RHEINMETALL GROUP indra gmv LEONARDO LARIMART a LEONARDO company iTTi e-technologies & business TNO innovation for life tekever AEROSPACE | DEFENSE | SECURITY SAAB

GOSSRA

Generic Open Soldier System Reference Architecture

Collaborative Project

PADR_FPSS_A_2017_800783

GOSSRA Architecture for Standardisation - Vol. 7

Security View

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	Final Release

Table of Contents

Table of Figures

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 Sparx Systems Enterprise Architect (version 13) /8/.

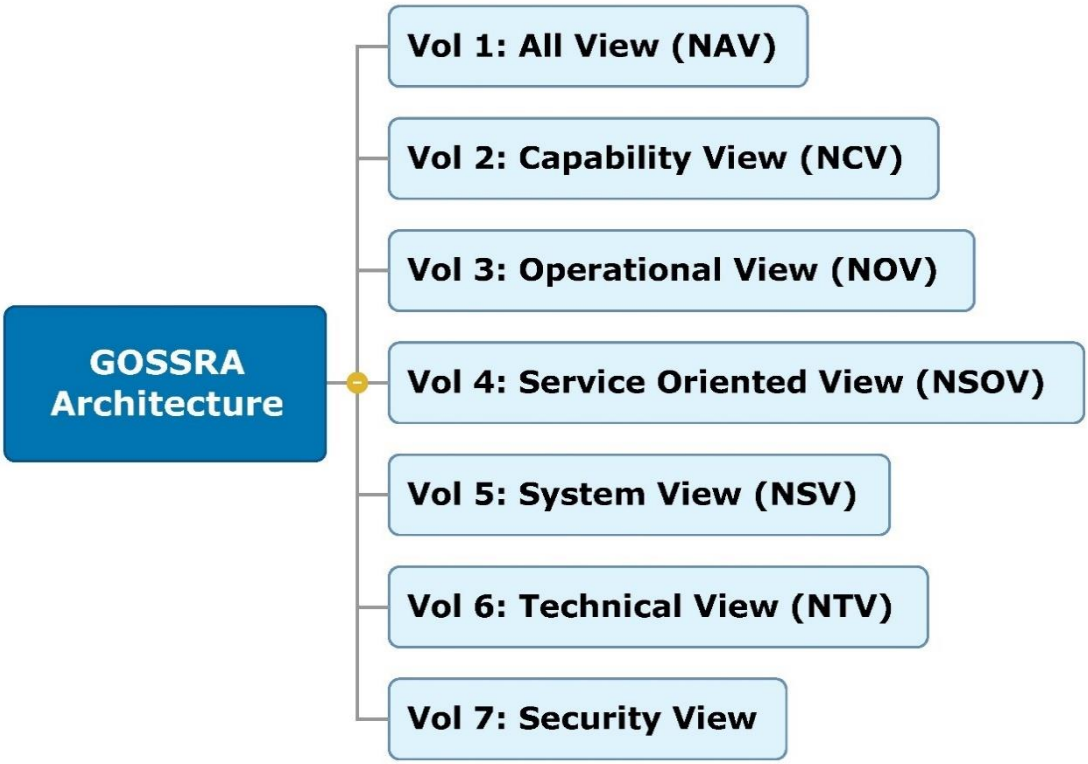

Figure 1-1 – GOSSRA Document Structure

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 Security View

2.1 Overview

The Security View specifies the set of security mechanisms to be adopted for mitigate the IT Security Risk of DSS Key components.

The selected security mechanisms are the outcome of a DSS IT Security Risk Assessment (SRA), which is the methodology adopted to evaluate the DSS security risk level, and identify appropriate safeguards to mitigate it.

This document also describes the process, which has been followed in terms of

- adopted methodology,
- DSS Model for SRA,
- steps performed

To evolve from an initial risk evaluation to a more robust DSS configuration which includes specific security mechanisms.

The selected security mechanisms are based on the NIST Security Controls (/10/).

This chapter is organised as follow:

- **Section 2.1:** Overview (this section);
- **Section 0:**

- IT Security Risk Assessment Process Description, which provides
  - an overall description of the adopted methodology,
  - the DSS context description.
- **Section 2.3:** Security Risk Assessment, which describes the steps, which have been performed to identify the security mechanisms.
- **Section 2.4:** IT Security Mechanism Specification, which specifies DSS security mechanisms to apply to the DSS key components in order to lower the IT Risk Level.

2.2 IT Security Risk Assessment Process Description

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 risks to minimize the impact of a potential threat on their operations to accomplish their goals.

The MAGERIT methodology ([/9/]) has been selected to perform the DSS Security Risk Assessment. The methodology process model for risk management, which is depicted in Figure 2-1, is cyclic, and iterative and starts from determining the context. The MAGERIT methodology actually describes a common approach for SRA making it portable on other methodologies and thus can be seen as generic as they mostly describe common activities applicable to risk analysis. Similar processes are for example common for system or functional safety (MIL-STD-822 or IEC 61508) and it can be seen, that these processes are used for different standards in this domain.

Three main phases can be identified:

- **Identification:**
  identify what might happen, once known the context and our internal structure (equipment, facilities and people);
- **Analysis:**
  analyse the likelihood and consequences of all has been identified;
- **Evaluation:**
  interpret this in terms of business analysis, ideally using metrics that allow us to compare our operational risk with other risks that affect the organization and we have to manage in a comprehensive way.

Once the risks are evaluated, it is up to the management bodies to decide if the risk is acceptable or if there is the need to continue the mitigation.

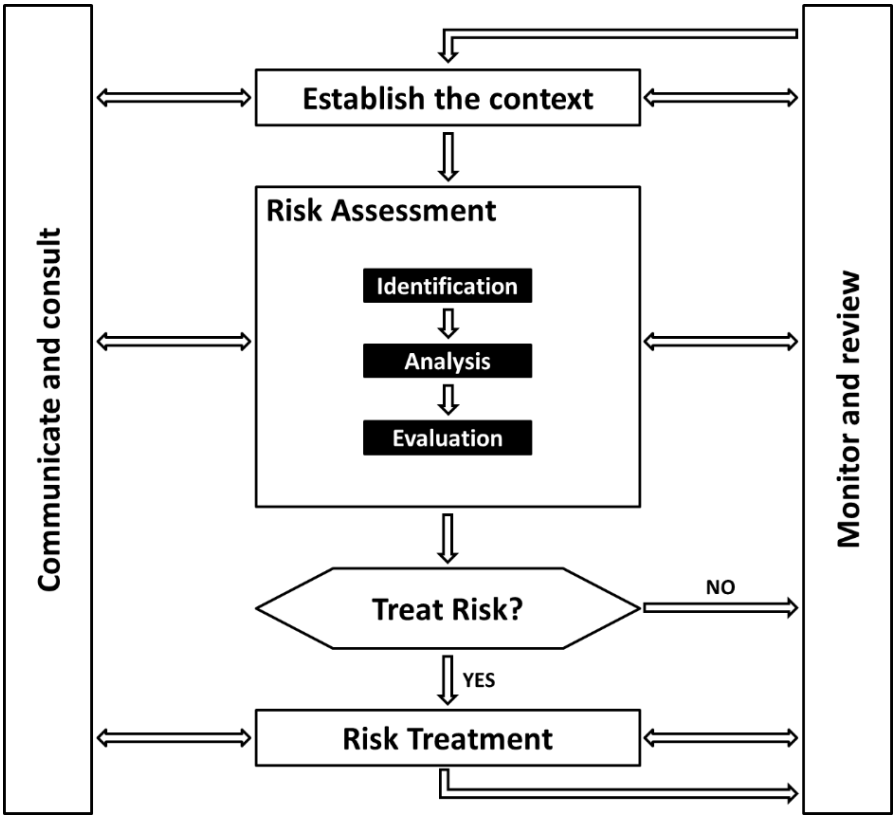

Figure 2-1 – Risk Management Framework

This is a complex decision and a need to find the point of balance between risks, opportunities and resources. It should not spend more to protect than the possible harm of failing to protect as it could be counterproductive to not accept risks without a counterpart in the benefits. But above all the most complicated are intangible risks of difficult quantifiable decisions such as reputation.

MAGERIT describes the following steps to complete the analysis (schema provided in Figure 2-2):

1. Set the context or **scope**.
2. Inventory the **assets** that need to be protected.
3. Characterize the **threats** on the assets.
4. Once defined what to protect (assets) and against what to protect (threats), it is possible to **calculate or estimate the potential risk**, defined as what is likely to happen if no countermeasures are in place.
5. Once evaluated the risks it is possible to **select protective measures** necessary or desirable to ward off potential risks.

When evaluated these safeguards, it is possible to estimate the residual risk. Safeguards are defined as protective measures in general, e.g. procedural and not only technical measures.

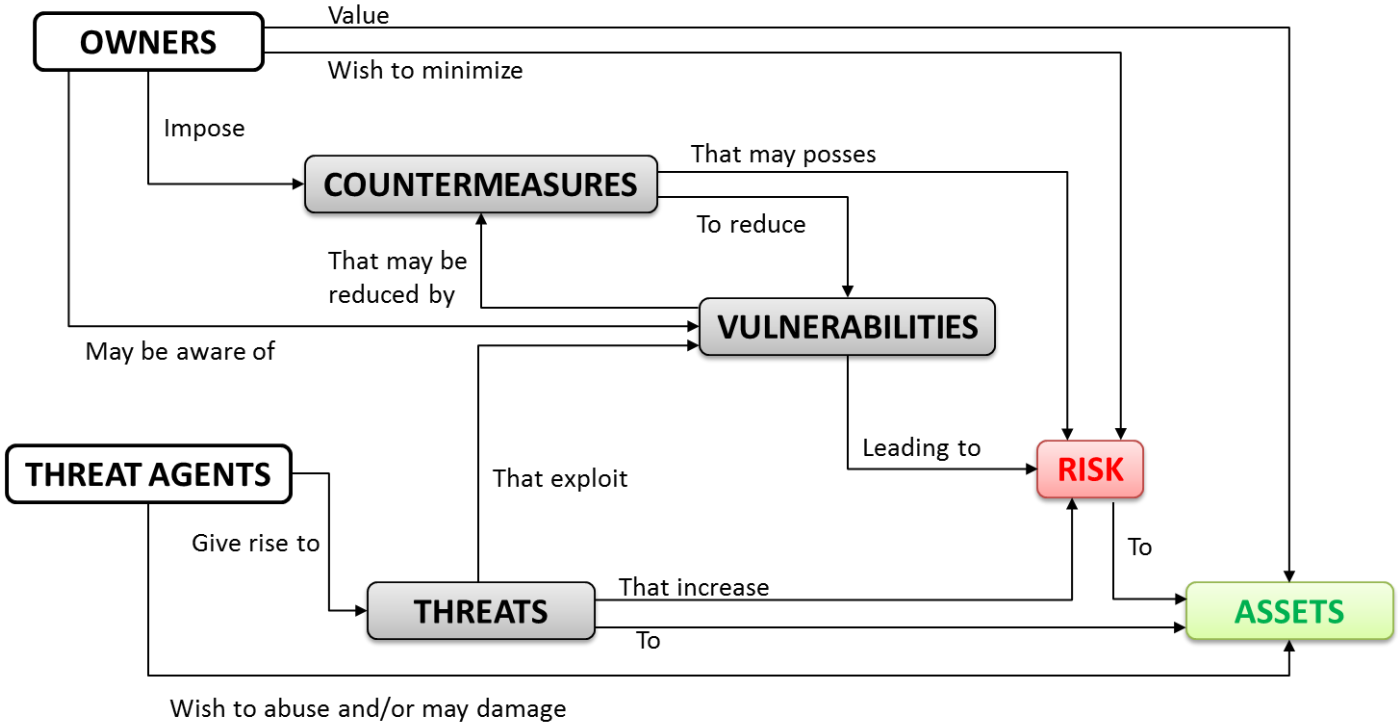

Figure 2-2 – Steps for Completing the Risk Analysis

MAGERIT distinguish between “essential assets” and “others”. Managed information and the services provided are essential. It is essential in the inevitable sense, being the reason for what the information system exists. Everything else, the own equipment or outsourced services, is subsidiary.

DSS *Essential assets* are those information (data) managed by the DSS in the operational phase.

DSS *Supporting assets* are services, software, hardware and personnel that carry and process these essential assets.

2.2.1 DSS Context for SRA

According to the MAGERIT methodology, SRA, for a DSS context, needs to be defined as starting point. This can be performed based on e.g. DSS communication scenarios for data exchange.

This section describes an example for a DSS system model which includes both

- DSS key services and
- DSS communication scenarios.

The example lists the most common features and interfaces and gives a guidance on how to approach systematically the SRA.

2.2.1.1 DSS Communication Scenarios for SRA

Functional Services for DSS can be organized according to the communication scenario. This type of schematization can help make DSS SRA elaboration and set the context or scope of SRA, according to the MAGERIT methodology ([RI]).

From the point of view of Operational Node Connectivity two different scenarios must be targeted:

- DSS Node External Connectivity
- DSS Node Internal Connectivity

Within these two communications scenarios a set of domains (Soldier Personal (DSS) Domain, Small Tactical Unit (STU) Domain, Inter-platform Domain, Joint Domain, Coalition Domain) have been identified, each detailing a given communications context, where a Soldier can operate either as a standalone unit or by interacting with other units of the system.

The Soldier Personal Domain can be referred to the “DSS Node Internal Connectivity” where the focus is centred on individual soldier in connection with internal sensors which represent devices or equipment used for acquiring data and especially tactical data. Such sensor systems typically use electro-optical, acoustic, or RADAR technology. “Power” is associated to the equipment which has electric/electronic functions.

The other domains are concerned with the “DSS Node External Connectivity” which provide basic equipment including sensors, effectors, computers, and communication equipment, to each individual soldier according to the branch and mission. Soldiers share awareness through a Common Relevant Operational Picture (CROP). The connection between the Platoon Commander System and the DSS Soldier-Squad establishes voice and data exchange via radio frequencies (RF) while enabling face-to-face communications. In this communication scenario the power services can include the possibility to exchange energy within the DSS Soldier-Squad, use re-charged batteries to get energy by another DSS or use a platform (ground, navy or air vehicle) to receive energy. When mounted on squad vehicle or helicopter, the DSS is connected, e.g. with a cable, in order to receive energy but also to be able to communicate by voice and exchange data.

A particular case in this scenario is Coalition DSS Squads/Teams that represents units of allied forces deployed in the same mission area when organized in multi-national forces (Coalition Domain). To establish and maintain a close cooperation of squads/teams of different nations a common communication service is necessary. For example, use of “Interoperability Radio”. Also, in this case the data to be exchanged are tactical data and NBC Information between multi-national squad DSS. Also, the exchange of energy if required needs to be possible.

For all communication scenarios, security countermeasures should be provided to protect the Availability, Integrity, Confidentiality, Authenticity and Accountability of the information managed or transferred by DSS and internally to DSS.

The following initial security solution are considered to be available when carrying out the DSS SRA:

- wireless and/or wired voice transmission will be protected by means of cryptographic mechanisms;
- wireless and/or wired data transmission will use a secure (encrypted) channel;
- operating systems, application software and cached data will be stored encrypted on the systems' storage;
- an Intrusion Detection System (IDS) or antivirus SW will exist within the system.

In this context a DSS security risk evaluation provides knowledge about the probability of a threat exploiting an asset's vulnerability as well as the potential impact it could have from a military operation, compliance, or technology perspective.

In order to finalize a security risk assessment and identify vulnerabilities capable of allowing threats to impact an entire DSS, individual sub-systems, or networks has been completed. This table shows security aspects associated to the Functional Services of a DSS to support Operational Services and related essential assets. This helps to identify the "essential assets" (according to the MAGERIT methodology) that must be protected and that will be translated in the DSS Security Risk Assessment.

2.2.1.2 DSS Key Services for SRA

Starting from the DSS Communication scenario described in section 2.2.1.1, the following system services have been identified as relevant candidate for DSS SRA:

- Basic DSS Services
  - Voice Communication
  - Data Transmission
  - Navigation
- Power Services
- Data Exchange Services
- C4I Services
  - Battlefield Management System (BMS)
  - Situational Awareness (SA)
  - Human RAS Interaction Services (HRI)
  - System Management Functional Area

2.3 The Security Risk Assessment for DSS Key Components

Due to the complexity of the whole DSS Reference Model, and related operational scenarios, focus is laid only on the key DSS components for the relevant communication scenarios, as described in section 2.2.1.1 for identifying the security mechanisms while following the MAGERIT methodology. This approach provides

- a better understanding about the adoption of a methodology to identify security mechanisms for a DSS Target System, e.g. MAGERIT, and
- a set of core security mechanisms which if applied to the DSS Key components can lower the IT risk level to operational values.

2.3.1 DSS SRA Approach

Before starting to describe the DSS SRA approach, it is necessary to establish the context correctly.

First of all, a precise overview of the security perimeter has to be done to focus the analysis, avoid over-design and define roles and responsibilities.

The following preparatory steps have been performed:

- *Personalization of SRA tool (configuration options)*: the NATO customization of the default NIST (/10/) catalogue of security control have been selected ;
- Analysis of the DSS Context, which is the communication scenario described in section 2.2.1.1 and applied to the STU Domain, i.e. DSS-STU Data Exchange;
- Identification of the initial countermeasures (if any): taking into account the DSS Context the following initial security countermeasures are supposed to be available in the DSS:
  - wireless and/or wired voice transmission will be encrypted
  - wireless and/or wired data transmission will be encrypted
  - operating systems, application software and cached data will be stored encrypted on the systems' storage
  - an IDS or antivirus SW will exist within the system
  - wireless link will be protected against unintentional jamming (EMI/EMC).

The SRA process has been supported by the PILAR toolset (/11/), which implements the MAGERIT methodology (/9/).

The SRA phases is summarised below:

- The first phase aims at evaluating the "risk value" for the *initial condition of a DSS SRA*, in terms of the risk level, when only basic set of security countermeasures are in place.
- The first phase results in a "matrix", which reports the risk level of each DSS key component, for each of the security "dimensions", i.e. Availability (A), Integrity (I), Confidentiality (C), Authenticity (Auth) and Accountability (Acc). This measure is a "qualitative" one.
- Starting from the outcome of the initial risk evaluation, the risk mitigation is the next phase, which identifies "*enhanced*" security requirements aiming at lowering, where necessary, the IT risk level of the DSS, and then identifies further countermeasures to reduce the initial "risk".
- The second phase results in a matrix, which shows to what amount the initial risk levels have been lowered by adopting the "*enhanced*" security requirements.

The following sections describe in details the key activity and results.

2.3.2 First Phase: Initial Risk Evaluation

Steps can be summarized with:

- DSS Assets Identification;
- Assets Dependency Relationship Definition ;
- DSS Assets (Initial) Evaluation

2.3.2.1 DSS Assets Identification

MAGERIT distinguishes between essential and dependent / sub-ordinate assets. *Managed Information* is essential and everything else, like services, own equipment or outsourced services are sub-ordinate assets.

An analysis of the DSS Context for SRA described in section 2.2.1, identifies the DSS essential assets for the SRA, summarises the outcomes of the performed analysis, and is organised as follows:

- DSS Functional Services, which list the DSS functional services addressed by the DSS Context for SRA;
- Description, which provides for a brief description of each specific service;
- Note, which reports supporting information such as, examples, constraints, or exceptions;
- DSS Security Assets, which lists the set of DSS security assets identified for each services.

DSS Functional Services		Description	Note	DSS Security Essential Assets
Basic DSS Services	Voice Communication	It provides devices/tools for a secure, reliable, comprehensible and bidirectional voice communications both in close and wide range and in any environment conditions.	• legacy CNR-Like point to multi-point voice service (Push-To-Talk voice) • voice Conference services such as voice group services by means ✓ of dedicated radio resources like Push-To-Talk voice ✓ of VoiP bearer services on all IP radio network	Essential asset that depends on this service: **Data Voice**
	Data Transmission	It provides devices/tools for a secure, reliable data transfer.	Data transmission is achieved using typical data ports of a radio device, such as Ethernet, USB, Serial, WiFi and Bluetooth. Data transmission also involves use of Wearable Personal Computer (WPC).	Essential asset that depends on this service: Real time data: • **Video streaming** • **VoIP calls** • **C2/C4I critical traffic** • **Fire support** • **Targeting** • **Data Exchange Services Control Data** Not Real time data: • **Messages** • **File** • **C2/C4I not critical traffic** • **Friendly Force Tracking (FFT)**

				• **Tactical Situation data**
	Soldier Protection	It provides devices and tools to increase the survivability of the soldier.	Only physical measures	**No IT mechanisms**
	Navigation	The functional service Navigation provides devices/tools: • for the determination of the best route to destination • for the consideration of topographic conditions and tactical situation • with several methods to guide along the best route to destination		Essential asset that depends on this service: • **Position/Route**
Assets Services in DSS		It includes: Power Supply Services, Power Distribution Services, Power Consumption Service, Power Information Services, and Power Control Services.	It represents the service from which depend all other services.	Essential asset that depends on this service: • **all data** • **power status**
Data Exchange (Inter-Platform, STU, Personal)		The Inter-Platform Data Exchange provides services to data exchange in the context of the battlefield, e.g. among different typologies of nodes.	Each data distribution relies on appropriate transport protocol(s), which is provided by the underlying network infrastructure.	Essential asset that depends on this service: **C4I data**

		The STU (Small Tactical Unit) Data Exchange provides services to data exchange in the context of a Squad/Team of dismounted soldiers, e.g. among DSS Nodes which are supposed to be within a given range of distance. The Personal Data Exchange provides services to data exchange in the context of the dismounted soldier, e.g. among the components of a same DSS Nodes	Tactical Data Link can be also operated directly over Radio Data Link.	
C4I Services	Battlefield Management System (BMS)	BMS displays and manipulates information and mapping relating to Battlefield Situational Awareness. The BMS services display and manipulate information relating to tactical and operational C2.	The BMS Services may exchange data on all of the Data Distribution Context	Essential asset that depends on this service: **C4I data**
	Situational Awareness (SA)	It will allow the access and control of sensors, both embedded and remote. SA services also provide for the acquisition, presentation and distribution of the sensor data, either sampled or streamed.	-	
	Human RAS (Robotic & Autonomous System) Interaction	It provides an operator for the set of capability to manage and control a (squad) of UxV(s). Typically, these	The HRI Services may exchange data in both Inter-Platform and, STU Data Exchange	

	Services (HRI)	services are available at DSS Squad level.	domains.	
	System Management	It provides services to manage the DSS as a system. It address the typical management functions, such as Fault Management, Configuration Management, Security Management, and Performance Management. Typically this set of services is supported by a centralized System Management Station. Moreover it also includes service to support (self-) coordination both in the STU and Inter-Platform domains.	Configuration management is concerned with monitoring system configuration information, and any changes that take place. DSS Security Management Services provide functions and tools to: • control access to assets in the DSS; • gather and analyses security-related information • manage DSS system authentication, authorization, and auditing, • configure and manage (i) security tools (such as firewalls, intrusion detection systems), (ii) security policies (such as access lists, trust naming schema).	

Table 2-1 – Functional Services to Support Operational Services and Related Essential Assets

DSS *Essential Assets* are:

- Voice (Voice)
- Real Time Data (RTD)
- Not Real Time Data (NRTD)
- Position (Pos)
- C4I Data (C4I D)
- Power Data Status (PWR)

DSS *Supporting assets* are the functional services, equipment (software, hardware, and infrastructure) and personnel that may process, transmit, and store the essential assets. The following supporting assets have been identified:

- Basic Service: Data Transmission (DT)
- Basic Service: Voice Communications (Voice S)
- Basic Service: Navigation (Nav)
- Services: C4I services (C4IS)
- Horizontal Service: Power services (PWR S)
- Horizontal Service: Data Distribution Services (DDS)
- Infrastructure: Facility Base Camp Charger (FBCC)
- Infrastructure: Platform (Platform)
- Infrastructure: other DSS Nodes (DSS)
- Equipment: Network devices (Net Dev)
- Basic equipment: Wearable Personal Computer (WPC)
- Basic equipment: Data Processing (Data Processing)
- Basic equipment: Radio & GNSS Receiver (Radio&Rec)
- Personnel: Operators (Ope)

2.3.2.2 Assets Dependency Relationship Definition

The analysis of DSS Context also addresses relationships among assets identified in the previous steps. In MAGERIT, it means that the value that some assets have to protect spreads to other assets on which they depend.

For instance: the value of the services spreads to the equipment (in terms of hardware/software) that supports it. The previously mentioned asset establishes the chain of spread from the value of what is essential to what must be protected for every type of user (person or entity).

Thanks to the graph of the dependence between assets, it is possible to focus on the value of the essential asset and let the tool calculate via the graph how much every subordinate asset should be protected.

The resulting dependency graph of the assets, following MAGERIT methodology, is shown in the figure below.

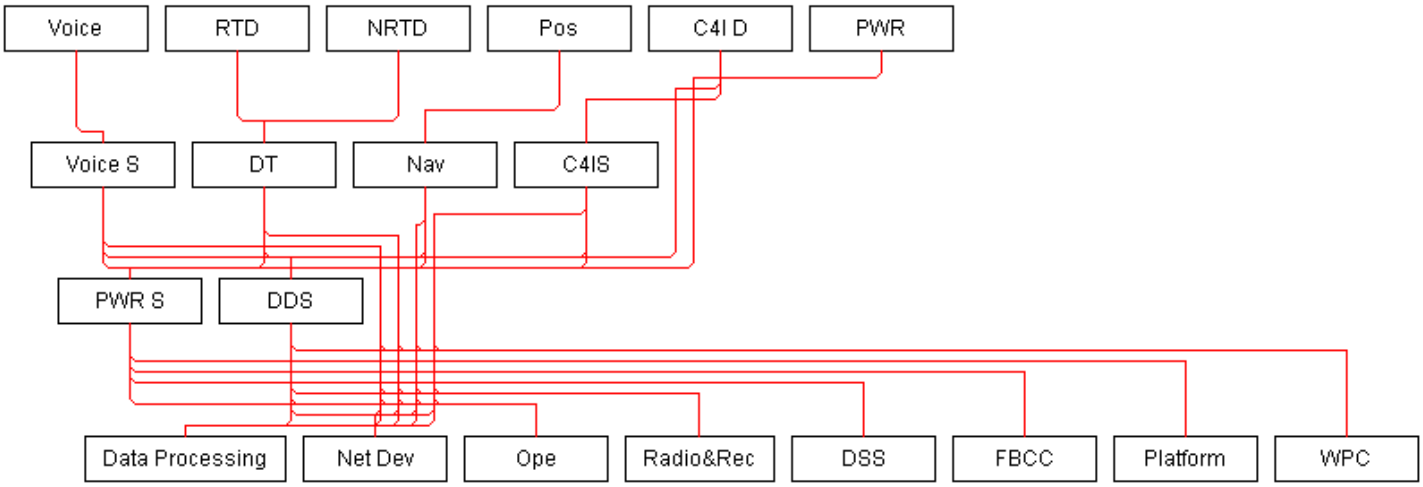

Figure 2-3 – Dependencies of DSS Assets

2.3.2.3 DSS Assets (Initial) Evaluation

MAGERIT allows to evaluate the assets (in grey rows in Table 2-2) then to spread their value to other assets (in green rows in Table 2-2) following the dependency graph (it means that the value that some assets have to protect, spreads to other assets on which they depend). At the end of dependencies definition, it is possible to know what *level of protection* needed by each asset, either directly or indirectly. In MAGERIT the *level of protection* is proposed in a range between 0 and 10. It is evaluated by the PILAR, which implements a set of rules aiming at standardize the risk analysis, so that the results for different assets are comparable. *Level of protection* evaluation process addresses the following security dimensions:

- **[A] Availability**
  is defined as “Ensuring timely and reliable access to and use of information” [ISACA, Cybersecurity Fundamentals Glossary, 2016];
- **[I] Integrity**
  is defined as “The property that sensitive data has not been modified or deleted in an unauthorised and undetected manner”;
- **[C] Confidentiality**
  is defined as “Preserving authorised restrictions on access and disclosure, including means for protecting privacy and proprietary information” [ISACA, Cybersecurity Fundamentals Glossary, 2016];
- **[Auth] Authenticity**
  is defined as “Undisputed authorship” [ISACA, Cybersecurity Fundamentals Glossary, 2016];
- **[Acc] Accountability**
  is defined as “The ability to map a given activity or event back to the responsible party” [ISACA, Cybersecurity Fundamentals Glossary, 2016].

The table below provides the level of protection needed for each asset in terms of the selected security dimensions. The higher the value, the more protection a given asset requires.

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS					
[D] Data					
[Voice] Voice	[5]	[5]	[7]	[3]	[3]
[RTD] Real Time Data	[9]	[5]	[7]	[7]	[3]
[NRTD] Not Real Time Data	[4]	[5]	[7]	[7]	[3]
[Pos] Position	[7]	[5]	[3]	[5]	[3]
[C4I D] C4I Data	[7]	[7]	[7]	[7]	[3]
[PWR] Power Data Status	[7]	[7]	[3]	[5]	[1]
[Services] Services					
[Basic] Basic					
[DT] Data Transmission	[9]	[5]	[7]	[7]	[3]
[Voice S] Voice Communication	[5]	[5]	[7]	[3]	[3]
[Nav] Navigation Service	[7]	[5]	[3]	[5]	[3]
[Horizontal] Horizontal					
[PWR S] Power Service	[9]	[7]	[7]	[7]	[3]
[DDS] Data Distribution Service	[9]	[7]	[7]	[7]	[3]
[C4IS] C4I Service	[7]	[7]	[7]	[7]	[3]
[E] Equipment					
[Net Dev] Network Devices	[9]	[7]	[7]	[7]	[3]
[Basic Equipment] Basic Equipment					
[WPC] Wearable Personal Computer	[9]	[7]	[7]	[7]	[3]
[Data Processing] Data Processing	[9]	[7]	[7]	[7]	[3]
[Radio&Rec] Radio&GNSS Receiver	[9]	[7]	[7]	[7]	[3]
[I] Infrastructure					
[Platform] Platform	[9]	[7]	[7]	[7]	[3]
[FBCC] Facility Base Camp Charge	[9]	[7]	[7]	[7]	[3]
[DSS] Other DSS Nodes	[9]	[7]	[7]	[7]	[3]
[P] Personnel					
[Ope] Operators	[9]	[7]	[7]	[7]	[3]

Table 2-2 – Level of Needed Protection for Assets

Criteria for evaluation of assets can be:

- Personnel Information
- Legal and Regulatory Obligations
- Security
- Commercial and Economics Interests
- Disruption of Activities
- Public Order
- Operations/Logistic Mission
- Administration & Management
- Loss of goodwill
- Crime Prosecution
- Personal safety
- Recovery Time Objective
- Classified Information

And shall be read according to the criteria in Table 2-3.

Criteria for evaluation					
Data	[A]	[I]	[C]	[Auth]	[Acc]
Voice	Operations/Missions: (5) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission beyond a local level	Operations/Missions: (5) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission beyond a local level	Operations/Missions: (7) is likely to cause damage to the operational effectiveness of security of operations/mission	Operations/Missions: (3) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission at local level	Operations/Missions: (3) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission at local level
RTD	Recovery Time Objective (7) RTO< 4 hours	Disruption of activities: (5) is likely to cause disruption to activities within an organization and some impact on other organizations	Security: (7) is likely to lead to a major breach of security, or prejudice the investigation of security incident	Disruption of activities: (7) is likely to impact other organization	Security: (3) is likely to lead to a breach of security, or prejudice the investigation of security incident
NRTD	Recovery Time Objective (4) 4 hours<RTO< 1day	Disruption of activities: (5) is likely to cause disruption to activities within an organization and some impact on other organizations	Security: (7) is likely to lead to a major breach of security, or prejudice the investigation of security incident	Disruption of activities: (7) is likely to impact other organization	Security: (3) is likely to lead to a breach of security, or prejudice the investigation of security incident
Pos	Personal safety: (7) may lead to injury to multiple individuals	Operations/Missions: (5) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission beyond a	Operations/Missions: (3) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission at local	Disruption of activities: (5) is likely to cause disruption to activities within an organization and some impact on other organizations	Operations/Missions: (3) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission at local

		local level	level		level
C4ID	Operations/Missions: (7) is likely to cause damage to the operational effectiveness of security of operations/mission	Security: (7) is likely to lead to a major breach of security, or prejudice the investigation of security incident	Operations/Missions: (7) is likely to cause damage to the operational effectiveness of security of operations/mission	Security: (7) is likely to lead to a major breach of security, or prejudice the investigation of security incident	Security: (3) is likely to lead to a breach of security, or prejudice the investigation of security incident
PWR	Operations/Missions: (7) is likely to cause damage to the operational effectiveness of security of operations/mission	Operations/Missions: (7) is likely to cause damage to the operational effectiveness of security of operations/mission	Operations/Missions: (3) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission at local level	Operations/Missions: (5) is likely to make it more difficult to maintain the operation effectiveness or security of operation/mission beyond a local level	Security: (1) could lead to a breach of security, or prejudice the investigation of security incident

Table 2-3 – Explanation of Asset Evaluation Results

2.3.2.4 Threat Analysis

In order to calibrate the threats there is the need to consider the following:

- probability of occurrence of a threat;
- impact on the affected assets if the threat occurs.

The *Probability of occurrence* can be modelled as:

Symbol	Level	Frequency
VH	Very High	100
H	High	10
M	Medium	1
L	Low	0.1
VL	Very Low	0.01

Table 2-4 – Likelihood of a threat

The second element to define a threat is to estimate the impact of its occurrence.

MAGERIT uses a value named *degradation*, caused by the incident, as an intermediate step that facilitates reasoning and increases the credibility of the results.

Degradation provides a qualitative measure of the loss in value of an asset as a result of the materialization of a threat. The SRA tool measures the “degradation” that each specific threat produces on DSS assets in terms of: [A] Availability, [I] Integrity, [C] Confidentiality, [Auth] Authenticity, and [Acc] Accountability. The consequences of a threat are evaluated as in Table 2-5.

Symbol	Level	Percentage
T	Total	100%
VH	Very High	90%
H	High	50%
M	Medium	10%
L	Low	1%

Table 2-5 – Degradation Values

By default, the tool applies the NATO/NIST attack profile that establishes which threats are likely for each asset, and estimates its likelihood and its consequences. The profile is an external file (either XML or Excel), and the file is referenced as TSV (Threat Standard Value) file. For each asset and security dimension, it specifies the standard likelihood, and degradation of value. The standard library establishes the available threats.

For each asset a set of applicable threats has been selected. The tool suggests the applicable threats associated to an asset. The user may revise the suggestion and associate the selected threats to the selected asset.

TSV specifies information per asset. When something is specified for an asset, it applies to every refinement (asset components) unless explicitly requalified. For every class, the most specific data apply.

The set of threats selected for DSS are listed in Figure 2-4.

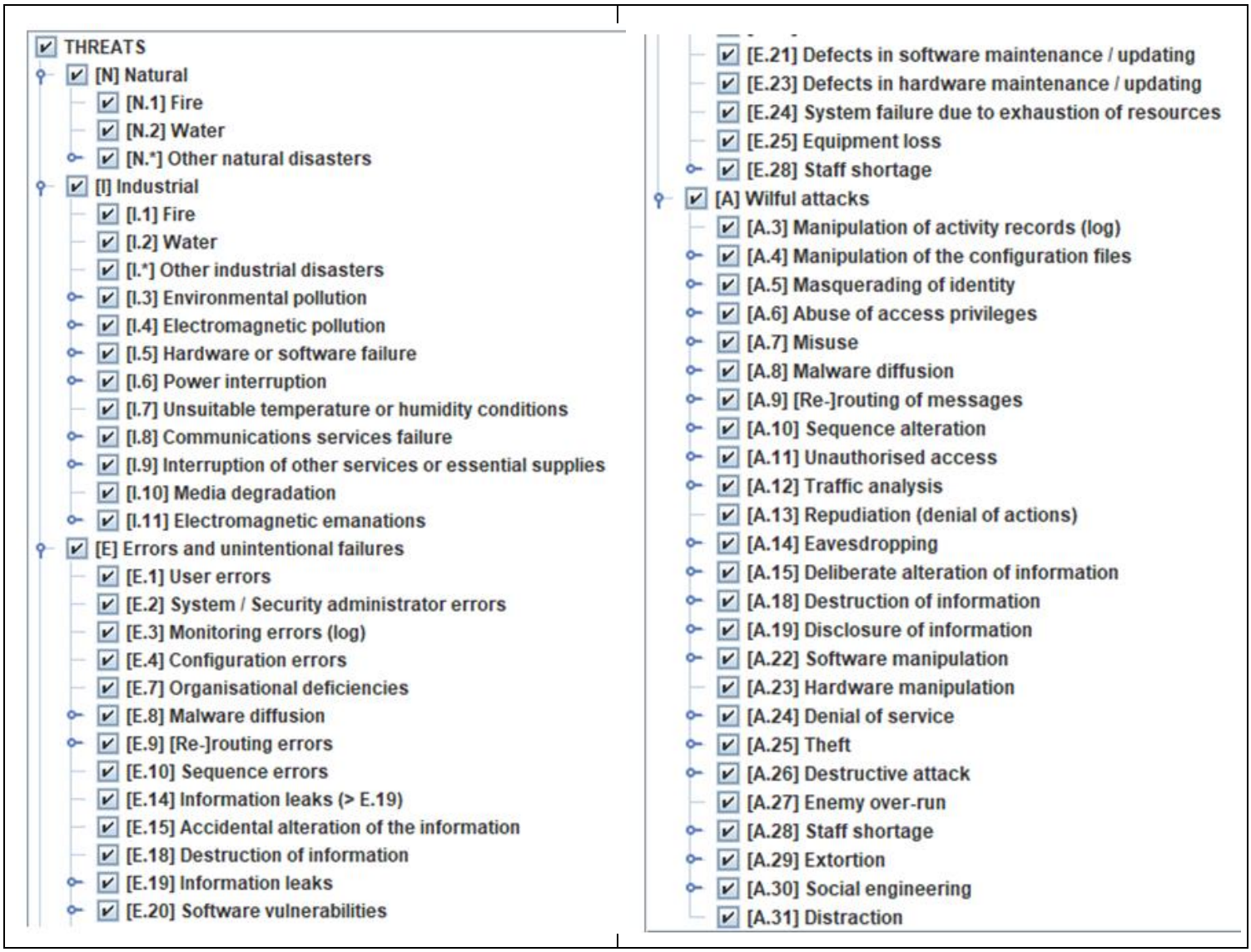

Figure 2-4 – Threats to DSS

2.3.2.5 Initial (Potential) Risk for DSS

Initial risk for DSS is based on the Risk Indicator that measures its probability to occurs. It is obtained by combining the threat *impact* with the threat *probability of occurrence*. A qualitative risk assessment produces a value of the risk as show in Figure 2-5.

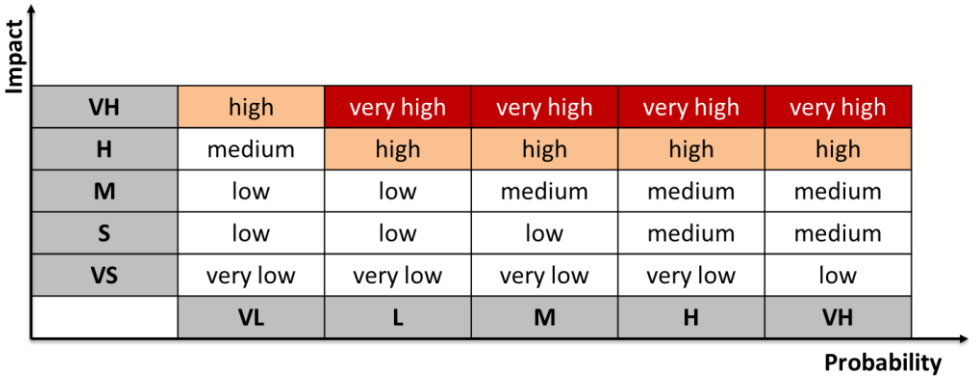

Figure 2-5 – Risk indicator

Initial Risk for DSS has been calculated considering only the minimum countermeasures. Figure 2-6 shows that as the initial risk is spread on each security dimension, the higher the value and the higher the risk. The tool identifies a Hot Zone, which is characterised by risk values in the range of 5 to 9.

asset	[A]	[I]	[C]	[Auth]	[Acc]
ASSETS	{7.4}	{6.3}	{6.3}	{5.9}	{3.3}
[D] Data	{5.9}	{6.3}	{6.3}	{5.9}	
[Voice] Voice	{1.2}	{3.9}	{6.3}	{3.6}	
[RTD] Real Time Data	{3.6}	{3.9}	{6.3}	{5.9}	
[NRTD] Not Real Time Data	{0.93}	{3.9}	{6.3}	{5.9}	
[Pos] Position	{3.7}	{2.5}	{0.81}	{1.2}	
[C4I D] C4I Data	{4.2}	{6.3}	{6.3}	{5.9}	
[PWR] Power Data Status	{5.9}	{5.4}	{0.46}	{3.0}	
[Services] Services	{6.6}	{5.4}	{4.5}	{5.1}	{3.3}
[Basic] Basic	{6.6}	{4.2}	{4.5}	{5.1}	{3.3}
[DT] Data Transmission	{6.6}	{4.2}	{4.5}	{5.1}	{3.3}
[Voice S] Voice Communication	{4.2}	{4.2}	{4.5}	{2.7}	{3.3}
[Nav] Navigation Service	{5.4}	{4.2}	{2.2}	{3.9}	{3.3}
[Horizontal] Horizontal	{6.6}	{5.4}	{4.5}	{5.1}	{3.3}
[PWR S] Power Service	{6.2}	{0}	{0}		
[DDS] Data Distribution Service	{6.6}	{5.4}	{4.5}	{5.1}	{3.3}
[C4IS] C4I Service					
[E] Equipment	{7.4}	{3.8}	{5.7}	{5.1}	
[Net Dev] Network Devices	{6.6}	{3.2}	{4.5}		
[Basic Equipment] Basic Equipment	{7.4}	{3.8}	{5.7}	{5.1}	
[WPC] Wearable Personal Computer	{7.4}	{3.2}	{5.7}		
[Data Processing] Data Processing	{6.6}	{3.2}	{4.5}		
[Radio&Rec] Radio&GNSS Receiver	{6.6}	{3.8}	{4.5}	{5.1}	
[I] Infrastructure	{6.2}				
[Platform] Platform	{6.2}				
[FBCC] Facility Base Camp Charge	{6.2}				
[DSS] Other DSS Nodes	{6.2}				
[P] Personnel	{5.4}	{4.5}	{5.4}		
[Ope] Operators	{5.4}	{4.5}	{5.4}		

Figure 2-6 – Initial Risk for Damaging a DSS Asset

Initial condition shows that DSS is subject to *high* initial risk for all security dimensions, with the only exception of the accountability. Figure 2-7 shows the top ten risks for a DSS.

potential | Initial | PILAR | summary (impact) | summary (risk)

asset	threat	R
[WPC] Wearable Personal Computer	[A.25] Theft	{7.4}
[WPC] Wearable Personal Computer	[E.24] System failure due to exhaustion of r...	{6.6}
[Data Processing] Data Processing	[E.24] System failure due to exhaustion of r...	{6.6}
[Net Dev] Network Devices	[E.24] System failure due to exhaustion of r...	{6.6}
[DT] Data Transmission	[E.24] System failure due to exhaustion of r...	{6.6}
[DDS] Data Distribution Service	[E.24] System failure due to exhaustion of r...	{6.6}
[WPC] Wearable Personal Computer	[A.24] Denial of service	{6.5}
[Data Processing] Data Processing	[A.24] Denial of service	{6.5}
[Net Dev] Network Devices	[A.24] Denial of service	{6.5}
[C4I D] C4I Data	[A.3] Manipulation of activity records (log)	{6.3}

Figure 2-7 – Top Ten (Initial) Risks on DSS

The risk analysis starts from a potential situation (minimal safeguards in place), which ends the first RSA phase. Then the second phase is started, which is the risk mitigation and applying the extra safeguards. Safeguards reduce the impact and/or probability. Usually one applies first *preventive measures* (which reduce the threat occurrence probability) and then defines *ex post measures* to limit the impact when the preventive resources become expensive, either in terms of cost, either in terms of productivity loss (system usage uncomfortable).

The analysis ends when the residual risk is preferably outside the hot zone.

2.3.3 Second Phase: Risk Mitigation

This phase aims at lowering the set of risk level values on an asset and security dimensions by selecting an appropriate set of safeguards. Security mechanisms are usually applied iteratively in different combinations in order to finally achieve an acceptable risk level. These security mechanisms represent a set of security services to be deployed on a specific Target DSS implementation.

The *Residual Risk Level* is the value of risk for each security dimension and for each asset which is evaluated after the adoption of the selected safeguards.

The adopted tool has a large catalogue of security measures under the name safeguards. Safeguards are organized as a tree, where top safeguards are refined into detailed safeguards.

DSS safeguards have been chosen among suitable measures suggested by the SRA tool, configured in accordance with the NIST [/10/] catalogue in order to work with the safeguards grouped in security controls;

As a first step the subset of safeguards that apply to DSS Context for SRA has been selected.

Safeguards are selected by security domains: each security domain may have different safeguards.

The tool calculates a *recommendation level* (0 to 10) for each safeguard in each domain, taking into account:

- the assets in the domain;

- level of security required, directly or indirectly, for each dimension for each asset in the domain;
- ability of each safeguard to protect each security dimension;
- inherent power (strength) of the safeguard.

Safeguards can be classified in two main groups:

- preventive safeguards, which reduce the probability that the threat will materialize.
- ex post measures, which do not influence the probability of occurrence, but limit the consequences.

In the left of Figure 2-8 are grouped measures that directly face the threats. In the right part there are the measures that do not face any threat themselves, but their absence would undermine the effectiveness of measures left column.

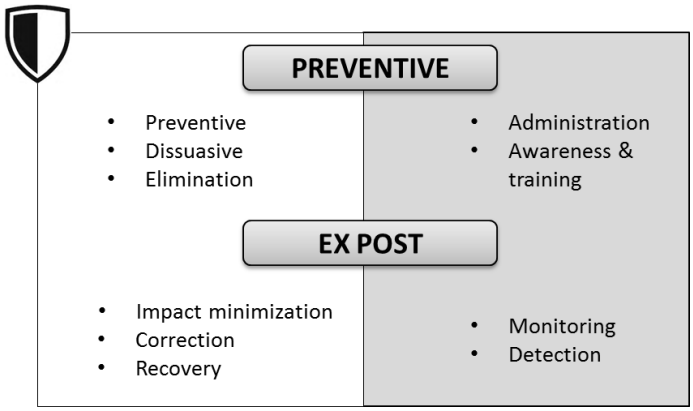

Figure 2-8 – Safeguards groups

Safeguards evaluation is based on a metric of maturity, which is provided by the SRA tool, and is classified as shown in Figure 2-9.

EFFECTIVENESS	-	0%	10%	50%	80%	90%	100%
LEVEL	NA	L0	L1	L2	L3	L4	L5
MATURITY	Not applicable	Non-existent	Initial / ad hoc	Reproducible intuitive	Defined Process	Managed and measurable	Optimised

Figure 2-9 – Safeguards evaluation

When evaluating the safeguards using the metric of maturity, a weight to each level will be given.

There are no universal rules on how to calculate this composition, so each tool uses its own heuristics, but the result will be between levels L0 and L5. Between these two points, 0% and 100%, is usually applied a Paretos' rule, which informally says that 20% of efficiency of protective measures mitigates risk by 80%, and for mitigating the remaining risk 20% it is necessary to increase another 80% of efficiency.

When the safeguards are upgraded, although not perfect, improvements in the system lead to marginal improvements in security.

The figure below depicts a comparison of the risk values between *Initial Risk* Levels (Initial Column) and *Residual Risk Levels* (PILAR column).

potential | Initial | PILAR | summary (impact) | summary (risk)

asset	threat	dimension	Initial	PILAR
[WPC] Wearable Personal Computer	[A.25] Theft	[A]	{7.4}	{3.8}
[WPC] Wearable Personal Computer	[E.24] System failure due to exhaustion of resources	[A]	{6.6}	{2.9}
[Data Processing] Data Processing	[E.24] System failure due to exhaustion of resources	[A]	{6.6}	{2.9}
[Net Dev] Network Devices	[E.24] System failure due to exhaustion of resources	[A]	{6.6}	{2.9}
[DT] Data Transmission	[E.24] System failure due to exhaustion of resources	[A]	{6.6}	{2.7}
[DDS] Data Distribution Service	[E.24] System failure due to exhaustion of resources	[A]	{6.6}	{2.6}
[WPC] Wearable Personal Computer	[A.24] Denial of service	[A]	{6.5}	{2.9}
[Data Processing] Data Processing	[A.24] Denial of service	[A]	{6.5}	{2.9}
[Net Dev] Network Devices	[A.24] Denial of service	[A]	{6.5}	{2.8}
[C4I D] C4I Data	[A.3] Manipulation of activity records (log)	[I]	{6.3}	{2.6}
[PWR S] Power Service	[A.26] Destructive attack	[A]	{6.2}	{2.8}
[FBCC] Facility Base Camp Charge	[I.1] Fire	[A]	{6.2}	{2.8}
[DSS] Other DSS Nodes	[N.1] Fire	[A]	{6.2}	{2.8}

Figure 2-10 – Comparison between Initial Risk and Residual Risk

The following considerations apply:

- Risk on Availability was significantly reduced by 33% (or more);
- Effectiveness in reducing the risk on Authenticity is high (efficiency between 30% and 60%).
- The result is a significant reduction of security risk on all axis. However, Availability and Integrity maintain a residual risk near the high value. This result can be explained because the analysis has been done on the DSS without introducing some countermeasures to the environment that hosts the DSS.
- The decision to accept the residual risk on the DSS is in charge to the management. Two important elements need to be demonstrated to defend the decision:
    - the **countermeasures are sufficient**: if the countermeasures do what they claim to do, the threats to the assets are countered;
    - the **countermeasures are correct**: the countermeasures do what they claim to do.

The next section describes the outcome of the safeguards selection, and specifies the set of security mechanisms selected to mitigate the DSS risk level.

2.4 IT Security Mechanism Specification

Starting from DSS SRA results, each technical security safeguards will be analysed in order to define specific and useful DSS security mechanism.

DSS safeguards have been chosen among suitable measures suggested by the SRA tool. Safeguards have been organized according to the NIST Security Controls (/10/).

For each security measure in DSS SRA, column [recommendation] is an estimate by the tool on the cost/benefits of the given safeguards.

It is a rank in the range [0 to 10], estimated by the tool taking into account the assets, the security dimensions, and the level of risk addressed by this safeguard.

It is a cost-effectiveness choice to deepen on those measures that have an immediate and strong reductive impact on the initial risks whose value is in the range [**5-9**].

2.4.1 DSS Non-Technical Safeguards

Physical and Environmental Protection, Personnel Security, System and Information Integrity, Contingency Planning safeguards, support technical safeguards to achieve a whole security solution to contrast DSS applicable threats. The selected Technical Safeguards, which are specified in section 2.4.2 suppose that the following non-technical safeguards are adopted:

- **Controls on Physical Access** to power and network distribution and transmission lines within DSS using physical security safeguards to help prevent accidental damage, disruption, and physical tampering.
- **Protection** of DSS **from Information Leakage** due to electromagnetic signals emanations (in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information).
- **Flaw Remediation** process and activities (patches, service packs, hot fixes, and anti-virus signatures). DSS should address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases can be used in remediating flaws discovered in the system.
- **Information System Monitoring**: anomalies within DSS include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses. DSS employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the system.
- **Alternate Storage Site**.
- **Information System Backup**.

2.4.2 DSS Technical Safeguards

DSS Technical safeguards identified by the tool allow us to concentrate on four main categories:

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

The introduction of those mechanisms into architecture is desirable because their “weight” in resolving the DSS initial risk is very high (on average, they worth 7).

The following paragraphs describe the set of safeguards selected for each categories.

Each paragraph also provides for a table (Table 2-6, Table 2-7, Table 2-8, and Table 2-9), which specifies the recommended security mechanisms and relate them to the selected safeguards. The tables include a row for each safeguard and its columns are organised as follows:

- **Recom.**
  provides a value of the effectiveness, and related costs, of a given safeguards
- **ID**
  identifier of the safeguards in the NIST Security Controls;
- **Name**
  safeguards name
- **Description**
  provides a generic description of the safeguard
- **Security Mechanisms**
  specifies the set of related security mechanisms to deploy in a Target DSS System.

2.4.2.1 Access Control Safeguards [AC]

The set of selected Access Control safeguards includes:

- Account Management and Access Enforcement
- Separation of duties
- Security attributes
- Wireless access
- Access for mobile devices

Account management

Account management requires that all users within DSS have to be managed according to a defined Account Management. Automated mechanisms could be used to support the management of information system accounts. Operations in account management could include:

- Removal of Temporary / Emergency Accounts
- Disable Inactive Accounts
- Automated Audit Actions (The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies)
- Role-Based Schemes
- Restrictions on Use of Shared Groups / Accounts
- Account Monitoring / Atypical Usage

Access enforcement

Access enforcement rely on enforcing authorized access at the system level and recognizing that DSS can host many applications and services in support of missions and operations. Access enforcement mechanisms can also be employed at the application and service level to provide increased information security. For example, DSS can enforce use of Discretionary Access Control (DAC) policies.

Separation of duties

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion.

Session locks

Session locks are temporary actions taken when users move away from the immediate vicinity of system or it leaves his personal devices for an imminent danger. The DSS could satisfy this control by means of biometrical mechanism within the personal devices.

Information is represented internally within DSS using abstractions known as data structures. Internal data structures can represent different types of entities, both active and passive. Active entities, also known as subjects, are typically associated with individuals, devices, or processes acting on behalf of individuals. Passive entities, also known as objects, are typically associated with data structures such as records, buffers, tables, files, inter-process pipes, and communications ports. *Security attributes*, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. DSS can define the types of attributes needed for selected information systems to support mission functions. For example, release markings or security labelling (classification level for objects and clearance (access authorization) level for subjects). This is applicable also to the personal devices.

Wireless access

In addition to the encryption mechanisms that could be used to protect access to the DSS wireless networks, wireless access must be protect by means of security mechanisms in reducing the power of wireless transmissions, in controlling wireless emanations and in using directional/beam forming antennas.

Access Control for Mobile Device

Mobile device for DSS is primarily a personal computing device. The processing, storage, and transmission capability of this device may be comparable to or merely a subset of desktop systems. Personal device has to be included within a configuration management and a device identification and authentication process. Container-based encryption provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields.

Table 2-6 specifies the recommended security mechanisms and relates them to the selected safeguards.

Recom.	ID	Name	Description	Security Mechanisms
5	AC-2	Account Management	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration.	DSS should: a. Identify roles mapped to accounts; b. Assign account managers for accounts; c. Establish conditions for group and role membership; d. Specify authorized users of DSS, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; e. Monitor the use of accounts; No group or shared accounts are to be used within the system.
5	AC-3	Access Enforcement	Access control policies (e.g., identity-based policies, role-based policies, control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in the system.	DSS should enforce use of Discretionary Access Control (DAC) policies over defined subjects and objects.
7	AC-5	Separation of Duties	Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.	DSS should: a. Separate, at a minimum, the administrative functions into three areas: System Administrator, Network Administrator and Information Assurance Officers; b. Define information system access authorizations to support separation of duties. Roles for network administration must be separated from other sensitive functions, such as cryptographic key management, hardware management, removable media data transfer, system security management, or access to particularly sensitive information.

5	AC-11	Session Lock	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of i system but do not want to log out because of the temporary nature of their absences.	DSS should satisfy this control by means of biometrical mechanism within the personal devices.
6	AC-16	Security Attributes	Security attributes, a form of metadata, are abstractions representing the basic properties or characteristics of active and passive entities with respect to safeguarding information. These attributes may be associated with active entities (i.e., subjects) that have the potential to send or receive information, to cause information to flow among objects, or to change the information system state. These attributes may also be associated with passive entities (i.e., objects) that contain or receive information. The association of security attributes to subjects and objects is referred to as binding and is typically inclusive of setting the attribute value and the attribute type.	DSS should: a. Provide the means to associate defined security attributes having defined security attribute values with information in storage, in process, and/or in transmission; b. Ensure that the security attribute associations are made and retained with the information; c. Establish the permitted defined security attributes for high and low side information systems; and d. Determine the permitted values for each of the established security attributes.
7	AC-18	Wireless Access	Wireless technologies include, for example, microwave, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication.	DSS should: a) Establish usage restrictions, configuration/connection requirements, and implementation guidance to prevent wireless access through conscious configuration actions. b) Protect wireless access to the system using authentication of both users and devices as appropriate (users to enterprise services and devices to wireless networks) and encryption. c) Disable, when not intended for use, wireless networking capabilities internally embedded within the system components prior to issuance and deployment. d) perform action or use mechanism in order to: (i) reduce the power of wireless

				transmissions so that the transmissions are less likely to emit a signal that can be used by adversaries outside of the physical perimeters of organizations; (ii) employ measures such as TEMPEST to control wireless emanations; and (iii) use directional/beam forming antennas that reduce the likelihood that unintended receivers will be able to intercept signals. As general rule, mission authorizations to allow selected users to configure wireless networking capability are enforced in part, by the access enforcement mechanisms employed within organizational information systems.
5	AC-19	Access Control for Mobile Devices	A mobile device is a computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non- removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, and/or built-in features for synchronizing local data with remote locations.	DSS should enforce: a) implementation of mandatory protective software (e.g., malicious code detection, firewall), b) scanning devices for malicious code, c)updating virus protection software, d)scanning for critical software updates and patches, e)conducting primary operating system (and possibly other resident software) integrity checks, f) and disabling unnecessary hardware (e.g., wireless, infrared). Furthermore, in order to protect access to classified information: a) Restricts the connection of classified personal devices to classified information systems in accordance with Partner Nation security policies. b) Prohibits the use of unclassified personal devices in transmitting

				classified information unless specifically permitted by the authorizing official. DSS should employ full-device encryption to protect the confidentiality and integrity of information on all personal devices.

Table 2-6 – Access Control Mechanisms

2.4.2.2 Audit and Accountability Safeguards [AU]

The set of selected Audit and Accountability safeguards includes:

- Audit Events
- Audit Reduction and Report Generation
- Time stamp
- Protection of audit information
- Audit Retention

Audit Events

Audit Events is any observable occurrence in a system. DSS should identify audit events as those events which are significant and relevant to the security and the environments in which the system operates in order to meet specific and ongoing audit needs. DSS shall enable security mechanism able to generate and collect security audit. Because of the distributed nature of the audit information, cross-organization sharing of audit information may be essential for effective analysis of the auditing being performed.

Audit reduction

Audit reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analyse. Events of interest can be identified by the content of specific audit record fields including, for example,

- identities of individuals,
- event types,
- event locations,
- event times,
- event dates,
- system resources involved,
- IP addresses involved, or
- information objects accessed.

DSS may define audit event criteria to any degree of granularity required, for example, locations

- selectable by general networking location (e.g., by network or subnetwork) or
- selectable by specific information system component.

To accomplish this safeguard specific SW COTS could be required (SIEM).

Time stamps

Time stamps generated by the system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Granularity of time measurements refers to the degree of synchronization between information system clocks and reference clocks, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. DSS may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities.

Protection of Audit Information

Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Protection could be obtained by means of cryptographic mechanisms. Individuals with privileged access to the DSS and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit activities or modifying audit records. To accomplish this safeguard specific SW COTS could be required (SIEM).

Audit Record Generation and Retention

Audit Record Generation and Retention enforces the DSS to generate and retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Table 2-7 specifies the recommended security mechanisms and relates them to the selected safeguards.

Recom.	ID	Name	Description	Security Mechanisms
5	AU-2	Audit Events	Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, and administrative privilege usage. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network.	DSS should determine if is capable of auditing the following events: 1. Authentication events 2. File and Objects events 3. User and Group Management events 4. Use of Privileged/Special Rights events: 5. Admin or root-level access 6. Privilege/Role escalation 7. Audit and log data accesses 8. System reboot, restart and shutdown 9. Information about data that crosses domains (e.g., filename, file size, file type, file metadata) 10. System fault/failure
5	AU-7	Audit Reduction and Report Generation	Audit reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behaviour in audit records. The report generation capability provided by the system can generate customizable reports. Time ordering of audit records can be a significant issue if the granularity of the timestamp in the record is insufficient.	The DSS should provide an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and b. Does not alter the original content or time ordering of audit records. DSS should provide the capability to process audit records for events of interest based on at a minimum, date/time of events; user identifiers; IP addresses involved in the event; type of event; and

				event success/failure. To accomplish this safeguard specific SW COTS could be required (SIEM).
7	AU-8	Time Stamps	Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This control enhancement provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.	The DSS should: a. Use internal system clocks to generate time stamps for audit records; b. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a granularity of time within one second. c. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than one second.
5	AU-9	Protection of Audit Information	This control focuses on technical protection of audit information. Protection could be obtained by means of Cryptographic mechanisms.	The DSS should protect audit information and audit tools from unauthorized access, modification, and deletion. Cryptographic mechanisms could be used for protecting the integrity of audit information: for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash. To accomplish this safeguard specific SW COTS could be required (SIEM)
5	AU-11	Audit Record Retention	System retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes.	DSS should retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
5	AU-13	Monitoring for Information Disclosure	The organization monitors information for evidence of unauthorized disclosure of organizational information.	DSS should use automated scripts to monitor specific information.

Table 2-7 – Audit and Accountability Mechanisms

2.4.2.3 Identification and Authentication Safeguards [IA]

The set of selected Identification and Authentication safeguards includes:

- Identification and authentication for internal and external users
- Device Identification and Authentication
- Authentication management
- Cryptographic Module Authentication

Identification and authentication for internal and external users

Internal users include operators (soldiers with different profiles). DSS should consider to use passwords, tokens, or biometrics to authenticate user identities, or multifactor authentication, or some combination thereof.

Access to the systems is defined as either local access or network access. Local access is any access to the systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks.

Network access is access to the system by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., public network). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between system-controlled endpoints and non-organization-controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network.

For privileged users, it is preferable to enforce a multifactor authentication when access is performed throughout the network. Multifactor solutions could require devices separate from the system gaining access for one of the factors during multifactor authentication which reduces the likelihood of compromising authentication credentials stored on the system. For example, adversaries deploying malicious code on the system can potentially compromise such credentials resident on the system and subsequently impersonate authorized users.

These separated multifactor authentication devices include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards. By these measures it is possible to resist replay attacks making it impractical to achieve successful authentications by replaying previous authentication messages or by recording/replaying previous authentication messages. Replay-resistant techniques include, for example, protocols that use or challenges such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.

External users are not allowed to log into the DSS.

Device Identification and Authentication

Devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device.

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet).

Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Many protocols can be used to comply with this safeguard.

Authenticator Management

Individual authenticators include, for example,

- passwords,
- tokens,
- biometrics,
- PKI certificates, and
- key cards.

Initial authenticator content is the actual content (e.g., the initial password). It is used to allow initial access to the system to then enable the configuration of individual authenticators. The initial authentication methods may not follow rules according to the individual authentications (e.g. password length or complexity).

DSS should support individual authenticator management by defined settings and restrictions for various authenticator characteristics including, for example,

- minimum password length,
- password composition,
- validation time window for time synchronous one-time tokens, and
- number of allowed rejections during the verification stage of biometric authentication.

Device authenticators include, for example, certificates and passwords.

Cryptographic Module Authentication

Authentication mechanisms may be required within a cryptographic module to authenticate an user accessing the module and to verify that the user is authorized to assume the requested role and perform services within that role.

Table 2-8 specifies the recommended security mechanisms and relates them to the selected safeguards.

Recom.	ID	Name	Description	Security Mechanisms
8	IA-2	Identification and Authentication (Internal Users)	This control applies to all accesses to the system.	The DSS should uniquely identify and authenticate internal users (or processes acting on behalf of organizational users) employing passwords, tokens, or biometrics, or multifactor authentication, or some combination thereof. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). In addition to identifying and authenticating users at the information system level (i.e., at logon), DSS could also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. The DSS should implement multifactor authentication for network access to privileged and non-privileged accounts, using biometrical mechanism. It is advisable to use the same mechanism also for local access. DSS should implement replay-resistant authentication mechanisms, by means of using protocol such as Transport Layer Security (TLS) and time synchronous or challenge-response one-time authenticators.
5	IA-3	Device Identification and Authentication	Devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device.	The DSS should uniquely identify and authenticate all devices before establishing a remote or network connection. DSS could use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol

				[TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Within DSS it is necessary to determine the required strength of authentication mechanisms by the security categories of information systems.
5	IA-5	Authenticator Management	Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Device authenticators include, for example, certificates and passwords.	Within DSS it is necessary to: a. Establish initial authenticator content for authenticators; b. Ensure that authenticators have sufficient strength of mechanism for their intended use; c. Change default content of authenticators prior to system installation; c. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators; d. Protect authenticator content from unauthorized disclosure and modification; e. Require individuals to take, and having devices implement, specific security safeguards to protect authenticators. In case of **password-based authentication**, the DSS should: (a) Enforce minimum password complexity; (b) Store and transmits only cryptographically-protected passwords; Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords; (d) Enforce password minimum and maximum lifetime restrictions; (e) Prohibit password reuse generation (does not apply to one

				time use passwords). To mitigate certain brute force attacks against passwords, DSS may also consider salting passwords. In case of **PKI-based authentication**, DSS should: (a) Validate certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforce authorized access to the corresponding private key; (c) Map the authenticated identity to the account of the individual or group; and (d) Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. In case of **Hardware Token-Based Authentication**, DSS should: a) Employ mechanisms that satisfy applicable token quality requirements (for example based on NIST FIPS 201-2 guidance).
5	IA-7	Cryptographic Module Authentication	Authentication mechanisms may be required within a cryptographic module to authenticate a user accessing the module and to verify that the user is authorized to assume the requested role and perform services within that role.	The DSS could implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable standards, and guidance for such authentication.
5	IA-8	Identification and Authentication (External Users)	External users include system users other than internal users explicitly covered by IA-2.	The DSS will not uniquely identify or authenticate external users or processes acting on behalf of these users. No external users are to log into the system. Eventually, authentication into the DSS will only be accomplished through smart cards when that capability is possible with the system component.

Table 2-8 – Identification and Authentication Mechanisms

2.4.2.4 System and Communications Protection Safeguards [SC]

The set of selected System and Communications Protection safeguards includes:

- Application Partitioning
- Security Function Isolation
- Information in Shared Resources
- Denial of Service Protection
- Boundary Protection
- Transmission Confidentiality and Integrity
- Network Disconnect
- Trusted path
- Cryptographic Protection
- Session Authenticity
- Thin nodes
- Heterogeneity

Application Partitioning

Management functionalities for information systems includes, for example,

- functions necessary to administer databases,
- network components,
- workstations, or
- servers,

And typically require privileged user access. The separation of user functionality from information system management functionality can either be physical or logical.

DSS should implement separation of system management-related functionality from user functionality by using

- different central processing units,
- different instances of operating systems,
- different network addresses,
- virtualization techniques, or
- combinations of these or other methods, as appropriate.

Security Function Isolation

DSS should isolate security functions from non-security functions by means of an isolation boundary (implemented via partitions and domains). Such safeguard can be obtained through integrity protection of the hardware, software, and firmware that perform those security functions.

Information In Shared Resources

This control prevents DSS information (including encrypted representations of information) produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to DSS system.

The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

Denial of Service Protection

Denial of service attacks can originate from external or internal sources. DSS resources, sensitive to denial of service, include, for example,

- physical disk storage,
- memory, and
- CPU time.

Common safeguards to prevent denial of service attacks related to storage utilization and capacity include, for example,

- instituting disk quotas,
- configuring information systems to automatically alert users when specific storage capacity thresholds are reached,
- using file compression technologies to maximize available storage space, and
- imposing separate partitions for system and user data.

A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect information system components on internal networks from being directly affected by denial of service attacks.

Also internal users can accomplish this kind of attack. Restricting the ability of those users to launch denial of service attacks requires that the mechanisms used for such attacks are unavailable. Moreover managing excess capacity ensures that sufficient capacity is available to counter flooding attacks (information flooding denial of service attacks).

To accomplish the safeguard, usually specific SW COTS are required (SIEM, IDS, IPS, AV/AM).

Boundary protection

Boundary protection involves for example,

- gateways,
- routers,
- firewalls,
- guards,
- network-based malicious code analysis and virtualization systems, or
- encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

Transmission Confidentiality and Integrity

This control applies to both internal and external networks and all types of DSS components from which information can be transmitted (e.g., mobile devices, SDR). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Cryptographic mechanisms implemented to protect information integrity include, for example,

- cryptographic hash functions which have common application in digital signatures,
- checksums, and
- message authentication codes.

Information can be either unintentionally or maliciously disclosed or modified during preparation for transmission or during reception including, for example,

- during aggregation, at protocol transformation points, and
- during packing/unpacking.

Transmission confidentiality and Integrity addresses also protection against unauthorized disclosure of information through Conceal / Randomize Communications. Encrypting the links and transmitting in continuous, fixed/random patterns prevents the derivation of intelligence from the DSS communications patterns.

Communication patterns include, for example,

- frequency,
- periods,
- amount, and
- predictability.

Changes to communications patterns can reveal information having intelligence value especially when combined with other available information related to mission functions.

Network Disconnect

Network Disconnect applies to both internal and external DSS networks. Terminating network connections associated with communications sessions include, for example,

- de-allocating associated TCP/IP address/port pairs at the operating system level, or
- de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

Trusted paths

Trusted paths are mechanisms by which users (through input devices) can communicate directly with security functions of information systems with the requisite assurance to support information security policies. The mechanisms can be activated only by users or the security functions of systems.

User responses via trusted paths are protected from modifications by or disclosure to untrusted applications. DSS should employ trusted paths for high-assurance connections between security functions and users (e.g., during system logons). Enforcement of trusted communications paths is typically provided via an implementation that meets the reference monitor concept.

Cryptographic Protection

Cryptography can be employed to support a variety of security solutions other than creation of secure channel. For example:

- provision of digital signatures, and
- the enforcement of information separation

When authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals to support random number generation and hash generation.

Session Authenticity

This safeguard addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. For example, this safeguard protects against man-in-the-middle attacks/session hijacking.

Thin nodes

The deployment of DSS components with reduced/minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber-attacks.

Heterogeneity

Increasing the diversity of information technologies within DSS reduces the impact of potential exploitations of specific technologies and also defends against common mode failures, including those failures induced by supply chain attacks. Diversity in information technologies also reduces the likelihood that the means adversaries use to compromise one system component will be equally effective against other system components, thus further increasing the adversary work factor to successfully complete planned cyber-attacks. An increase in diversity may add complexity and management overhead which could ultimately lead to mistakes and unauthorized configurations.

To accomplish this safeguard virtualization techniques could be used.

Table 2-9 specifies the recommended security mechanisms and relates them to the selected safeguards.

Recom.	ID	Name	Description	Security Mechanisms
7	SC-2	Application Partitioning	Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.	The DSS should separate user functionality (including user interface services) from information system management functionality by using: a) different central processing units, b) different instances of operating systems, c)different network addresses, d)virtualization techniques, e) or combinations of these
6	SC-3	Security Function Isolation	Such isolation controls access to and protects the integrity of the hardware, software, and firmware that perform those security functions.	The DSS should isolate security functions from nonsecurity functions by means of: a). code separation b). the use of access control mechanisms and c) by implementing least privilege capabilities.
5	SC-4	Information In Shared Resources	This control prevents information from being available to any current users/roles (or current processes) that obtain access to shared system resources after those resources have been released back to the system. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.	DSS should prevent unauthorized and unintended information transfer via shared system resources.
6	SC-5	Denial of Service Protection	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. System can restrict the ability of individuals to connect and transmit arbitrary information on the transport medium (i.e., network, wireless spectrum). System can also limit the ability of individuals to use excessive information system resources.	DSS must protect against or limits the effects of the following types of denial of service attacks: • network • operating system, • and application layer By employing security safeguards appropriate (such as, but not limited to IDS, IPS and firewalls) for the DSS components and elements. To accomplish the safeguard specific SW COTS are required (SIEM, IDS, IPS, AV/AM)

				DSS should manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks. DSS should: (a) Employ monitoring and audit collection tools to detect indicators of denial of service attacks against the information system; and (b) Monitor system resources to determine if sufficient resources exist to prevent effective denial of service attacks. SIEM is needed to manage properly this aspect.
5	SC-6	Resource priority	System protects the availability of resources by allocating processor and memory resources by: (one or more); priority; quota; process priority, resource availability.	DSS should provide for resource prioritization.
6	SC-7	Boundary Protection	This safeguard includes monitoring and control communications at the external boundary of the DSS.	DSS should: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with a security architecture; c. Establish a traffic flow policy for each managed interface; d. Protect the confidentiality and integrity of the information being transmitted across each interface.
5	SC-8	Transmission Confidentiality and Integrity	Protecting the confidentiality and/or integrity of the information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). This safeguard enhancement addresses protection against	The DSS must protect the confidentiality and integrity of transmitted information employing encryption techniques The DSS should maintain the confidentiality and integrity of information during preparation for transmission and during reception. The DSS should implements cryptographic mechanisms to

			unauthorized disclosure of information through Conceal / Randomize Communications.	conceal or randomize communication patterns unless otherwise protected by alternative physical safeguards.
5	SC-9	Transmission Confidentiality	See SC-8	-
5	SC-10	Network Disconnect	Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.	DSS should terminate the network connection associated with a communications session at the end of the session with the exception of tactical systems which should not have this control.
6	SC-11	Trusted Path	System establishes a trusted communications path between the user and the security functions of the system: security functions to include at a minimum, information system authentication and re-authentication.	DSS should provide a trusted communications path that is logically isolated and distinguishable from other paths.
5	SC-13	Cryptographic Protection	Cryptography can be employed to support a variety of security solutions.	DSS should implement all uses and types of cryptography required for each use (e.g., National Security Agency - approved cryptography for protection of classified information; FIPS-validated cryptography for provision of digital signatures and hashing) in accordance with applicable directives, policies, regulations, and standards.
6	SC-14	Public Access Protection	Capability provided by AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10	
6	SC-16	Transmission of security attributes	Security attributes can be explicitly or implicitly associated with the information contained in organizational information systems or system components.	DSS should associate with information exchanged between information systems and between system components.

5	SC-23	Session Authenticity	Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.	DSS should protect the authenticity of communications sessions. DSS only allows the use of authorized certificate authorities for verification of the establishment of protected sessions. Reliance on certificate authorities (CAs) for the establishment of secure sessions includes, for example, the use of Secure Socket Layer (SSL) and/or Transport Layer Security (TLS) certificates.
6	SC-25	Thin nodes	Thin nodes reduce the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to cyber-attacks.	DSS should employ components with minimal functionality and information storage.
5	SC-29	Heterogeneity	Changes can result in an increased work factor for adversaries in order to carry out successful cyber-attacks. Changing virtual operating systems or applications, as opposed to changing actual operating systems/applications, provide virtual changes that impede attacker success while reducing configuration management efforts. In addition, virtualization techniques can assist organizations in isolating untrustworthy software and/or software of dubious provenance into confined execution environments.	The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications.
5	SC-33	Transmission preparation Integrity	See SC-8	

Table 2-9 – System and Communications Protection Mechanisms

3 Integrated Dictionary

3.1 Abbreviations and Acronyms

AC	Alternating Current
AM	Amplitude Modulation
AU	Audit mechanisms
AV	Anti Virus
BMS	Battery Management System
CNR	Combat Net Radios
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CROP	Common Reference Operational Picture
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DAC	Discretionary Access Control
DDS	Data Distribution Services
DEU	Deutschland (Germany)
DNV GL	Det Norske Veritas Germanischer Lloyd (NLD)
DSS	Dismounted Soldier System
DT	Data Transmission
EAP	Extensible Authentication Protocol
EDA	European Defence Agency
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Spain
ET	Ejercito de Tierra
EU	European Union
FIPS	Federal Information Processing Standards Publication 197
GMT	Greenwich Mean Time
GNSS	Global Navigation Satellite System
GOSSRA	Generic Open Soldier System Reference Architecture
HRI	Human RAS Integration
IA	Authentication mechanisms
ID	Identification
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
ISACA	Information Systems Audit and Control Association
IT	Information Technology
ITA	Italy
LCG-DSS	Land Capability Group – Dismounted Soldier Systems
MAC	Medium Access Control

MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MDE	Ministerio de Defensa de España
MIL	Militar
NATO	North Atlantic Treaty Organization
NAV	NATO All View
NBC	Nuclear Biological Chemical
NCV	NATO Capability View
NEC	Network Enabled Capability
NIST	National Institute of Standards and Technologies
NLD	Netherlands
NOV	NATO Operational View
NSOV	NATO Service Oriented View
NSV	NATO System View
NTV	NATO Technical View
PADR	Preparatory Action on Defence Research
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POL	Poland
PRT	Portugal
PU	Public
Pwr	Power
RAS	Robotic & Autonomous System
RF	Radio frequency
RTD	Real Time Data
RTO	Recovery Time Objective
SA	Situational Awareness
SC	Secure Communications
SDR	Software Defined Radio
SI	Individual Source (FELIN DSS)
SIEM	Security Information Event Management
SRA	Security Risk Assessment
SSL	Secure Socket Layer
STU	Small Tactical Unit
SW	Software
SWE	Sweden
TCP	Transmission Connection Protocol
TLS	Transport Layer Security
TSV	Threat Standard Value
UHF	Ultra-High Frequency
USB	Universal Serial Bus
UTC	Coordinated Universal Time
VH	Very High
VHF	Very High Frequency
VL	Very Low

WPC	Wireless Power Consortium
WPC	Wearable Portable Computer
XML	Extensible Marcup Language

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/ 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.

/10/ NIST SP 800-53 Rev.4 January 2015 - Security and Privacy Controls for Federal Information Systems and Organizations

/11/ EAR / PILAR: https://www.ar-tools.com/en/index.html