept of *swarming* is described in more detail. Also, agile command and control concepts are presented and compared with legacy C2 concepts.

An **Operational Node Connectivity Description (NOV-2)** and the **Operational Information Requirements (NOV-3)** illustrate which information is needed and which information needs to be exchanged categorized into Soldier Personal Domain, Small Tactical Unit (STU), Intra-Platform Domain, Joint Domain, and Coalition Domain.

The **Organisational Relationship Chart (NOV-4)** identifies the key players in the operational domain and illustrates the organizational relationships amongst them.

The **Operational Activity Model (NOV-5)** defines operational activities for different roles and mission control during Battle/engagement, Peace missions, Humanitarian operations, CIMIC/OOTW (Civil Military Cooperation / Operations Other Than War), and Generic tasks for a Dismounted Soldier during any mission.

Specifically noted is the **NOV-6 Operational Activity Sequence & Timing Description** which consists of three specific typical scenarios (for Mechanised Infantry, Regular Infantry and Special Forces) and a typical schedule of activities and usage of soldier system components.

Finally, a comprehensive set of **Non-Functional Requirements** is defined.

Service Oriented View (NSOV)

A service is understood in its broadest sense, as a well-defined way to provide a unit of work, through which, a provider supplies a useful result to a consumer.

The **NSOV-1 Service Taxonomy** is categorized in three main domains:

- **Operational Services:** services to accomplish a mission,
- **Functional Services:** services provided by the DSS to support the soldier/STU, and
- **Enterprise Services:** services provided by the enterprise.

NSOV-2 Service Definitions describes the services defined in the taxonomy in more detail. This Sub-view, serves the purpose of delineating and defining services in order to understand the operational domain in terms of services supporting operational activities of a soldier or STU using the DSS.

Finally, **NSOV-3 Services to Operational Activities Mapping** maps the Operational Services to the activities defined in the Operational View (NOV).

System View (NSV)

The System View describes the systems and sub-systems that provide support to the required services or functions. In this Reference Architecture following different domains were identified and used:

- **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 which interacts with another platform, e.g. a Vehicle. This domain also includes the Mounted Soldier in a NGVA 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 which interacts with units belonging to an allied force.

Each domain considered the following parts and tailored them if not applicable:

- **Electronic Components**, which addresses the electrical components and power requirements
- **Data Exchange Services**, which addresses the data exchange in terms of middleware, data model and protocol
- **Soldier Applications**, which addresses the generic applications concepts for the soldier system
- **Communication Components**, which addresses the communication components such as radios and their underlying theory
- **Human Interface Devices**, which addresses the human input devices
- **C4I Applications**, which addresses the architecture aspects in respect to C4I applications
- **Sensors**, which addresses the integration and usage of data of sensors
- **Effectors**, which addresses the integration and usage of data of components on the effector including sensors

To provide a better overview, standards were represented in protocol stack diagrams.

In the System View, standards are recommended for the different architectural elements for each domain. Standardisation of interfaces (signals, connectors, etc.) is considered as the main driver

for modularity, interoperability, support of innovations, etc. and will provide huge benefits in all domains.

Figure 1-1 summarizes recommended interface standards in exemplary for the personal domain applied on a typical DSS configuration. Such figures are defined for each defined domain.

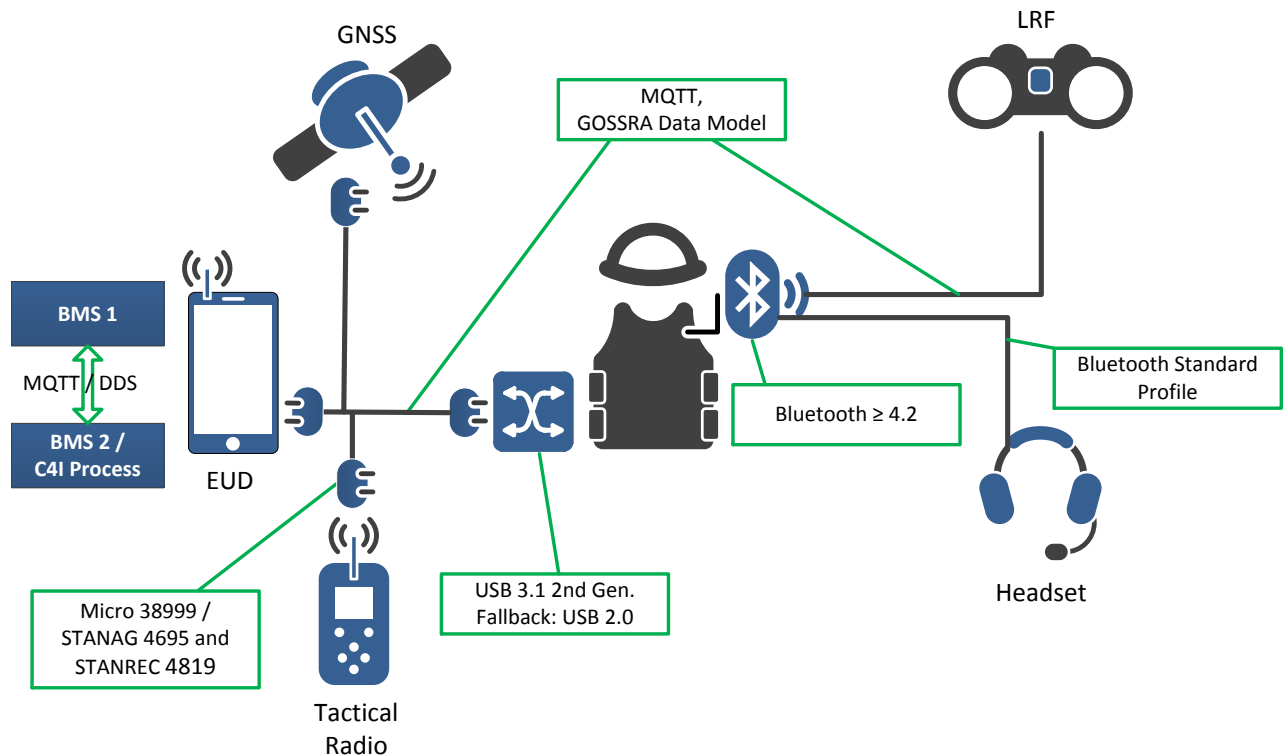


Figure 1-1 – Reference Architecture interfaces in a common DSS

Technical View (NTV)

The **NTV-1 Technical Standards Profiles View** states the standards, which are carefully selected and recommended for Soldier Systems. It also provides rationales for the selection of the standards and the considered alternatives.

Especially worth to mention is the use of:

- Micro 38999 and USB 3.1 2nd Generation which additionally offers an enhanced power management (USB 2.0 as fall back)
- Bluetooth with a Version newer than 4.2 for local wireless data connections
- STANAG 4677 or STANAG 5525 for tactical data exchange between soldier systems, especially in a multi-national environment.

NTV-2 Technical Standards Forecast discusses the development of the main recommended standards and predicts how they will evolve.

Security View

The Security View provides an approach for an IT Security Risk Assessment (SRA) for the DSS which is used to identify risks, caused by potential cyber threats. By knowing these risks, an organization can determine if, how, and when they intend to mitigate them to minimize the impact of a potential threat.

The recommended DSS SRA has been based on the MAGERIT methodology /12/, which uses the cyclic process model for risk management. A threat analysis is performed for each asset category, and initial risks are identified assuming a fundamental set of Safeguards in the categories:

- Access Control mechanisms [AC],
- Identification and Authentication mechanisms [IA],
- Audit mechanisms [AU], and
- Secure Communications [SC].

2 All View

2.1 NAV-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 2-1). It is accompanied by a formal architecture represented by a set of computer files, compiled by using the SparxSystems Enterprise Architect (version 13) /8/.

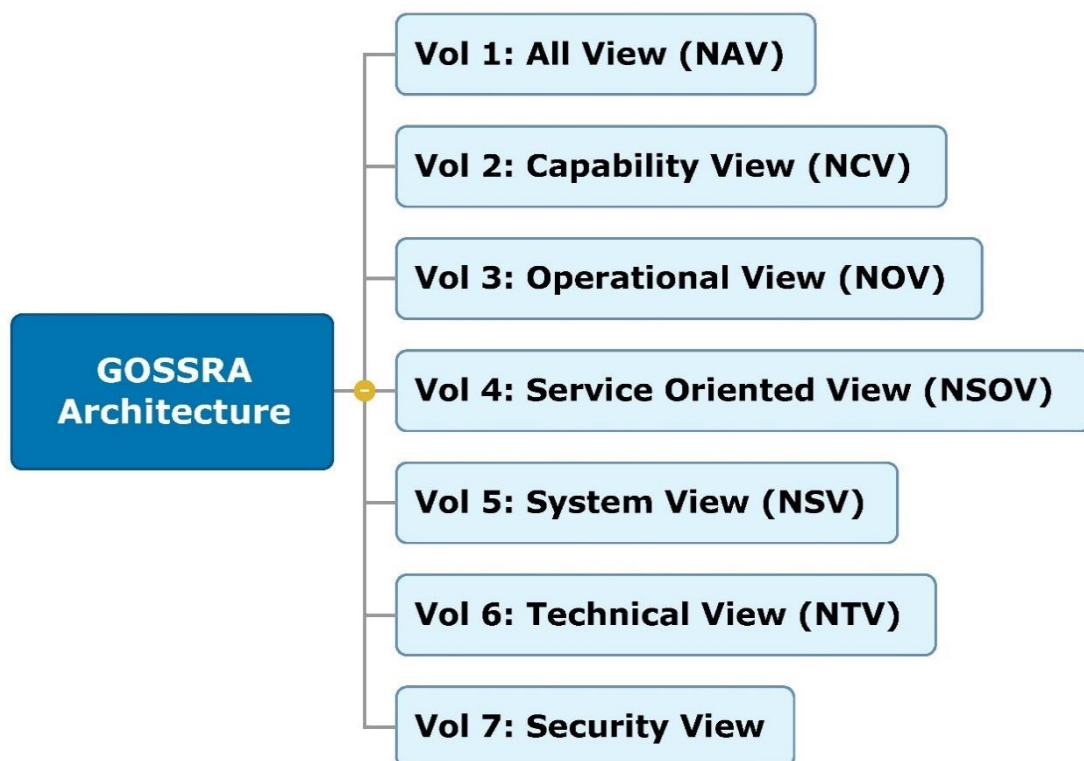


Figure 2-1 – GOSSRA Document Structure

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**.

2.1.1 Identification

This set of documents represents 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 I 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)
 - Ronald Ronald 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.

2.1.2 Scope

2.1.2.1 Architectural 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.

2.1.2.2 Architectural Framework

This Reference Architecture shall follow up on the work already carried out in other projects, studies, or working groups and complies with the NATO Architectural Framework (NAF) v3 which is required for inclusion in the EDA Architecture Repository and used by many European and NATO nations (NAF v3.1 /9/, /10/ and /11/).

2.1.2.3 Views and Sub-Views

The concept of the NATO Architectural Framework NAF v3.1 and its guidelines were used. The selected views from NAF v3.1 are

- **All View,**
- **Capability View,**
- **Operational View,**
- **Service Oriented View,**
- **System View, and**
- **Technical View.**

The NAF v3.1 Views are extended by the **Security View** which includes all security aspects for a soldier system and relates to several NAF v3.1 views.

2.1.2.4 Reference Architecture and Target Architectures

The scope of a Reference Architecture is to provide a consistent set of architectural best practices, high-level solutions, guidelines, recommendations and standards, forming an asset base to derive independent target projects from. Reference architectures are usually developed under a common Overarching Architecture.

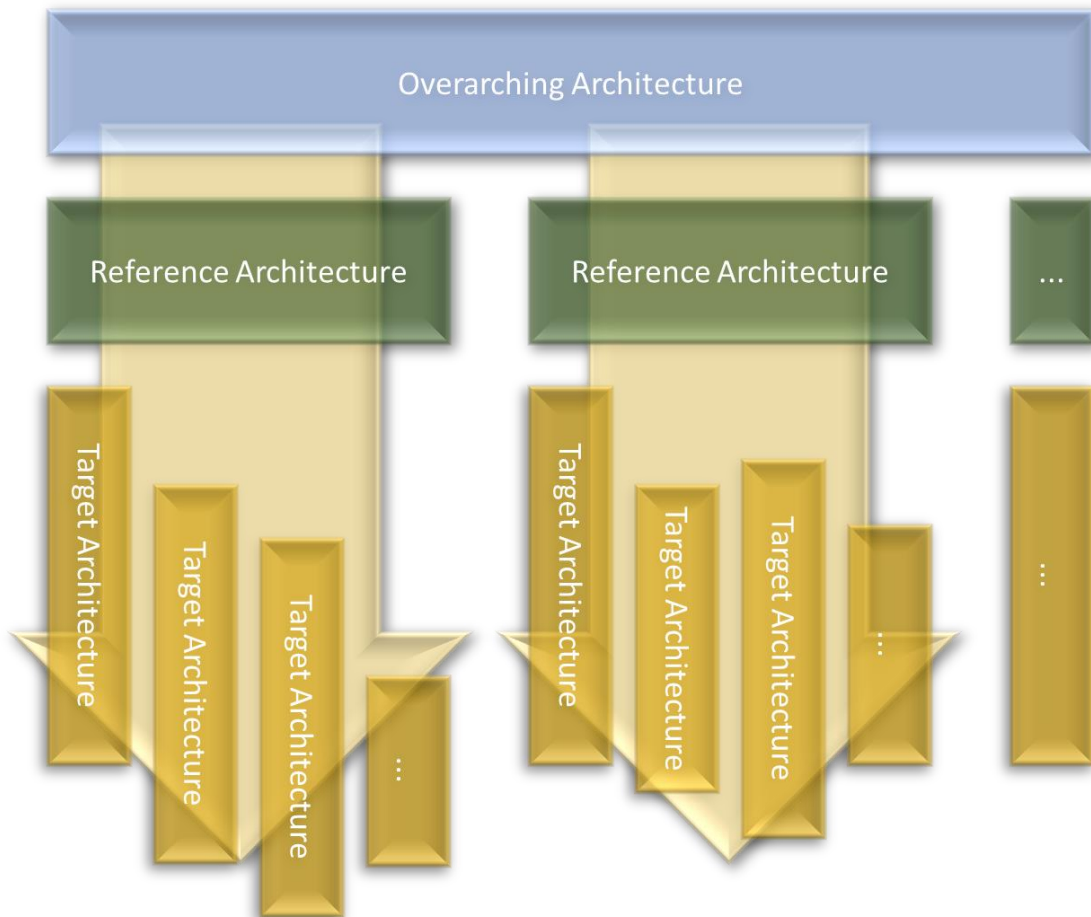


Figure 2-2 – Way from Overarching to Target Architecture

A reference architecture by definition, GOSSRA aims at providing a template to be conveniently used by the widest range of users, like the software and hardware engineers that develop the components of the system, the stakeholders that need to procure and maintain it, communication experts, and so forth.

To reach this ambitious goal, the GOSSRA template relies on a two-dimensional structure based on views and domains. The NATO architecture framework GOSSRA adheres to, standardises the views of the system that must be considered to represent it comprehensively. NAF views are then described according to five domains, encompassing not only the DSS *per se*, but also the interactions with peer- and higher-level systems.

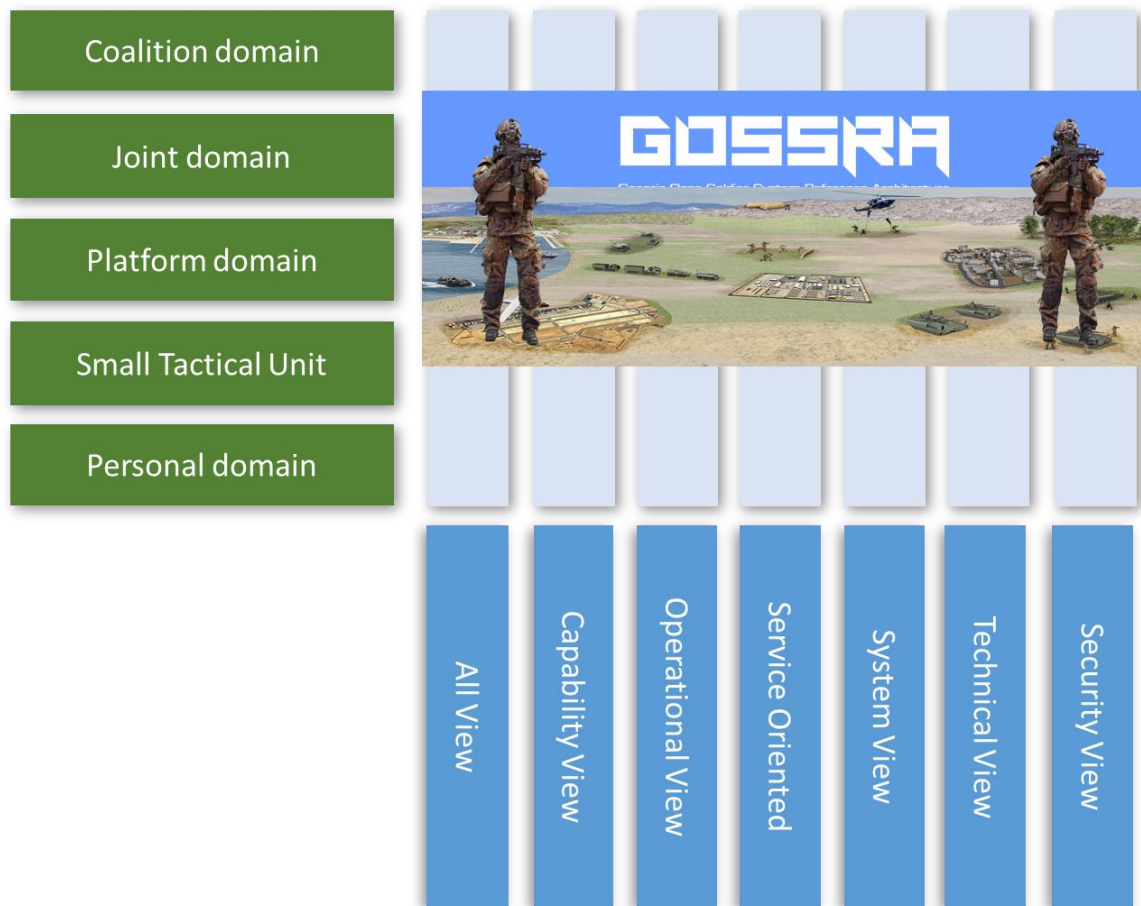


Figure 2-3 – GOSSRA Views and Domains

A target architecture derived from GOSSRA, i.e. an actual DSS project and its associated set of capabilities, services and infrastructures, is easier to develop, procure and maintain. Also, by complying to the same principles and standards, all derived target architectures are easily interoperable and can share several aspects, including project governance and management.

This methodology ensures that each target architecture can be developed independently, e.g. to fit nation's specific requirements and peculiarities, and at the same time it will still benefit from the power to be GOSSRA compliant.

Moreover, a derived target architecture is not forced to implement every single aspect covered in the template. But, whenever a relevant aspect needs to be developed, GOSSRA can provide a reasoned and reasonable approach to it.

2.1.3 Contextual Background

2.1.3.1 Technical Challenges in the Soldier Systems Domain

With the success of miniaturized, powerful electronics and computing capabilities in the civil domain and the need for networked systems and sub-systems with extensive information exchange in the military domain, Soldier Systems are getting more and more complex.

Moreover, Soldier Systems can be used more efficiently with all relevant data available. This data will not only be generated by the soldiers themselves or by the systems they carry, but will increasingly be originated from other sources (higher echelon units, vehicles, other soldiers, unattended sensors, etc.). Exchange of data between Soldier Systems and these sources via a common communication network is therefore paramount.

2.1.3.2 Challenges in Development, Procurement and Interoperability

Architectures for the Soldier Systems to be procured are individually developed in many European nations by the specific nation's Soldier System companies.

Today, most European / NATO nations have their own approaches to soldier modernization programmes. Many nations are still in the prototyping stage or working on concepts for the modern Soldier Systems. The results are nation specific systems which, with exceptions, are proprietary and totally lack interoperability for all electrical, electronic and IT aspects. However, operating in an EU-/ NATO-Coalition-Context or even with non-military partners, demands a high level of interoperability.

2.1.3.3 Generic architectures and their Benefits

Over the years, Open or Generic Architectures have started to be seen as a key to make such complex systems manageable and realizable. At the same time, such Reference Architectures enable affordability of this Soldier Systems by

- increasing operational effectiveness by complete networking of all systems,
- reducing integration effort through standardisation and interoperability,
- allowing innovation by upgrading sub-systems which can be easily integrated,
- enhancing competition for sub-systems by making them interchangeable,
- reducing technical risks by using sub-systems and integration approaches with high Technology Readiness Levels (TRL),
- reducing logistic and maintenance efforts by lowering the variety of different sub-system, and
- increasing the number of suppliers and by using a common technical approach.

2.1.3.4 Potential Impact for Federated Mission Networking (FMN) and the TES (Tactical Edge Syndicate) Initiatives

Federated Mission Networking (FMN) is a framework in NATO that provides an effective and efficient means to enable sharing of information in coalition environments. It is a capability aiming to support command and control and decision-making in future operations through improved information-sharing. It provides the agility, flexibility and scalability needed to manage the emerging requirements of any mission environment in future NATO operations.

Federated Mission Networking is based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities. Federated Mission Networking is built on lessons learned from the Afghanistan Mission Network (AMN) implementation and on the NATO Network Enabling Capability Programme /13/.

The main functional strategic objectives of FMN are to provide:

- seamless human-to-human communication across the force and
- a single view of the battle space across the Mission Network.

The scope of FMN has been targeted mainly on multinational networks in mission areas for the higher hierarchical (deployed, fixed) levels, such as multinational command posts. Recently, however, a new working group has been established within FMN to focus on the tactical levels.

This Tactical Edge Syndicate (TES) has been tasked by the FMN Capability Planning Working Group to develop specifications for operational information exchange related aspects of Federated Mission Networking, covering Command and Control (C2) levels from brigade command down to battalion, company, and platoon level at the tactical and mobile edge.

It is recommended for the TES working group to consider and analyse this Reference Architecture.

For the development of specifications for operational information exchange, the NCV (Capability View) and NOV (Operational View) are of interest for a generic description of the information needs for small tactical units. Furthermore, the NSOV (Service Oriented View) provides a set of services similar to the NATO C3 Taxonomy, but, aiming at lowest tactical levels.

With respect to proposed standards and protocols, TES should consider the recommendations in the NSV (System View) and NTV (Technical View), especially the two international interoperability standards (STANAG 4677 Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability) and VMF (Variable Message Format)) shall be considered for FMN. Most relevant for TES are the Coalition and Joint domain whereas the personal, STU and inter-platform domain may be less relevant to FMN.

2.1.4 Aim and Purpose

2.1.4.1 Aim

The overall aim is to have a reference architecture widely available and standardised that will be widely used for Soldier System definition, design and development in order to take a bigger step in advancing Soldier Systems and reduce effort and cost.

2.1.4.2 Purpose

The purpose of the Generic Open Soldier System Reference Architecture (GOSSRA) is to represent a comprehensive architecture for soldier systems which shall

- promote interoperability and interchangeability for national dismounted soldier programmes both at the system level and the component level,
- enable to equip the soldier for each mission with equipment that is readily interchangeable,
- consider the data distribution concept with reduced cabling effort,
- foster harmonized on-the-man concept of open power architecture for soldier systems,
- allow for a modular approach to support different soldier's equipment configurations,
- consist of operational, system and technical architectural views,
- be geared towards standardisation,
- be supported by a roadmap to establish a standard,
- require much lower integration efforts,
- increase component production numbers,
- reduce life cycle costs,
- guide component developers, and
- make best use of Commercial-Off-The-Shelf products (COTS).

2.1.4.3 Decision Support Needs for Soldier System Procurement

The purpose of the architecture is also to provide decision support for the procurement of soldier systems. The decision to procure a soldier system needs answers to the following questions:

- What capabilities must be supported?
- What operational issues are important?
- What services are expected from the system and their sub-systems?
- How to build the system?
- Which sub-systems need to be considered and how to interface them?
- What interfaces need to be provided by sub-systems?
- What components and devices need to be considered?
- What technologies are available today and what technologies are expected in the future?
- What standards are relevant?

2.1.5 Tools and File Formats

The architecture is compiled as a *Microsoft Word* document and is distributed as a *pdf* portable format file. Figures have been developed using *Microsoft Visio*, *Microsoft PowerPoint* and *SPARX Systems' Enterprise Architect*.

The document is accompanied by a set of files produced by the *SPARX Systems' Enterprise Architect* software tool which represent the Reference Architecture as a formal architecture.

2.2 Findings

This chapter provides a summary of the essential aspects of the architecture developed in the Capability, Operational, Service Oriented, Systems, Technical, and Security Views in Vol. 2 to Vol. 6 with following vision.

- Nations procure with reference to this Reference Architecture.
- Soldier System providers produce Soldier Systems which comply with this Reference Architecture.
- Soldier System suppliers produce devices which comply with this Reference Architecture.
- Soldier Systems become less expensive and more suited for the purpose they are procured.
- Each soldier will be equipped with a highly modern Soldier System that benefits from latest technological developments and is optimised for their specific role.
- The common architecture allows procurement agencies and users to choose for Soldier Systems, sub-systems or the devices the most suitable supplier, promoting open competition and pricing.

2.2.1 Capability View (NCV, Vol. 2)

The Capability View describes the capability of Dismounted Soldiers and Small Tactical Units (STUs) which may include related mobile platforms also considering combined and joint operations. The STU stands for a group of individual soldiers organised as military team, group, company, or any other organisation depending on the specific national needs and doctrines.

Soldiers are then categorised as:

- Individuals or Basic Soldiers (e.g. with a basic dismounted soldier system),
- Specialist Soldiers (e.g. with additional specialist equipment), and
- STU Leaders.

The **Capability Vision (NCV-1)** describes the following Capability Goals categorized under eight Capability Categories (see Figure 2-4):

- **Command, Control, Communication, Computing, Intelligence (C4I)**
A DSS shall provide support to address the core questions for an infantry soldier ("What is my task", "Where am I", "Where are my comrades", "Where is the enemy", "What is my environment") by
Multisensory Approach, Automated Functions, Enhanced Radio-Based Combat Identification (RBCI), Quick and Rich Information Sharing, Tactical versus Personal Choices, and Hemisphere Awareness.
- **Intelligence, Surveillance, Target Acquisition, Reconnaissance (ISTAR)**
A DSS shall provide ISTAR capabilities mainly to improve the situational awareness, target acquisition and designation, and decision making of a soldier by
Info-fusion, STU as a Sensor, Data Capture and Analysis, CROP (Common Relevant Operational Picture), Tactical Augmented Reality (TAR), EW Resilient Network, Info Security & Access Control, Non-human Intelligence Cooperation, and Smart Power Management & Systems.
- **Effective Engagement**
A DSS shall improve the coordination and support for a soldier to engage a target during day, night and all-weather conditions by
Shooting Around Corners, Auto-Fire Control, Body Worn Sensor Integration, TAR (Tactical Augmented Reality), Electronic Warfare (EW), and Small Arms-Sensor-Networking.
- **Mobility**
A DSS shall enable a soldier to move either mounted or dismounted in an unhindered manner in all types of terrain and environmental conditions, and in special configuration cases, augment mobility in difficult and 'no-go' terrain by
Reduction in Size, Weight and Power (SWaP) (reduce what needs to be transported, combine functions, exoskeletons, soldier borne cooling), Autonomous vehicles and its applications (cargo carrier, UGVs, new fuel/engine types), Digitization (modularity).
- **Protection and Survivability**
A DSS shall help the soldier to endure the physical and psychological stresses of a battle space or operational area, through adaptive camouflage, concealment from sensors, and protection against hostile fire, splinters, stabbing weapons and the din of battle by
Safeguarding against Non-Lethal High-Power Weapons, Electronic Warfare, CBRNE, Zero Emission (thermal, EM emissions, communications, visual), Clothing with Biometric Sensors, Temperature Management/Climate Control, and Integrated Protection.

- **Sustainability and Logistics**

A DSS shall enable the soldier to configure its equipment in accordance to the needs of the mission; in advance and during mission. Sustainability reflects that the soldier is able to operate the DSS for a longer period of time by

Integrated Logistics, Sustainable Power, Commonality & Interchangeability of Connectors, Potential Alternative Power Sources, Enhanced Modularity, automated in-situ Software Update and Device Upgrades, Production and Manufacturing Models, Additive Manufacturing, and Aerial Resupply.

- **Education and Training**

A DSS shall enable a soldier to train the system by the use of operational equipment by *Multifarious Approaches to Training (E-Learning, Virtual Reality (VR), Re-using gaming software, Re-use C4I system as training harness, Training facilities as a compound / during the mission, "Hardware in the loop", Artificial Intelligence (AI) support), Enable Multiple Training Domains (Individual Skill Development, "C4I" Training, Platform Training, Safety and Medical Training, User Level Maintenance, and Collective Training / Tactical Training, Joint / Combined Training.*

- **Multi-National Interoperability**

This Capability Goal focusses on addressing the specific gaps in interoperability in terms of Tactical, Technical and Logistic Interoperability.

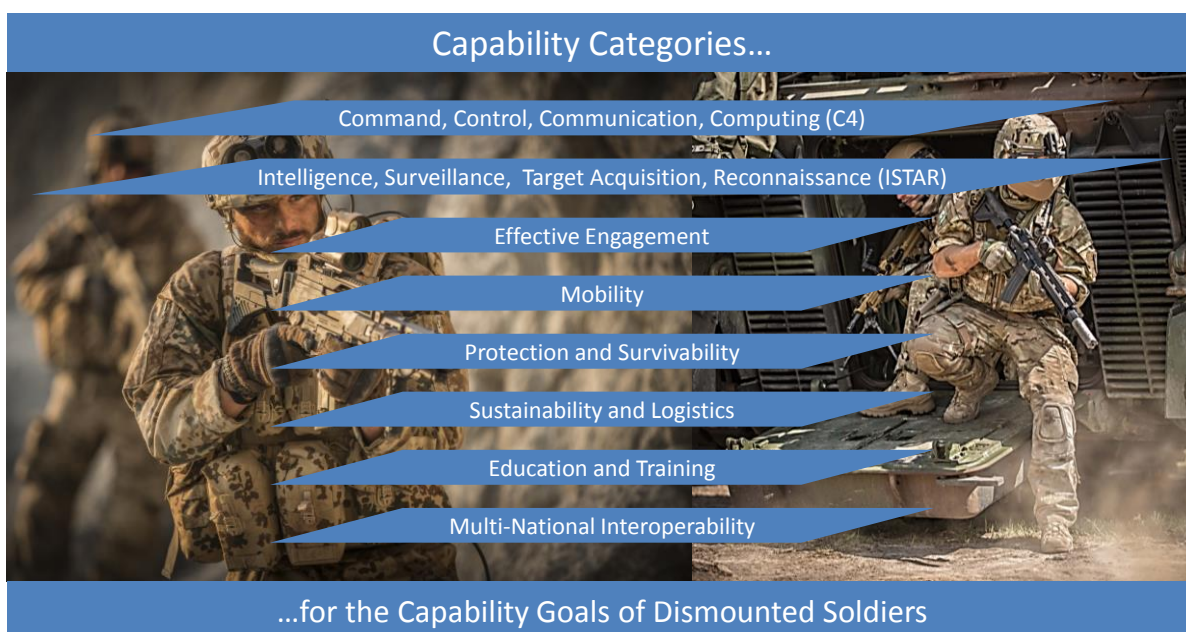


Figure 2-4 – Categories for the Capability Vision

The **Capability Taxonomy (NCV-2)** is based on the Capability Goals previously introduced and defines the vocabulary for the capabilities used throughout the architecture.

Dependencies between capabilities are illustrated in **NCV-4 Capability Dependencies**.

Finally, in **NCV-6 Capabilities to Activity Mapping**, the Capability Goals, which are broken down in sub-capabilities as stated in the taxonomy (NCV-2), are related to the Operational Activities. **NCV-6** indicates of how each capability, contributes to several operational activities.

2.2.2 Operational View (NOV, Vol. 3)

The **High-Level Operational Concept Description (NOV-1)**, see Figure 2-5, is defined considering the typical scenarios and situations where a soldier equipped with a DSS operates.



Figure 2-5 – High Level Operational Concept Description

In general, the broad spectrum of requirements for a Dismounted Soldiers system (DSS) covers operations in various military branches including also other than regular infantry, namely, Armoured Corps, Corps of Engineers, Mountain Infantry, Marines, Paratroopers, Special Operation Forces, etc.

The underlying concepts of military operations are defined in this view and a new concept of *swarming* is described in more detail. Further, the operational needs with emphasis on interoperability and methods for improving soldier system effectiveness are analysed.

Finally, agile command and control concepts are presented and compared with legacy C2 concepts.

The **Operational Node Connectivity Description (NOV-2)** illustrates the operational domain's needs for information exchange in support of operational activities. The Section is subdivided into:

- Soldier Node Internal Connectivity (**Soldier Personal Domain**),
- Small Tactical Unit (STU) Node Internal Connectivity (**Small Tactical Unit Domain**), and
- Small Tactical Unit (STU) Node External Connectivity (**Intra-Platform Domain, Joint Domain, Coalition Domain**).

Operational Requirements (NOV-3) identify the information needed in information spaces related to each domain in the above list.

One of the challenging objectives is to design a DSS capable of providing accurate and complete situational awareness in a very efficient manner, reducing to a minimum extent, the soldier's burden. Information overload is a known and important stress factor especially for soldiers in combat. Hence, the trade-off between increased weight/volume/power consumption of additional equipment and mobility needs to be carefully balanced.

The **Organisational Relationship Chart (NOV-4)**, see Figure 2-6, identifies the key players in the operational domain and illustrates the organizational relationships amongst them. This chart was developed by extracting and harmonizing from organisations of different European countries. The three **generic role-related configurations** mentioned in the Capability View are described in more detail

Other branches for joint operations, such as Armoured Corps, Artillery, Corps of Engineers, Army Air Corps, Signal Corps, Close Air Support, NBC Defence Corps, Military Units of Logistics, Military Police, Military Transportation Service, Geographic Information Service, Medical Service, NGO's, and Local / International Authorities, are identified and their relationship described.

Operational Activity Model (NOV-5) defines C4I activities, general tasks and specific tasks for different types of operations:

- battle/engagement,
- peace operations
 - peace keeping
 - peace enforcement
 - peace building, and
 - humanitarian operations.

Specifically noted is the **NOV-6 Operational Activity Sequence & Timing Description** with three specific scenarios

- High-Intensity Attack for Mechanised Infantry (24h)
- Military Evacuation Operation with Special Forces (72h), and
- Cordon and Search Operation with Regular Infantry (36h).

A typical schedule of activities for the participant soldiers and their usage of soldier system components for operations of varying durations (24, 36 and 72 hours) is defined.

Non-Functional Requirements have also been identified. These kinds of requirements, although not strictly operational and not required under the NAF v3 guidelines, are an important constraint to be considered when designing a DSS.

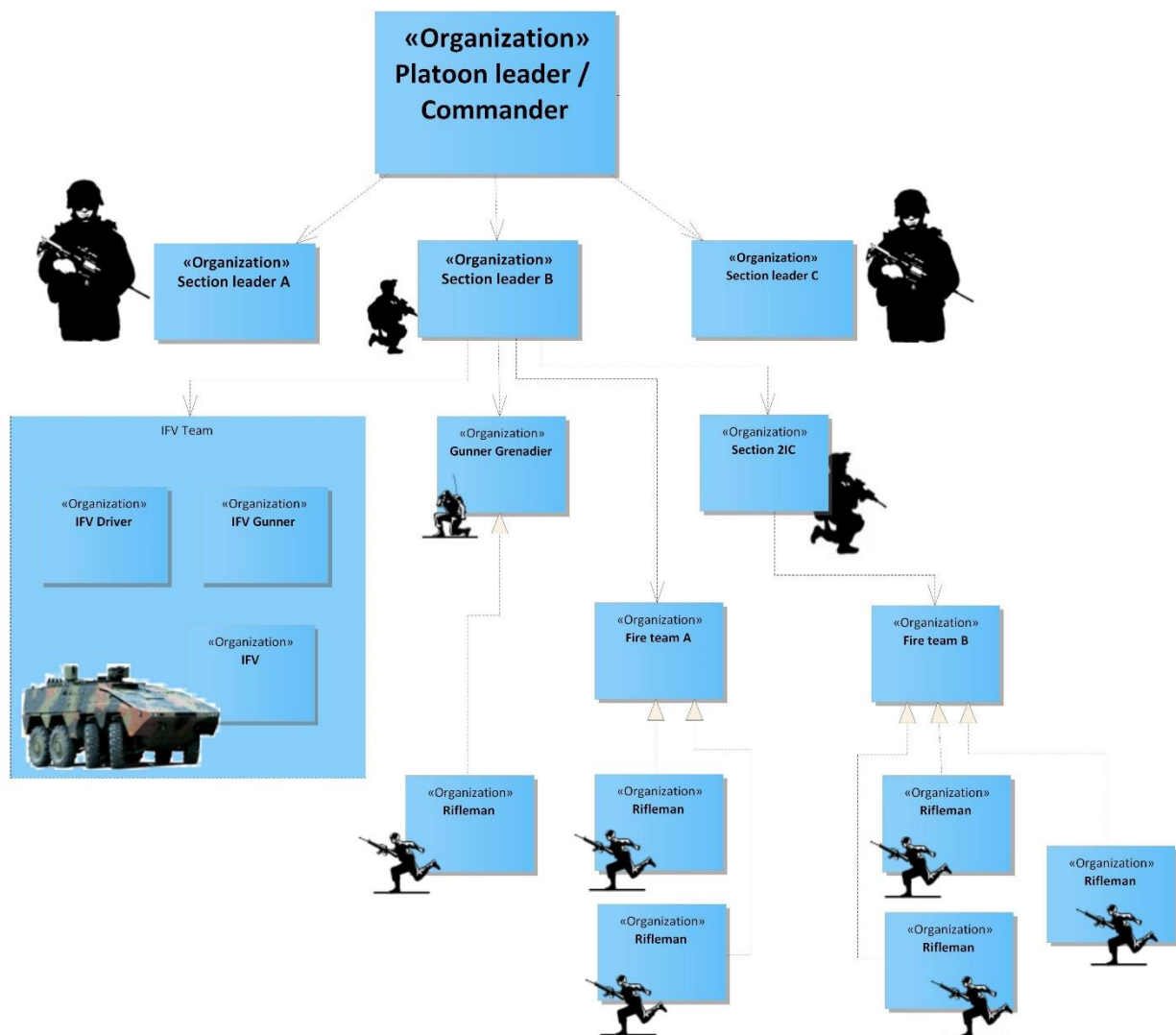


Figure 2-6 – Organisational Relationship Chart

2.2.3 Service Oriented View (NSOV, Vol. 4)

A service, within the NSOV, is understood in its broadest sense, as a well-defined way to provide a unit of work, through which, a provider supplies a useful result to a consumer, regardless of the services' construction or implementation.

The **Service Oriented View** services are identified and defined considering two main types of services:

- **Operational Services:** Services provided by the individual soldier or the STU to higher order echelons or other units
- **Functional Services:** Services provided by the Soldier System to the soldier / STU

The **Enterprise Services** are considered for the future and just mentioned briefly but not defined in detail.

NSOV-1 Service Taxonomy defined the services for these service types (see Figure 2-7).

The **Operational Services** are defined according to the already defined Capability Goals in the Capability View. From these Operational Services, the Functional Services are derived to be provided by the technical system, in order to support the soldier to perform the Operational Services.

The Soldier System is defined in the NSV System View such that it provides exactly these Functional Services.

NSOV-2 Service Definitions provides a detailed description of each service defined in the taxonomy. It is therefore useful to lookup the descriptions when reading the taxonomy.

Finally, **NSOV-3 Services to Operational Activities Mapping** maps the Operational Services to the activities defined in the NOV Operational View.



Figure 2-7 – DSS Services

2.2.4 System View (NSV, Vol. 5)

The NATO System View describes the systems and sub-systems that provide support to the required functions. It associates the system resources to the NCV Capability View, NOV Operational View and to the NSOV Service Oriented View. Following different domains were identified and used:

- **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 Squad or Team with Dismounted Soldier as nodes.
- **Inter-platform Domain** which addresses the needs of a Soldier as a node which interacts with another platform, e.g. a Vehicle. This domain also includes the Mounted Soldier in a NGVA 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 which interacts with units belonging to an allied force.

It was considered as utmost important not to purely focus on an individual soldier but rather on how he operated in his environment with all others and especially in a group which actually is the usual application of soldiers. The document for standardization was structured according to the domains above which enables the reader to directly find the domain of his interest.

First, the System View introduces the system domains and Soldier System Devices and Configurations (see Figure 2-8 as example).


| | 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 - Small 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 2-8 – Example of Equipment needed for all Different Roles

Then, the domains shown above are detailed. The main part contains layered reference architectures for each domain. The Reference Architecture layers starting from the top are:

- **Soldier Application**, which defines the key architectural concepts to design soldier applications,
 - which can easily evolve,
 - where each component is highly focused on specific capabilities and
 - whose components are loosely coupled to minimize the impact of a component changes on the others.
- **C4I Applications**, which defines the reference architecture for the C4I application family. Specifically, application architectures for the following C4I functional areas has been addressed:
 - Battlefield Management Services,
 - Situational Awareness,
 - System Management, and
 - Human RAS (Robot & Autonomous Systems) Interaction.
- **Data Exchange Services**, which define the set of protocols providing for data exchanges among application components covering all, tactical, control, and management data flows. Different protocol suites have been selected to fulfil the different data exchange needs of each domain. Data exchange services play a key role in application component loose coupling.
- **Voice & Data Communication**, which defines the set of protocol layers, which support Data Exchange Services, i.e. networking down to the radio channel, to transfer both data and voice. Specifically, the concept of “Waveforms” has been adopted as design solution which exploits SW Defined Radio capabilities to provide standard packaged protocol suites which improve communication agility and interoperability in Joint Multinational Operations.
- **Electronic Components**, which defines the physical architecture of the DSS, i.e. signal and power distribution among its components. The key issues of cabling and power management have also been addressed to improve interoperability among national equipment and reduce the SWaP.

Additionally, requirements are provided for an easy to read guidance through the mandatory and optional requirements of the architecture. They are especially important in order to guarantee the conform usage of the selected standards. To provide a better overview the standards were represented in protocol stack diagrams as shown in Figure 2-9 and Figure 2-10.

The System View specifically defines most important internal, external interfaces and concepts as mandatory e.g. to enable interoperability or interchangeability of devices (see Figure 2-9 and Figure 2-10). Within the personal domain, five main categories of interfaces are described as mandatory standard.

For the **system bus**, it was decided to use USB 3.1 2nd Generation for wired connections. As this is new to Solider Systems, USB 2.0 is defined as fall-back technology. For wireless connection, Bluetooth with a version greater 4.2 is chosen or NFC for very short range connections.

To connect devices in a generic way, **connectors and signals** are defined. It was not possible at the time, when this architecture was written, to find a standardized USB 3.1 2nd Generation connector, but different vendors announced possible solutions such as the recommended Micro 38999. Hence, the necessary signals for USB 3.1 2nd Generation are defined to allow interchangeable pinings of connectors. Concerning USB 2.0 connections, the STANAG 4695 is a good reference and is also considered in other parts in the military domain.

In order to exchange information between the devices of or entities inside a Soldier System (personal domain), MQTT is defined as **Information Exchange Mechanism (IEM)**. MQTT provides especially good usage of computing resource and bandwidth. As it is spread in the civil world (e.g. for Industry 4.0), interchangeable reference implementations are widely available with high TRLs which reduces risk for the DSS market (e.g. for companies providing peripherals).

Additionally for more complex tasks of information exchange in the personal domain, the Data Distribution Service (DDS) is chosen as an optional protocol. DDS provides efficient exchange and update of information, e.g. for the BMS domain with a high amount of devices or entities.

In order to ensure interoperable data exchange, it is also necessary to describe the **data structures** that hold the information, additional to the information exchange mechanism. These data structures are defined in a data model which uses XSD with XML for data exchange.

The recommended data model for the devices of a Soldier System is developed from the UK Land Data Model which was the basis for GVA (UK DefStan 23-09) and NGVA (NATO STANAG 4754). As the UK Land Data Model misses C4I Data, the C4I is taken from the data model (JDSSDM) of STANAG 4677 and, thus, serves the majority of requirements for the Soldier System domain.

For multimedia purposes, the most common standards such as H.264/H265, MP3, G.711, JPEG, PNG, and TIFF are recommended to be supported and used.

To improve the extendibility of a Soldier System an **APP-based HMI concept** is defined. This concept together with the layers in Figure 2-9 and Figure 2-10 enables porting different Applications between different soldier systems and also adapt to new devices or capabilities.

Concerning the external interfaces, namely the Small Tactical Unit, Joint and Coalition domain, following is recommended.

The **connectors and signals** from the personal domain enable exchange of equipment and batteries also between Soldier Systems of different nations.

The well spread NATO standards STANAG 4677 and STANAG 5525 are chosen for the **communication** between Soldier Systems, enabling interaction with coalition and joint forces. However, these standards are also recommended for the Small Tactical Unit domain which makes the Soldier System more future-proof and opens it up for alternative vendors. Hence, Soldier Systems of different vendors within one force becomes possible.

For **ISR Video streaming** and related tasks, STANAG 4609 and the related NATO standards are recommended.

| | | | |
|--|--|-------------|-----------------|
| Application | APP-Based HMI concept | | |
| Data Structures | GOSSRA Data Model (XML) | | |
| Information Exchange Mechanisms | MQTT (Mandatory) / DDS (Optional for BMS-Data) | | |
| Connectors/Signals | Micro 38999 | STANAG 4695 | N/A |
| Systembus | USB 3.1 2nd Gen. | USB 2.0 | Bluetooth ≥ 4.2 |
| Make full use of standard-profiles of the Systembusses | | | |

Figure 2-9 – Personal Domain Standards

| | | |
|--|----------------------------|-------------|
| Connectors/ Signals(e.g. Battery exchange) | Micro 38999 | STANAG 4695 |
| Communication | STANAG 4677 or STANAG 5525 | |

Figure 2-10 – STU, Coalition and Joint Domain Standards

2.2.5 Technical View (NTV, Vol. 6)

The **NTV-1 Technical Standards Profiles View** states the standards, which are carefully selected and recommended to be used for the electrical and electronic components of Soldier Systems.

A significant part of NTV-1 deals with standards for radio communication, either line of sight (LoS) or beyond line of sight (BLoS) which relates to VHF/UHF and HF/SATCOM. Further tables with standards are provided in the following categories:

- Physical Interfaces,
- Media Formats,
- Data Exchange Services,
- Transport Services,
- Audio Exchange,
- Remote Controls,
- Power Quality,
- Energy / Power Management,
- Product Conformity, and
- Laws and Regulations.

The tables are split into common standards (such as Product Conformity) and standards that are actually referred to in the System View.

NTV-2 Technical Standards Forecast discusses the development of the main recommended standards and predicts how they will evolve for a first evaluation about the feasibility of the future concepts.

2.2.6 Security View (Vol. 7)

The Security View provides a recommended approach for an IT Security Risk Assessment (SRA) for the DSS. Security Risk Assessment is used to identify risks, caused by potential cyber threats. By knowing these risks, an organization can determine if, how, and when they want to mitigate these to minimize the impact of a potential threat on their operations to accomplish their goals.

Security issues for DSS can be organized according to the soldier system communication scenario for the data exchange. This type of schematization can help make DSS SRA elaboration and determine the Safeguards. The DSS SRA has been based on the MAGERIT methodology [12], which uses the cyclic process model, shown in Figure 2-11, for risk management. This framework is useful for all kinds of risks, but is applied here to the risks arising from the use of information systems.

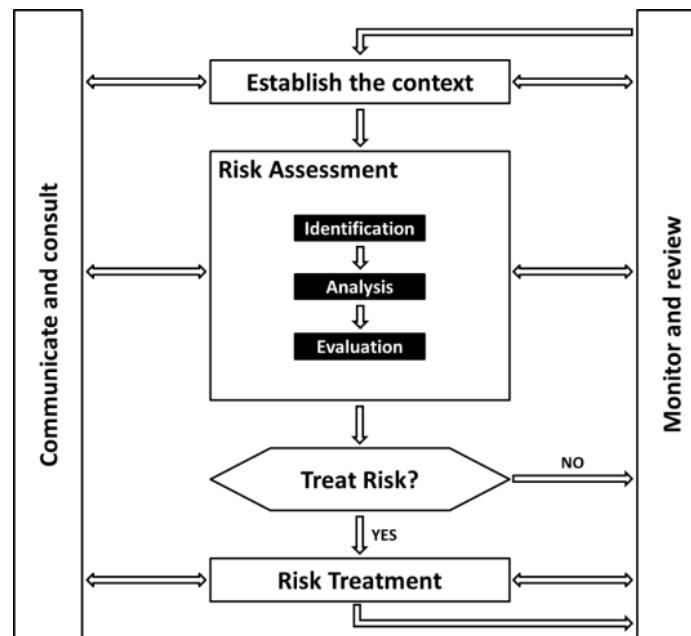


Figure 2-11 – Risk Management Framework

After the description of the key steps of the MAGERIT methodology,

- the key DSS assets are identified,
- the threats analysis for each asset category is performed, and
- the initial risks for DSS are identified by using an appropriated software tool.

A set of Safeguards has been identified in this architecture to mitigate the initial risks. Both preventive safeguards to reduce the probability that the threat will materialize and ex-post safeguards to delimit the consequences are considered.

DSS safeguards are chosen among suitable measures suggested by the SRA tool and organized according to the NIST Security Controls. The DSS identified technical safeguards with the focus on four main categories:

- Safeguards related to the Access Control mechanisms [AC]
- Safeguards related to the Identification and Authentication mechanisms [IA]
- Safeguards related to the Audit mechanisms [AU]
- Safeguards related to the Secure Communications [SC]

2.3 NAV-2 Integrated Dictionary

2.3.1 Abbreviations and Acronyms

| | |
|---------|---|
| AC | Alternating Current |
| AMN | Afghanistan Mission Network |
| APP | APPLication |
| AI | Artificial Intelligence |
| AU | Audit mechanisms |
| IA | Authentication mechanisms |
| BMS | Battery Management System |
| CBRNE | Chemical, Biological, Radiological, Nuclear and Explosive |
| CIMIC | Civil Military Cooperation |
| COTS | Commercial off-the-shelf |
| CROP | Common Reference Operational Picture |
| DDS | Data Distribution Services |
| DNV GL | Det Norske Veritas Germanischer Lloyd (NLD) |
| DEU | Deutschland (Germany) |
| DSS | Dismounted Soldier System |
| ET | Ejercito de Tierra |
| EM | Electro Magnetic |
| EW | Electronic Warfare |
| EDA | European Defence Agency |
| EU | European Union |
| XML | Extensible Markup Language |
| FMN | Federated Mission Networking |
| GVA | General Vehicle Architecture |
| GOSSRA | Generic Open Soldier System Reference Architecture |
| HF | High Frequency |
| HMI | Human-Machine Interface |
| IEM | Information Exchange Mechanism |
| IT | Information Technology |
| ISTAR | Intelligence, Surveillance, Target Acquisition and Reconnaissance |
| IP | Internet Protocol |
| ITA | Italy |
| JDSS | Joint Dismounted Soldier System |
| JDSSDM | Joint Dismounted Soldier System Data Model |
| JPEG | Joint Photographic Experts Group |
| LCG-DSS | Land Capability Group – Dismounted Soldier Systems |
| MQTT | Message Queue Telemetry Transport |
| MAGERIT | Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información |
| MDE | Ministerio de Defensa de España |
| NIST | National Institute of Standards and Technologies |
| NAV | NATO All View |
| NAF | NATO Architectural Framework |
| 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 |
| NEC | Network Enabled Capability |
| NATO | North Atlantic Treaty Organization |
| NBC | Nuclear Biological Chemical |
| OOTW | Operations Other Than War |
| POL | Poland |
| PNG | Portable Network Graphics |
| PRT | Portugal |
| PADR | Preparatory Action on Defence Research |
| PU | Public |
| RBCI | Radio-Based Combat Identification |
| RAS | Robotic & Autonomous System |
| SATCOM | SATellite COMMunications |
| SC | Secure Communications |
| SRA | Security Risk Assessment |
| STU | Small Tactical Unit |
| SW | Software |
| ESP | Spain |
| STANAG | Standardisation Agreement (NATO) |
| SWE | Sweden |
| TAR | Tactical Augmented Reality |
| TES | Tactical Edge Syndicate |
| TIFF | Tag Image File Format |
| TRL | Technology Readiness Levels |
| TCP | Transmission Connection Protocol |
| UHF | Ultra-High Frequency |
| UK | United Kingdom |
| USB | Universal Serial Bus |
| UDP | User Datagram Protocol |
| VMF | Variable Message Format |
| VHF | Very High Frequency |
| VR | Virtual Reality |
| XSD | XML Schema Documentation |

2.3.2 Referenced Documents

2.3.2.1 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

2.3.2.2 Document related references

- /9/ NATO Architecture Framework, Version 3, Annex 1, (AC/322)D(2007)XXX
- /10/ Guidelines for the Development of Architectures Compliant to NAFv3, EDAU1/1201/RP/008-2013, 12/08/2013
- /11/ Guidelines for the Development of Architectures Compliant to NAFv3, Annex I, EDAU1/1201/RP/008-2013, 12/08/2013
- /12/ Amutio, M. A., Mañas, J. A. (2014). MAGERIT version 3.0 Methodology for Information Systems Risk Analysis and Management, Book I - The Method, Spanish Ministry of Finance and Public Administration, July 2014.
- /13/ <https://www.act.nato.int/activities/fmn>