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. 6

Technical View (NTV)

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/.

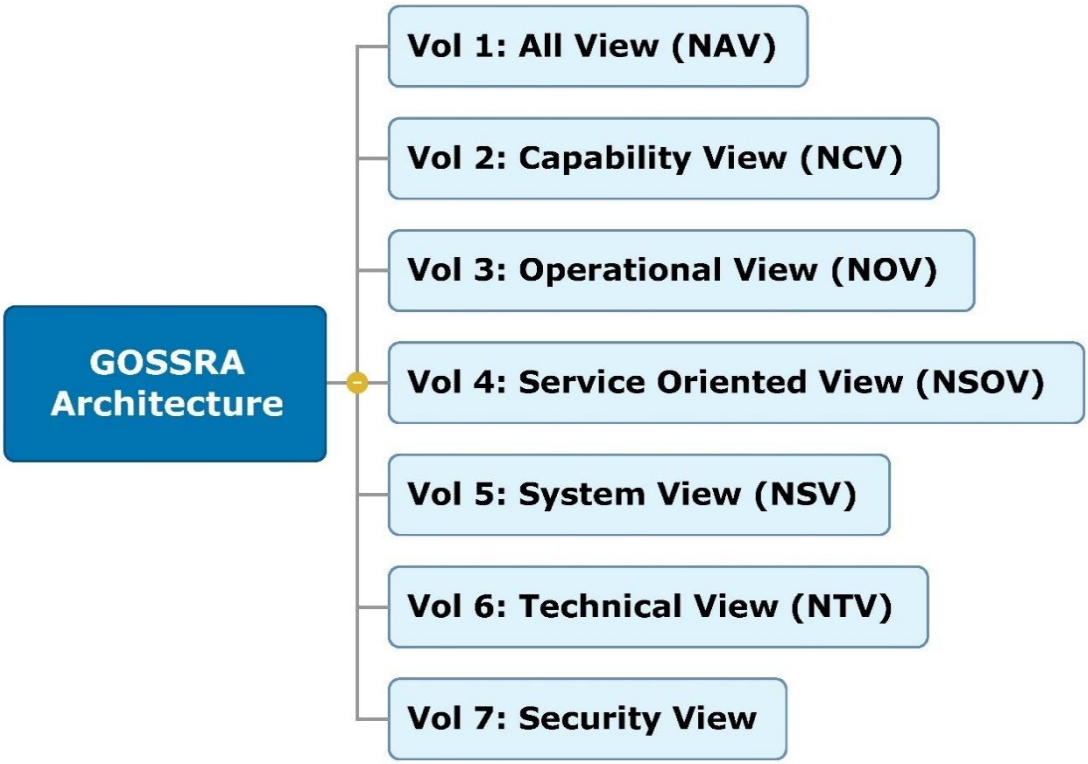

Figure 1-1 – GOSSRA Document Structure

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 Technical View

2.1 Introduction

The Technical View lists the standards which are recommended to be used for the whole life cycle of a Soldier System. Especially the System View refers to the listed standards in this volume and defines where the standards are applied to covering specifically the data management and electronics infrastructure components of soldier systems.

Additionally, there are standards listed which apply to Soldier Systems in general, such as NATO Glossary of Terms, NATO Architecture Framework, CE Marking, etc.

The Volume is organised into three sections

- NTV-1 Technical Standards Profiles
- NTV-2 Technical Standards Forecast

The Technical Standards Profiles relate to

- Generally Applicable Standards
- Safety Related Standards
- Testing Related Standards
- Smart Battery Related Standards
- Power Quality Related Standards
- Energy / Power Management Related Standards
- Product Conformity Related Standards
- Laws and Regulations
- Standard Descriptions according to the System view

Forecast for the standards are given for the domains

- Electronics Technical Standards Forecast
- Software Technical Standards Forecast
- Radio Communication Technical Standards Forecast
- Human Interface Devices Standards Forecast
- Sensors Technical Standards Forecast

2.2 NTV-1 Technical Standards Profiles

The Technical Standards Profile (NTV-1) provides a list of **recommended standards,** which guides and constrains the implementation of GOSSRA system as defined in the various sub-views and requirements of the NATO System View /5/.

The NTV-1 standards are preferably NATO standards as the GOSSRA Architecture aims at being standardized by NATO which is the most important international standardisation body in the military domain.

2.2.1 Generally Applicable Standards

The following sections will show the generally applicable standards from the categories:

- General NATO,
- Safety Related,
- Testing Related,
- Power Related,
- Product Conformity,
- Laws and Regulations.

The set of standards is just informative, hence they are not described further. **The set of standards is not complete**. Additionally standards may be replaced by other standards that are more applicable to the target architecture.

2.2.1.1 General NATO Standards

Table 2-1 lists NATO Standards which are generally applicable to all areas of the soldier system domain.

Subcategories	Std Type	Std #	Part	Ed	Title
Applicable Standards	STANAG	5524			Catalogues Consultation, Command and Control (C3) standards usable in NATO
Glossary and Definitions	AAP	6		2008	NATO Glossary of Terms and Definitions
	AAP	15		2008	NATO Glossary of Abbreviations used in NATO Documents and Publications
	AAP	42		2007	NATO Glossary of Standardization Terms and Definitions

Table 2-1 – General Standards

2.2.1.2 Safety Related Standards

Table 2-2 lists common safety standards which apply to soldier system and which are recommended to be considered when a target architecture is derived.

Subcategories	Std Type	Std #	Part	Ed	Title
Health and Safety	OHSAS	18001			The Health and Safety & OHSAS Guide
Power Sources	IEC	62282	6-101	2015	Micro fuel cell power systems - Safety - General requirements
	IEC	62133		2012	Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for portable sealed secondary cells, and for batteries made from them, for use in portable applications
	IEC	62281		2.0	Safety of primary and secondary lithium cells and batteries during transport
	IEC	62902		1.0	Secondary batteries: Marking symbols for identification of their chemistry
	UN		38.3		Recommendations on the Transport of Dangerous Goods
	IEC	62485	1	1.0	Safety requirements for secondary batteries and battery installations - Part 1: General safety information
Electro-Magnetic Fields	IEEE	C95.1		2005	Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
Functional Safety	IEC	61508		2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
	MIL-STD	882E		2012	System Safety

Table 2-2 – Safety Related Standards

2.2.1.3 Testing Related Standards

Table 2-3 lists standards which apply to the testing of soldier systems and also peripheral equipment.

Subcategories	Std Type	Std #	Part	Ed	Title
Life Requirements	NATO AECTP	600		2	The Ten Step Method for Evaluating the Ability of Material to Meet Extended Life Requirements and Role and Deployment Changes
Environment	NATO STANAG	4370		5	Environmental Testing
	NATO AECTP	100		4	Environmental Guidelines for Defence Materials
	NATO AECTP	200		4	Environmental Conditions
	NATO AECTP	230		1	Climatic Conditions
	NATO AECTP	240		1	Mechanical Conditions
	NATO AECTP	300		3	Climatic Environmental Tests
	NATO AECTP	400		3	Mechanical Environmental Tests
	US DoD MIL-STD	810		g	Department of Defence Test Method Standard: Environmental Engineering Considerations and Laboratory Tests
EMC	NATO AECTP	250		C Version 1	Electrical and Electromagnetic Environmental Conditions

	NATO AECTP	500		4	Electromagnetic Environmental Effects Tests and Verification
	US DoD MIL-STD	461		g	Military Standard: Electromagnetic Interference Characteristics Requirements for Equipment

Table 2-3 – Test Standards

2.2.1.4 Power Related Standards

As soldier systems use electrical energy power standards are quite important. In this section power related standards are listed and categorized in:

- Power Sources
- Batteries
- System Management
- Energy / Power Management related
- Military Vehicle 28 VD
- Information and Communication Technology Related

Subcategories	Std Type	Std #	Part	Ed	Title
Power Sources	Def-Stan / VG	61-23 / 97010	/-01	2011	Generic Fuel Cell / Brennstoffzellen (Allgemein)
	Def-Stan / VG	61-23 / 97010	Sup 01 / -02	2011	Methanol Fuel Cell System / Methanol-Brennstoffzelle
	Def-Stan	61-17		5	The Selection and Introduction of Batteries and Fuel Cells for Service Use
	Def-Stan	61-21	Sup. 100	1	Alkaline Manganese Dioxide Battery 4.5V NSN 6135-99-260-9158
	Def-Stan	61-21	Sup 101	1	Specification for Alkaline Manganese Battery 1.5V NSN 6135-99-792-8475
	Def-Stan	61-21	Sup 103	1	Lithium Manganese Dioxide Battery 6V, 1.4 Ah (Nominal) NSN 6135-99-395-9403
	Def-Stan	61-21	Sup 104	1	Alkaline Manganese Dioxide Battery 4.5V NSN 6135-99-738-4038

	Def-Stan	61-21	Sup 06	2	Specification for LR14 Type Alkaline Manganese Dioxide Battery (for high drain-rate applications) 1.5V, NSN 6135-99-605-6658
	Def-Stan	61-21	Sup 75	2	Lithium-Ion Power Systems (LIPS)
	UL	1642		2012	Standard for Lithium Batteries
	UL	2054		2004	Standard for Household and Commercial Batteries
	UL	2271		2013	Batteries for Use In Light Electric Vehicle (LEV) Applications
	DIN EN	61960		2012	Secondary cells and batteries containing alkaline or other non-acid electrolytes - Secondary lithium cells and batteries for portable applications (IEC 61960:2011); German version EN 61960:2011
	IEC	62282	6-200	3	Micro fuel cell power systems - Performance test methods
	IEC	62282	6-400	PWI	Micro fuel cell power systems - Power and data interchangeability

	SBS-IF	SBS 1.1	Test	2.0	Smart Battery Data Accuracy Testing Guidelines
Batteries	SBS-IF	SBS 1.1	Charger	1.1	Smart Battery Charger Specification
	SBS-IF	SBS 1.1	Data	1.1	Smart Battery Data Specification
	SBS-IF	SBS 1.1	Data Add	1.02	SBDS – Addendum For Fuel Cell Systems
	SBS-IF	SBS 1.1	Batt Sel	1.1	Smart Battery Selector Specification
	SBS-IF	SBS 1.1	Batt Man	1.0	Smart Battery System Manager Specification
System Management				2, 2000	System Management Bus (SMBus) Specification Version 2.0
Military Vehicle 28 VD	US DoD MIL-STD	1275		e	Department of Defense Interface Standard: Characteristics of 28 Volt DC Electrical Systems in Military Vehicles
	US DoD MIL-STD	704		f	Department of Defense Interface Standard: Aircraft Electric Power Characteristics
Information and Communication	Industrial USB		7.2	2.0	USB Serial Bus Specification,

Technology Related	Implementer Forum				Electrical Power Distribution
	Industrial USB Implementer Forum		LPM-ECN	2.0	USB 2.0 Link Power Management Addendum [/54/]
					USB 3.1 Power Management [/53/]
	Industrial open	ACPI		5.0a	Advanced Configuration and Power Interface Specification

Table 2-4 – Power Sources Standards

2.2.1.5 Product Conformity Related Standards

Table 2-5 lists product conformity standards as guidance to be considered.

Subcategories	Std Type	Std #	Part	Ed	Title
Product Conformity	ISO / IEC	17050	1	2004	Conformity Assessment – Supplier's declaration of conformity, General Requirements
	ISO / IEC	17050	2	2004	Conformity Assessment – Supplier's declaration of conformity, Supporting Documentation

Table 2-5 – Product Conformity Related Standards

2.2.1.6 Laws and Regulations

Table 2-6 lists common laws and regulations are described that should be considered for the Soldier System life cycle.

Subcategories	Std Type	Nation	Date	Title	Description
Laws and Regulations		EU	2008	CE Marking	Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93
		EU	05-04-2016	Blue Guide	Blue guide on the implementation of EU product rules 2016
		EU	2006	Directive	Directive 2006/66/EC of the European parliament and of the council of 6 September 2006 on batteries and accumulators and waste batteries and accumulators and repealing Directive 91/157/EEC

Table 2-6 – Laws and Regulations

2.2.2 Standards Related to System View (NSV) Sections

Table 2-7 shows the standards addressed in or related to the System View. Due to the direct applicability to the system view these standards are described further. The exact usage of the standard and possible sub-standards is shown in the System View (see /5/). Were it was found to be useful, a rationale was integrated into the standards description.

Service Area	Service	Standard
Physical Interfaces	Wired	Micro 38999 [/52/]
		USB 3.1 2nd Gen [/53/]
		USB 2.0 (as a Fallback) [/54/]
	Wireless	Bluetooth > 4.2 [/55/]
		NFC [/56/][/57/]
Media	Video	H.264 [/58/]
		H.265 [/59/]

Service Area	Service	Standard
		MP4 [/60/]
		Matroska [/61/]
	Audio/Voice	FLAC [/62/]
		MPEG-2 [/63/]
		G.711 [/64/]
	Imaging	JPEG/JFIF [/65/]/105/]
		PNG [/66/]
		TIFF [/67/]
Data Exchange Service	Data Delivery: Data Distribution Services	DCPS [/20/] RTPS [/21/] X-Type [/22/] IDL [/23/]
	Data Delivery: Message Queue Telemetry Transport	MQTT[/70/] MQTT-SN[/70/]
	Streaming	RTP [/24/] H.323 [/28/] RTSP [/29/] SIP [/30/] SDP [/71/]
	Tactical Data Delivery: Variable Message Format	VMF[/25/]
	Tactical Data Delivery: Joint Dismounted Soldier System Interoperability Network	Security [/14/] Data Model [/15/] Loaned Radio[/16/] IEM [/17/]

Service Area	Service	Standard
		Network Access [/18/]
Application	Architecture	NGVA Vol.1 [/9/]
	Power Infrastructure	NGVA Vol.2 [/10/]
	Data Infrastructure	NGVA Vol.3 [/11/]
	Data Model	MDA[/26/] UML[/27/] NGVA Vol.5 [/19/]
Transport Service	Transport Protocols	TCP [/32/] UDP[/33/]
	Routing Protocols	IP [/34/] OLSR [/35/] DLEP[/36/] IPv6 [/37/]
Audio Exchange	Wired	Analog 4W
		USB Audio
		USB Eth. VoIP G.711/G.726 [/64/]
	Wireless	Bluetooth > 4.2 [/55/]
Remote Controls	Wired	USB [/53/] [/54/]
		Custom analogue
	Wireless	Bluetooth > 4.2 [/55/]
Line-on-Sight Communications	Voice & Data Comms	STANAG 4204 / 4205
		STANAG 4246 (HQ I/II)
		STANAG 4372 (SATURN ed.4)
		STANAG 5630 Series (NATO NB ed.1)

Service Area	Service	Standard
Beyond Line-Of-Sight Communications	HF Home	STANAG 4285
		STANAG 4539
		MIL-STD-188-141C
		STANAG 4538
		STANAG 5066
	SATCOM Dedicated Ch./ DAMA	MIL-STD-188-181A
		MIL-STD-188-182A
		MIL-STD-188-183
C4I	General	ADatP-34 (NISP)
	Soldier System Interoperability	STANAG-4677 (AEP-76)
	Tactical Command Post	MIP
		VMF
	Friendly Force Tracking	ADatP-36
		ADatP-37

Table 2-7 – NTV-1 Electronics Technical Standards Profile

2.2.2.1 Physical Interfaces

2.2.2.1.1 USB

USB started approx. 20 years ago as a joint, civil industrial effort by the USB Implementers Forum (USB-IF) to define a uniform connector to plug devices into computers. USB versions below v2.0 had a poor throughput, can be regarded as fully obsolete. Even from backward compatibility point of view these versions are also for DSS of no interest and will therefore not be discussed here.

USB 2.0

USB-IF ratified version 2.0 at the end of 2001. It added a higher maximum signalling rate of 480 Mbit/s (High Speed or High Bandwidth), in addition to the USB 1.x Full Speed signalling rate of 12 Mbit/s. However, due to bus access constraints, the effective throughput of the High Speed signalling rate is limited to only 280 Mbit/s. USB 2.0 sends data in semi-duplex (only one direction at a time).

A pro of v2.0 is that the cable length supported is 5 m. It is doubtful, however, if this length is relevant for a DSS. More relevance of v2.0 in DSS is for reasons of compatibility with legacy devices such as sensors, if necessary. In general, the usability of USB 2.0 in DSS will be restricted to non-time critical or static data low bandwidth exchange (e.g. including system initiation, status and configuration). USB 2.0 architecture features a shared bus, with a polling interval of 0.125 ms.

Release name	Release date	Maximum transfer rate	Note
USB 1.0	January 1996	Low Speed (1.5 Mbit/s)	
USB 1.1	August 1998	Full Speed (12 Mbit/s)	
USB 2.0	April 2000	High Speed (480 Mbit/s)	
USB 3.0	November 2008	SuperSpeed (5 Gbit/s)	Also referred to as USB 3.1 Gen 1 by USB 3.1 standard
USB 3.1	July 2013	SuperSpeed+ (10 Gbit/s)	Also referred to as USB 3.1 Gen 2 by USB 3.1 standard

Table 2-8 – USB Versions

USB 3.1

USB (Universal Serial Bus) 3.1 Gen. 2 is a standard for full-duplex cable-based interfacing computers and electronic devices, based on version 3.1, Gen 1. It features a high transfer rate (near the theoretical maximum) that can transfer data at a rate up to 10 Gbit/s and therefore it is also referred to as SuperSpeed USB 10 Gbps whereas Gen. 1 featured a rate of 5 Gbit/s.

Its structure is dual-bus, allowing simultaneous operation of different USB versions. The physical architecture is a tiered star topology with a root hub and hubs at lower levels to provide bus connectivity to devices. Reported average latencies for the several transfer modes (q.v.) are between approx. 30 and 50 µs.

The use of unicast and the limited amount of multicast packets, combined with asynchronous notifications enables links that are not actively passing packets to be put into reduced power states, allowing for improved power management. The maximum practical cable length supported is 3 m, at a maximum of 10 Watts (assumed non-high power delivery). Note this is substantially lower than the cable length supported by USB 2.0.

Intel's Thunderbolt interface competes with USB 3.1 Gen. 2. For use within DSS systems, the improved capabilities seem attractive. However, this might come with some disadvantages such as more pins (larger connectors), increased power usage and possibly worse EMC characteristics. This needs to be investigated further.

USB-C

USB C (formally known as Type-C) is a 24-pin plug connector system for the simultaneous transport of data and energy. This last feature is based on the USB-PD (Power Delivery) standard. Note that USB-C is just a connector shape which means that the underlying technology is not necessarily USB 3.1 but could just be USB 2 or USB 3.0. It should hence be noted that a device that implements USB-C does not necessarily support USB 3.1, USB-PD or Alternate Mode. On the other hand, USB-C fully utilizes USB-PD, allowing for configuration of any arbitrary device as a power source and/or a power sink and flexible negotiation of voltages and maximum currents in case the power exceeds 15 W. Therefore, USB-C is closely tied to PD.

While USB-C connectors are not backwards compatible, the standards indicate that USB-C adapters can be used with older devices. Backward interoperability is simply achieved by a physical adapter with a USB-C connector on one end and a larger, 'older-style' USB port on the other end.

The USB-C connector is fully reversible which makes it much easier to plug in. This is a considerable pre for a DSS implementation where the user's attention should not be on the way a cable should be plugged in. Particularly in stressful conditions this feature is relevant.
Evidently, the integrated data and energy transport and its smaller size are advantageous for a DSS as well. The small size allow for connection to all kinds of devices and peripherals, e.g. from smartphones to external hard disks. The question from DSS-perspective however, is whether the physical structure is resilient enough for military use.

Figure 2-1 – USB-C Connector

The USB Type-C 1.0 specification was finalized and published by the USB Implementers Forum (USB-IF) in August 2014 and became a common feature in devices in the course of 2015. USB-C was developed at roughly the same time as the USB 3.1 specification.

USB-C cables can carry significantly more power than version 3.1 (applying PD revision 2.0): i.e. 100 W, which allows charging larger devices such as laptops. However, it should be checked if a USB-C device actually supports PD. USB-C is designed to feature the maximum USB v3.1 Gen. 2 transfer speed of 10 Gbit/s.

In general the following aspects should be considered when applying whatever USB version in DSS:

- If streaming sensor data (audio, video or tactile) is required, data should be transported with a latency below the perception threshold. This implies a protocol with small data packets;
- The system must be capable of resuming interrupted stream connectivity. In this respect, USB is not optimal.

Transfer modes and frame sizes

IN-transfers send data to the PC. When the host initiates an IN-transfer the device has to respond with data for the host. OUT-transfers send data to the device. When the host performs an OUT-transfer it sends a packet of data that the device must capture. There are four types of IN and OUT-transfers in USB:

- **A bulk transfer** is used to reliably transfer data between host and device, using a CRC. If the CRC is correct the transfer is acknowledged, and the data is assumed to have been transferred error-free. If the CRC is not correct, the transfer will be retried. If the device is not ready to accept data it can send a negative-acknowledgment, NAK, which will cause the host to retry the transfer. Bulk transfers are not considered time critical, and are scheduled around the time critical transfers discussed below.
- **Isochronous transfers** are used to transfer data in real-time between host and device. When an isochronous endpoint is set up by the host, the host allocates a fixed bandwidth to the isochronous endpoint. Since a fixed and limited amount of bandwidth has been allocated, there is no time to resend data if anything goes wrong. The data has a CRC as normal, but if the receiving side detects an error there is no resend mechanism.
- **Interrupt transfers** are used by the host to regularly poll (but not ad-hoc interrupt, confusingly) the device to find out whether something worthwhile has happened, e.g. to check whether the MUTE button of an audio device has been pressed. Note that the regular polling of data gives the same sort of functionality that a host-interrupt would provide.
- **Control transfers** are very much like bulk transfers. Control transfers are either positive or negative acknowledged and are delivered in a non-real-time fashion. Control transfers are used for operations that are outside the normal data flow, such as querying the device capabilities, or endpoint status. Predefined classes such as 'USB Audio Class' or 'USB Mass Storage Class' are defined to enable cross platform interoperability.

All transfers are made in USB frames. High Speed and SuperSpeed(+) USB (i.e. USB 2.0 and 3.0/3.1, respectively) frames span 125 µs; Full Speed USB frames (USB 1.1) span 1 ms. Isochronous and Interrupt transfers are transmitted at most once a frame.

2.2.2.1.1.1 Rationale for USB

The data bus of the personal domain is the most critical and central component in the soldier system. It is not only the question of performance. For example the power consumption and the possibility of disturbance of the system is also critical.

For the personal domain two data busses were considered.

- USB Version >= 2.0
- Gigabit Ethernet

The choice to narrow down possible bus systems was driven by the following aspects

- Number of pins/lanes
- Power consumption
- Data rates

- Number of standard devices for DSS

USB 3.1 Gen.2 looks an ideal candidate for transporting information. Supports:

- high BW in the range of GBs;
- plug&play device management;
- easy USB to Ethernet conversion to access the Radio bus.

Another appealing service is Power Delivery (PD), which includes:

- Increased power levels up to 100W (via profile management)
- Power direction no longer fixed (especially useful for the Radio)
- Optimized power management allowing each device to take only the power it requires.

In the first place USB looked like the most promising standard to be chosen. In the decision process the following objections were made and answered.

Objections:

1. USB in general is much easier to disturb in EW than Ethernet
2. USB 3.1 2nd Gen. has a much higher frequency than Ethernet and USB 2.0 and may be detected easier.
3. The speeds provided by USB 3.1 2nd Gen are not needed in the System

Comment on Objection 1: Yes, due to the smaller potential difference on the USB data lines it is easier affected by EW-Measures. An attacker may need approximately three times the power to disturb Ethernet that he would need for USB. The number is a first guess based on the potential lift and the frequency considering no shielded cable. All high performance bus systems can be jammed. Thus, Ethernet as well as USB require a proper electronic shielding in the whole system to handle this issue.

Comment on Objection 2: All high performance serial bus systems need high frequencies to transfer data. Another solution would be parallel busses with a certain number of lanes. This would increase the cabling issue since e.g. 16+ lanes would be needed. Hence, all affordable bus systems will have this issue and will be subject to detection issues. As already mentioned it is necessary to have a proper shielding in the whole system to handle this issue.

Comment on Objection 3: Use cases are currently rare, but TNO provided good evidence that the Bandwidth as well as the low latency will be used e.g. for 3D-Hearing for the soldier (low latency) or a panoramic view for the soldier improving his current visual senses.

Considering the comment on objection 3 it was possible to decline USB 2.0 as the main bus. Both standards USB and Ethernet are capable of transferring power, but for Ethernet transferring power results in a reduction of bandwidth.

Hence, it was decided to use USB 3.1 2nd Generation with USB 2.0 as a fall back option.

This may influence the pinning of the data connector since it could be a USB-C convertible pinning.

Considering wireless technologies, the evaluation of current sensors has shown that Bluetooth is the dominating interface on the market for sensors. Considering the evolvement of Bluetooth in the past years shows, that it is a future proof standard. These evolvements also introduced import technical improvements, which are mostly also important for the DSS domain as e.g. Low-Power implementations and transmit power adjustments, latter decreases the probability of detection of the radio signal. Additionally it is fielded in the several current soldier systems and thus has been proven to be a valid and important standard.

2.2.2.1.1.2 Modularity & Integration Technical Standards Profiles

The technical architecture based on standard physical wired and wireless buses, permits integrating future modules and devices using a consistent interconnect configuration.

Adopting commercially available standards paves the way to using standard COTS/MOTS devices as the Computing Platform (CP), which encompasses several advantages. For instance:

- their development and update is mostly paid by the market;
- they are available before the requirement specifications are prepared;
- they have a larger user base, so they are cheaper and more tested.

On the other hand (see also /39/) they often:

- need adapters to comply with military grade connection requirements;
- become obsolete at a faster pace than procurement is able to sustain;
- lack the ability to include custom functions;

Especially as regards the wired bus, in /40/ it is stated that the US Nett Warrior (NW) program plans to acquire in excess of 50,000 cables, based on current production and fielding projections. Cables of the NW are of just two types: Power and Personal Area Network (PAN).

The economics of a single type of cable/connector set, dual use for power and/or data, interchangeability, and daisy chaining capability for extended length will result in significant cost avoidance (see /40/).

As stated above, the possibility to have standard cables, connectors, and wirings must be carefully considered.

2.2.2.1.2 Micro 38999

The Micro 38999 connector is a miniaturized version of the well-known MIL-DTL-38999 which was used by the Generic Vehicle Architecture as well as the NATO Generic Vehicle Architecture. The connector is currently non-standardized, but provided by different Vendors in an interoperable configuration. In the current state of play it is in the standardization process.

Rationale

The connector was chosen, due to the fact, that no other dual-sourced connectors for USB 3.1 2nd Generation were available on the market.

2.2.2.1.3 Wireless Interfaces

2.2.2.1.3.1 Bluetooth

The Bluetooth protocol is standardized by the Bluetooth Special Interest Group (SIG) and describes all the layers of the OSI stack. The latest version of the standard dates from 2016 (Bluetooth v5.0). Nowadays, Bluetooth is mainly used for point-to-point connections with wireless headsets, hands-free systems, computer accessories (replacement of wired serial data transfer), wireless speakers and smart watches. Theoretically, Bluetooth allows for the realization of limited mesh networks. However, these so-called piconet and scatternet functionality is virtually never used.

Bluetooth uses the very busy 2.4 GHz ISM band and is hence susceptible to noise. The protocol is therefore based on frequency hopping, which means that the two communicating nodes alter their

radio frequency (i.e. 2.4 GHz sub-band) very fast. This implies that very regularly a noise-free frequency is encountered. This makes Bluetooth connections very robust, but also relatively slow: sub-bands are quite narrow (1 MHz) and the system clocks of both devices must be carefully synchronized. Consequently, Bluetooth typically does provide throughputs more than a few Mbit/s. That is more than enough for sound but not for video or the transport of large data volumes.

The range of Bluetooth links depends on e.g. the power class of the Bluetooth chip. Most mobile consumer devices (phones, headset, etc.) use class 2, which emits up to 2.5 mW and has an indoor range of 5 to 10 meters. Class 1 equipment (100 mW) ranges over 20 meters and is sometimes used in industrial applications.

The first two relevant versions of Bluetooth, v1.1 and v1.2, standardized the lower communication layers as IEEE 802.15.1. SIG did however not recognize the added value of this standard and discontinued its maintenance.

Bluetooth has the important property that already in 1999 it was being developed for energy efficient use by devices using a battery. This makes Bluetooth ideally suited for Internet-of-Things applications. Since the requirements for energy efficiency have become more stringent than in 1999 the Bluetooth SIG developed the Bluetooth Low Energy (BLE) profile, as part of the Bluetooth v4.1 and v4.2 standards. However, this is not a compulsory part. Moreover, it is also a completely different protocol than the original Bluetooth. Both protocols are not mutually interoperable, implying careful installation of the proper Bluetooth profiles during communication systems development. Differences between the classic Bluetooth and Bluetooth BLE are illustrated in the Figure. Interestingly, the radio power consumption of BLE is not substantially lower than the classic Bluetooth. This makes the attainable ranges comparable. BLE handles data traffic more efficient than the original Bluetooth version.

	Bluetooth V2.1	Bluetooth Low Energy
Standardization Body	Bluetooth SIG	Bluetooth SIG
Range	~30 m (class 2)	~50 m
Frequency	2.4-2.5 GHz	2.4-2.5 GHz
Bit Rate	1-3 Mbit/s	~200 kbit/s
Set-Up Time	<6 s	<0.003 s
Voice Capable?	Yes	No
Max Output Power	+20 dBm	+10 dBm
Modulation Scheme	GFSK	GFSK
Modulation Index	0.35	0.5
Number of Channels	79	40
Channel Bandwidth	1 MHz	2 MHz

Figure 2-2 – Bluetooth v2.1 protocol compared with BLE

In general it can be said that lack of interoperability Bluetooth was always a handicap. Evidently, this complicates its use in DSS as well. In some cases the cause was at lack of proper implementation of the standard in chips. However, in most cases it was caused by the coexistence of multiple versions of the standard and/or implementation of different profiles of the standard. Only devices that have a lot of processing power for generic applications (e.g. computers, some phones) support all Bluetooth profiles. Small "embedded devices" only support the profiles for their specific application. At present, 35 different profiles are defined.

Also usability has long been a problem for the adoption of Bluetooth in the market. In particular, safely linking two devices (‘pairing‘) has long been a difficult and lengthy process. Later versions of Bluetooth have gradually improved on this point.

The latest version, v5.0, features a transmission capacity of 384 Mbit/s at 3-fold range of the latest version, v4.2: i.e. 300 m. This would imply that Bluetooth starts competing other type of protocols, medium range, like WiFi. Together with the low energy consumption feature (continued from v4.1 and v4.2), the security/privacy feature and the fast set-up time, this new version shows promising for use in DSS. It does however, not feature backward interoperability with any previous Bluetooth version.

2.2.2.1.3.2 Near Field Communication

“Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1½ in) of each other.

NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards and allow mobile payment to replace or supplement these systems. This is sometimes referred to as NFC/CTLS (contactless) or CTLS NFC. NFC is used for social networking, for sharing contacts, photos, videos or files. NFC-enabled devices can act as electronic identity documents and keycards. NFC offers a low-speed connection with simple setup that can be used to bootstrap more capable wireless connections.”[1]

2.2.2.1.3.3 Rationale for wireless standards

The following Wireless communication standards were considered WiFi, Bluetooth, NFC and ZigBee for the personal domain as possible PAN-Networks. From a technical point of view all of the standards are capable of handling DSS use cases, hence the comparison was made not with a technical focus.

One very important factor was the **COTS-/MOTS-Availability of Equipment**. Hence, this influences the usage as well as the distribution of the standard. In case no equipment is available on the market the standard may not be used or usage may be delayed. Additionally gateways will be introduced to adapt legacy equipment leading to higher power consumption. An analysis of the currently available equipment showed that Bluetooth is already common in the MOTS-Domain, while WiFi is barely and ZigBee as well as NFC are currently not supported. Considering DSS equipment in the COTS-Domain it is nearly the same as for the MOTS domain, but NFC-Devices are more common.

[1] https://en.wikipedia.org/w/index.php?title=Near-field_communication&oldid=925463296

All standards considered in the DSS Personal Domain as PAN-Networks need to be **applicable to battery driven devices**, as all devices on the DSS are usually battery driven. Hence, extensive use of energy is not acceptable in this domain. Comparing ZigBee, WiFi and Bluetooth in terms of power consumption /69/ has shown that Bluetooth is the most power saving standard. NFC is usually used in handheld devices and, due to the extremely short range, it has a low power consumption. /114/ has shown that Bluetooth is the most power saving standard. NFC is usually used in handheld devices and, due to the extremely short range, it has a low power consumption.

The tactical acceptance of the standards is important, since selecting an untrusted standard may reduce the acceptance by the user and lead to parallel implementations of other standards to serve the wireless communication. Bluetooth and WiFi are currently already used in different Soldier Systems as well as their peripherals, while NFC and ZigBee are not used so far. In Addition of Bluetooth was recommended on the Second Stakeholder Workshop by the German MoD and was widely supported. Especially new versions of Bluetooth supporting adaptive transmission power level drive the trust in this civil standard. Considering the small range for NFC-Communication it is marked as neutral for the tactical acceptance.

Categories	WiFi	Bluetooth >= 4.2	NFC	ZigBee
Availability of MOTS- Equipment	**o**	**+**	**-**	**-**
Availability of COTS- Equipment	**o**	**+**	**o**	**-**
Applicability to battery driven devices (host and slave)	**-**	**+**	**+**	**-**
Tactical acceptance / already deployed	**o**	**+**	**o**	**-**

Table 2-9 – Wireless Standards comparison

2.2.2.2 Network, Transport and Session Layer Standards

2.2.2.2.1 RTP / RTCP / SRTP / SRTCP

The Real-Time Protocol Transport Protocol is a protocol designed for the transport of audio and video data over a network. Its purpose is to provide a framework for end-to-end delivery of media, and has therefore seen use in many Voice-over-IP (VoIP) applications. RTP is capable of providing synchronization of and jitter compensation by marking packets with timestamps. Due to these features, data is usually sent over UDP allowing for fast data transfer.

RTP is operated in conjunction with the RTCP protocol (Real-time TCP) to allow the peers involved in an RTP session to exchange data on the quality of service of said session. A common use of the RTCP protocol is to facilitate flow control mechanisms in order to prevent network congestion.

The RTP protocol is an open protocol which is standardized through RFC documents, and by the use of RTP audio or video profiles. These profiles are used to specify the specific parameters used by the RTP protocol, tailored to the encoding used in the used audio / video encoding.

The RTP and RTCP protocols are unsecure by default. To increase security, the SRTP and SRTCP protocols (Secure RTP and Secure RTCP respectively) have been developed. These protocols provide both an authentication and an encryption layer. AES is used as the default cipher in a stream cipher configuration.

Being a secure alternative to RTP and RTCP, the SRTP and SRTCP protocols are good candidates for audio and video stream transport in a DSS. Due to the end-to-end design, some care should be taken in session set-up (e.g. through session protocols such as SIP) to provide a reliable service. The protocols can be used in both broadcasting and streaming scenarios.

2.2.2.2.2 Recommendation H.323

H.323 is a hybrid system constructed of centralized intelligent gatekeepers, multipoint control units (MCU), gateways, and less intelligent endpoints.

Endpoints (i.e. terminals) provide point-to-point and multipoint conferencing for audio and, optionally, video and data. Gateways interconnect to Public Switched Telephone Network (PSTN) or ISDN networks for H.323 endpoint interworking. Gatekeepers provide admission control and address translation services for terminals or gateways. MCUs are devices that allow two or more terminals or gateways to conference with either audio and/or video sessions.

H.323 call signalling is based on the ITU-T Recommendation Q.931 protocol and is suited for transmitting calls across networks using a mixture of IP, PSTN, ISDN, and QSIG over ISDN.

Although the H.323 standard is more complete in its latest revisions, issues have arisen, such as long call-setup times, overhead of a full-featured conferencing protocol, too many functions required in each gatekeeper, and scalability concerns for gatekeeper call-routed implementations. In this respect, SIP solves some of the problems found in H.323 and offers a good alternative (see relevant section).

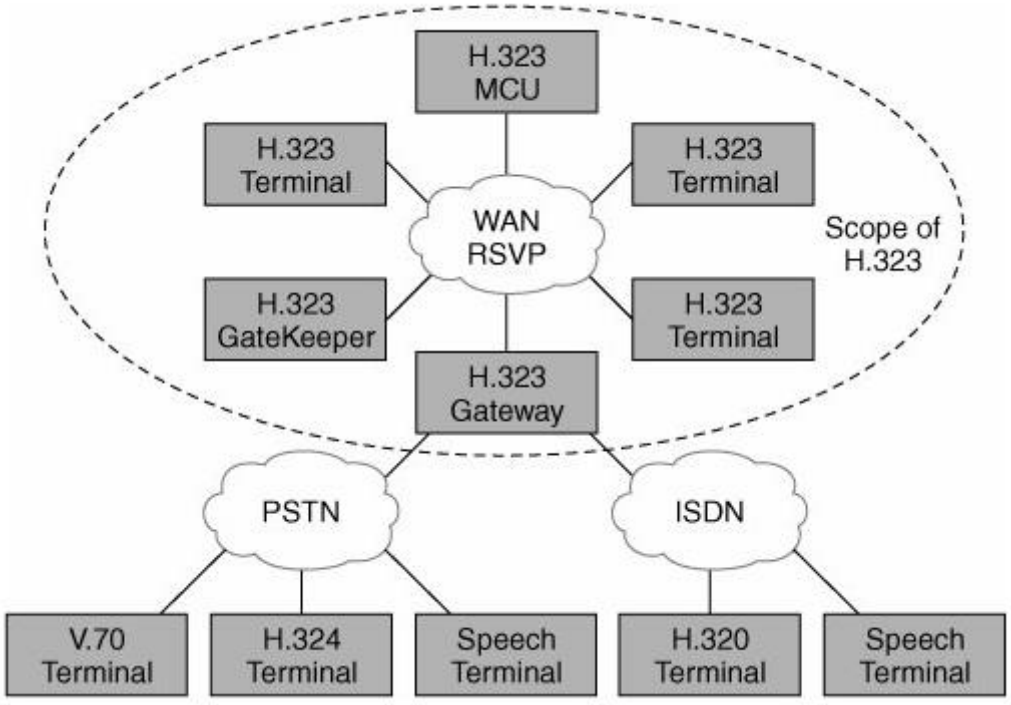

Figure 2-3 – H.323 Hybrid System

2.2.2.2.3 Real Time Streaming Protocol (RTSP)

The Real Time Streaming Protocol (RTSP) is an application-layer protocol for the setup and control of the delivery of data with real-time properties.

RTSP version 2.0 is published as RFC 7826 (see /29/). It is to be noted that, although based on the now obsolete RTSP 1.0, RTSP 2.0 is not backwards compatible other than in the basic version negotiation mechanism.

RTSP is designed for use in entertainment and communications systems to control streaming media servers. RTSP allows to establish and control media sessions between end points. Clients of media servers issue common media control commands, such as play, record and pause, to facilitate real-time control of the media streaming from the server to a client (Video On Demand) or from a client to the server (Voice Recording).

The transmission of streaming data itself is not a task of RTSP. Most RTSP servers use the Real-time Transport Protocol (RTP) in conjunction with Real-time Control Protocol (RTCP) for media stream delivery. However, some vendors implement proprietary transport protocols.

2.2.2.2.4 Session Description Protocol (SDP)

The Session Description Protocol (SDP) is a method to describe the media supported in a session. SDP does not deal with establishing the session, but only with describing the media supported by the endpoints in the call. The IETF published the original specification as a Proposed Standard in April 1998, and subsequently published a revised specification as RFC 4566 in July 2006 (see /71/).

SDP is used for describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP is intended to be general purpose so that it can be used in a wide range of network environments and applications.

However, SDP does not deliver any media by itself but is used between endpoints for negotiation of media type, format, and all associated properties. The set of properties and parameters are often called a session profile.

An SDP session description consists of a number of lines of text of the form:

<type>=<value>

Where <type> must be exactly one case-significant character and <value> is structured text whose format depends on <type>.

In actual use, the call owner sends multicast messages which contain the description of the session e.g. the name of the owner, the name of the session, the coding, the timing etc. Depending on these information, the recipients of the advertisement take a decision about participation in the session.

SDP is designed to be extensible to support new media types and formats. SDP can be used in conjunction with Real-time Transport Protocol (RTP), Real-time Streaming Protocol (RTSP), Session Initiation Protocol (SIP) and even as a standalone format for describing multicast sessions.

2.2.2.2.5 Session Initiated Protocol (SIP)

In every communication session, there needs to be a standard for the control of that session. For instance, it is necessary to communicate about how a connection should be set up. The Session Initiation Protocol SIP is a protocol which is designed to provide this type of communication.

SIP identifies two parties, a client who wishes to set up a connection to some destination, and a server, who responds to the client requests by providing information whether this connection could be set up. The SIP protocol is similar to the HTTP protocol, in that it is text-based, and that it uses response codes to categorize the answers by the server.

Being a signalling protocol, SIP only provides a method for the orchestration of communication. For other parts of the communication (e.g. the transfer of data), other protocols are needed. For example, in a live-video conference call setting, SIP can be used to set-up a RTP session over UDP which is used to transmit VP9-encoded video. Although SIP messages are unsecured by default, they can be secured using Transport Layer Security (TLS).

In Voice-over-IP communication, the SIP protocol is often used as the main signalling protocol. This is also reflected in SIP terminology, which corresponds to regular telephone terminology. This is also a potential use-case for SIP in a DSS, where it could be used to set up communication, for instance, it could be used to set-up a multicast voice communication channel between a group of soldiers. Due to the SIP protocol seeing widespread use in the telephone industry, it might also be used to connect the DSS to external systems if so desired.

2.2.2.2.6 UDP

Stands for "User Datagram Protocol." It is part of the TCP/IP suite of protocols used for data transferring. UDP is a known as a "stateless" protocol, meaning it doesn't acknowledge that the packets being sent have been received. For this reason, the UDP protocol is typically used for streaming media. While you might see skips in video or hear some fuzz in audio clips, UDP transmission prevents the playback from stopping completely.

2.2.2.2.7 TCP

Stands for "Transmission Control Protocol." TCP is a fundamental protocol within the Internet protocol suite — a collection of standards that allow systems to communicate over the Internet. It is categorized as a "transport layer" protocol since it creates and maintains connections between hosts.

TCP compliments the Internet protocol (IP), which defines IP addresses used to identify systems on the Internet. The Internet protocol provides instructions for transferring data while the transmission control protocol creates the connection and manages the delivery of packets from one system to another. The two protocols are commonly grouped together and referred to as TCP/IP.

When data is sent over a TCP connection, the protocol divides it into individually numbered packets or "segments." Each packet includes a header that defines the source and destination and a data section. Since packets can travel over the Internet using multiple routes, they may arrive at the destination in a different order than they were sent. The transmission control protocol reorders the packets in the correct sequence on the receiving end.

TCP also includes error checking, which ensures each packet is delivered as requested. This is different than UDP, which does not check if each packet was successfully transmitted. While the built-in error checking means TCP has more overhead and is therefore slower than UDP, it ensures accurate delivery of data between systems. Therefore TCP is used for transferring most types of data such as webpages and files over the Internet. UDP is ideal for media streaming which does not require all packets to be delivered.

2.2.2.3 Media

2.2.2.3.1 FLAC

FLAC, which stands for 'Free Lossless Audio Codec', is an encoding format for audio. The FLAC encoding has been defined within the FLAC project, which defines additional parts. Within the project, a container format for FLAC-encoded audio and encoder and decoder reference implementations are provided.

The FLAC-encoding is a so-called lossless encoding, it has been designed in such a way that after decoding audio encoded with FLAC, the original source data can be recovered. The efficiency of the encoding process is guided using a configurable compression level parameter, which allows a user to trade longer encoding time (and a slightly longer decoding time) for a better compression.

The FLAC container format is designed in such a way that it allows for fast encoding and decoding, as well as streaming. This means that the decoder is able to start the decoding process at any point in the stream.

The encoding, container, and reference implementations are released under royalty-free licenses. An open-source library (libflac) is available which allows the integration of FLAC into other software packages. The FLAC codec is supported by default on Android and Windows 10, and can be compiled for Linux.

The FLAC encoding format may be useful in a DSS in scenarios where retaining the quality of an audio recording is important. The configurable encoding speed make FLAC a candidate for the encoding of live-streamed audio. For voice and speech encoding, the Opus codec may be a better candidate, as it has been designed to optimize the encoding/decoding for this purpose.

2.2.2.3.2 G.711

This ITU-T standard dates from 1972 and is also known as Pulse code modulation (PCM) of voice frequencies. G.711 is primarily used in telephony for audio compression and expanding and a required standard in many technologies, for example in H.320 and H.323 specifications. It can also be used for fax communication over IP networks (as defined in T.38 specification). G.711 is a very commonly used narrowband audio waveform codec that provides toll-quality audio at 64 kbit/s, passing audio signals in the 300–3400 Hz range.

The signals are sampled at 8,000 samples per second, with a tolerance of 50 parts per million (ppm). Non-linear (i.e. logarithmic) quantization is used with 8 bits to represent each sample, resulting in 64 kbit/s transmission rate.

There are two slightly different compression versions:

- μ-law, which is used primarily in North America and
- A-law, which is in use in most other countries.

Two enhancements to G.711 have been published:

- G.711.0 (2009) featuring lossless data compression to reduce the bandwidth usage by 50% and
- G.711.1 (2008) increasing audio quality by increasing bandwidth. Depending on the sample rate (8 or 16 kHz), bandwidth may increase to 4000 and 7000 Hz, respectively.

For DSS, G.711.0 seems more relevant for traffic that is shared within the dismounted group, when military frequencies in the VHF and lower UHF band are used. An essential consideration will be which voice quality or rather speech intelligibility, will be acceptable in military operations. If this is

regarded too low at G.711.0, G.711.1 might be preferable with the increased bandwidth as a penalty. In 2012, annexes are added to G.711.1, enhancing the lossless data compression feature and the so-called super wideband (14.000 Hz), respectively.

2.2.2.3.3 HEVC/H.265

HEVC/H.265 (also known as MPEG-H Part 2). It supports videos up to a resolution slightly higher than 8K (7680x4320). HEVC introduces many new compression techniques, which improve the compression performance of its predecessor (AVC/H.264). Its performance is comparable to the VP9 codec.

The HEVC codec is covered by many patents. The patent owners (among which Apple, Microsoft, Motorola and Samsung) are grouped into two large patent pools (HEVC LA and HEVC Advance), which require licensing fees for the development and use of hardware supporting HEVC. HEVC Advance has recently waived the royalties for the use of software-based HEVC.

Qualcomm, Intel, NVIDIA and ARM provide CPUs, GPUs and SoCs with hardware acceleration support for HEVC. As such, the HEVC codec can be efficiently used in most modern smartphones and computer systems.

If the patent licensing is not an issue, HEVC/H.256 could be employed as the main codec for video applications in a DSS. The SoC implementations allow applications to encode/decode HEVC/H.256 with a higher power efficiency than would be attainable with a software-based encoder/decoder.

2.2.2.3.4 Matroska (MKV)

The Matroska file format is a multimedia container format, designed to support multiple tracks of audio and video, as well as subtitles. Matroska files are serialized using the Extensible Binary Markup Language (EBML), a binary extension to XML. This allows the Matroska standard to be easily extended / adapted if required. Other features of Matroska are error resilience, fast seeking and support for stereoscopic video.

From a streaming perspective, Matroska is not optimized for live streaming purposes, but is suited to be used in non-live streaming. As such, it may be used in conjunction with HTTP adaptive streaming technologies.

Matroska is released as an open standard, and its usage does not incur royalties. The libEBML parser, which can be used to parse Matroska files, is released under the LGPL license. The Matroska format is supported on all mayor operating systems and mobile devices.

In a DSS, the Matroska format can be used as a container for media files. Due to its flexible design, it is able to contain any audio or video format, which makes it suitable for usage in combination with lesser-known formats. Although the format is not suitable for live-streaming, it can be used for regular streaming.

An alternative container format similar to Matroska is the WebM container format, which is defined as a subset of Matroska. As such, it only supports VP8/VP9 encoded video and Opus encoded audio.

2.2.2.3.5 MPEG-4 Part 14 (MP4)

MPEG-4 Part 14 (also known as MP4), is an extension to the ISO Base Media File Format (ISOBMFF), and serves as a multimedia container. MP4 features a wide support for many video

and audio codecs, as well as multiple audio/video tracks, subtitles and stereoscopic video. The HEVC and H.264 video codecs are commonly used in conjunction with the MP4 container format.

MP4 is a suitable candidate for HTTP adaptive streaming, as its header is included at the beginning of a file. This allows clients to efficiently skip through a video while only fetching video data which is needed, and nothing more. For live-streaming, MP4 can be used if using a technique known as fragmented streaming. Fragmented streaming entails that the format of an MP4 file is used to keep appending new data, while still serving a valid MP4 file. Although this approach can be used to achieve real live-streaming, it can be considered as a workaround. More suitable alternatives for live-streaming would be MPEG-TS (which can contain the same type of streams as MP4), or WebM.

The MP4 format is likely to be covered by patents. However, the largest patent pool MPEG-LA does not charge royalties to end-users. Therefore, royalties only apply in encoding/decoding software or hardware. Note that the H.264 and HEVC codecs commonly used in conjunction with MP4 are definitely covered by patents from the MPEG-LA patent pool.

In a DSS, the MP4 format can be used as a container format for audio and video data. As a storage format, MP4 can be used to transfer recorded media to and from one or more DSSs. As multiple SoCs are available which support H.264 / HEVC (and therefore MP4), the MP4 format can be used in scenarios where high-efficiency decoding is required.

2.2.2.3.6 PNG

PNG, which can be pronounced "ping" or "P-N-G," is a compressed raster graphic format. It is commonly used on the Web and is also a popular choice for application graphics.

The PNG format was introduced in 1994, after the GIF and JPEG formats had already been around for several years. Therefore, PNG includes many of the benefits of both formats. For example, PNG images use lossless compression like GIF files, so they do not have any blurring or other artefacts that may appear in JPEG images. The PNG format also supports 24-bit color like the JPEG format, so a PNG image may include over 16 million colors. This is a significant difference between GIF and PNG, since GIF images can include a maximum of 256 colors.

Unlike the JPEG and GIF formats, the PNG format supports an alpha channel, or the "RGBA" color space. The alpha channel is added to the three standard color channels (red, green, and blue, or RGB) and provides 256 levels of transparency. JPEG images do not support transparent pixels and GIF images only support completely transparent (not partially opaque) pixels. Therefore, the PNG format allows Web developers and icon designers to fade an image to a transparent background rather than a specific color. A PNG with an alpha channel can be placed on any color background and maintain its original appearance, even around the edges.

While the PNG image format has many benefits, it is not suitable for all purposes. For example, digital photos are still usually saved as JPEGs, since PNGs take up far more disk space. GIFs are still used for animations since PNG images cannot be animated. Additionally, GIFs are still used on many websites since browsers only recently provided full support for the PNG format. However, now that most browsers and image editing programs support PNGs, it has become a popular file format for web developers and graphic artists.

2.2.2.3.7 TIFF

Stands for "Tagged Image File Format." It is a graphics file format created in the 1980s to be the standard image format across multiple computer platforms. The TIFF format can handle color depths ranging from 1-bit to 24-bit. Since the original TIFF standard was introduced, people have been making many small improvements to the format, so there are now around 50 variations of the

TIFF format. So much for a universal format. Recently, JPEG has become the most popular universal format, because of its small file size and Internet compatibility.

2.2.2.3.8 VoIP CODECs

As mentioned in 2.2.2.2.5, a VoIP call consists of two or more endpoints exchanging short data packets. The call starts with the caller endpoint contacting the called one(s) using a call control protocol like SIP2.0. During this phase, no actual audio is exchanged yet. A negotiation phase then follows, in which the parts agree on the format of the data packets that will be exchanged over the network during the call (audio, video, or both). The format is a set which includes sample rate, duration, compression law of the audio samples carried by the data packets, it is referred to as a CODEC and it is usually implemented as a piece of software.2.2.2.2.5, a VoIP call consists of two or more endpoints exchanging short data packets. The call starts with the caller endpoint contacting the called one(s) using a call control protocol like SIP2.0. During this phase, no actual audio is exchanged yet. A negotiation phase then follows, in which the parts agree on the format of the data packets that will be exchanged over the network during the call (audio, video, or both). The format is a set which includes sample rate, duration, compression law of the audio samples carried by the data packets, it is referred to as a CODEC and it is usually implemented as a piece of software.

Most VoIP CODECs are derived directly from POTS (Plain Old Telephone Service) hence the audio bandwidth is limited from 300 to 3,400 Hz and the dynamic range is compressed within 40dB or less. The G.711 codec, also known as PCM (pulse-code modulation), complies with those conditions. The analogue audio signal is converted into 8bit samples at a rate of 8k samples per second, resulting in a 64kb/s stream (note: signal is actually sampled at a higher, 13 or 14bit, resolution, then compressed into 8bit samples according to a series of logarithmic coefficients; though the series are similar, the compression coefficients are slightly different in USA vs EU, and take the name of μ-Law and A-Law respectively). The stream is divided into portions, few milliseconds each, and sent as RTP data packets over the network. The VoIP version of G.711 commonly uses 160 byte payloads, i.e. 20ms per packet.

G.711/PCM (see section 2.2.2.3.2) is widely taken as a reference for all the speech codecs because it is openly available, simple to implement and requires little processing power. Also, it has good voice quality.

According to ITU-T Recommendation P.800 (Methods for Subjective Determination of Transmission Quality), the voice quality of the codec can be quantified using a Mean Opinion Score (MOS). MOS assigns a subjective rating of 1 to 5, the highest, the better.

MOS Rating	Quality	Degradation
5	Excellent	None
4	Good	Perceptible, but not annoying
3	Fair	Slightly annoying
2	Poor	Definitely annoying
1	Bad	Unacceptable

Table 2-10 – Mean Opinion Score for Transmission Quality

The MOS of G.711/PCM is above good. However, according to ITU-T P.800, MOS is determined with the talker "seated in a quiet room with volume between 30 and 120 dB and a reverberation time less than 500 ms (preferably in the range 200–300 ms). The room noise level must be below 30 dB with no dominant peaks in the spectrum." Unfortunately, these conditions are rarely met in the battlefield.

Moreover, the bandwidth required to maintain G.711 is about 80kb/s per conversation, which is quite high by any standard.

In the table below (abridged, revised and expanded from Cisco, Voice Over IP - Per Call Bandwidth Consumption) some commonly available codecs are compared with respect to MOS, packet size, and BW consumption. All listed codecs are publicly available and require no license.

Codec & Bit Rate [kb/s]	MOS	Voice Payload Size	Bandwidth (approx.)	Notes
G.711 (64 kb/s)	4.1	160 Bytes; [20ms]	87.2 kb/s	PCM, low CPU usage
G.726 (32 kb/s)	3.85	80 Bytes; [20ms]	55.2 kb/s	ADPCM
G.728 (16 kb/s)	3.61	60 Bytes; [30ms]	31.5 kb/s	ITU-T, LD-CELP
G.729 (8 kb/s)	3.92	20 Bytes; [20ms], also available with 10ms frame length	31.2 kb/s	CS-ACELP, no longer require license, also available in G.729.1 version (better voice quality, scalable)
GSM-ESR (8 kb/s)	3.7	20 /30 ms	13kb/s (payload)	ETSI, ACELP
iLBC (8kHz/16bit)	3.92	160 Bytes; [20ms], also available with 30ms frame length	15kb/s or 13.3kb/s (payload)	RFC-3951, LPC

Legend:

- Sampled voice codecs: PCM (Pulse-code modulation), ADPCM: Adaptive differential PCM.
- Synthesized voice codecs (vocoders): LPC (Linear Predictive Coding), CELP (Code-excited linear prediction), LD-CELP (Low delay CELP), ACELP (Algebraic CELP), CS-ACELP (Conjugate Structure ACELP).

Table 2-11 – Common Codecs with Mean Opinion Scores

It is to be noted that sampled voice codecs offer a good representation of the whole signal captured by the microphone. The listener makes generally very little effort not only to understand the conversation, but also to detect the talker's identity. Ambient noise, if left unfiltered, can provide information on the place the talker is speaking from.

On the other hand, vocoders offer a much lower bandwidth occupation, although at the price of a higher processing power and a lower MOS. Detecting the identity of the talker is less straightforward, and little information other than pure speech is actually encoded. The heavy speech-optimisation of vocoders can have some drawbacks. For instance, completely removing all ambient noise is not always a desirable characteristic.

Also, some vocoders may behave sub-optimally in non-English language conversations, Codecs supported by GOSSRA VoIP speech calls should include at least:

- G.711, because it is a widespread reference, especially useful in testing environments;
- GSM-ESR, also widespread, offers a lower voice quality, but much lower bandwidth usage,
- G.729 or G.729.1, offer good voice quality at reasonable bandwidth usage.

2.2.2.4 Data Exchange Service

2.2.2.4.1 Data Delivery

In this chapter the chosen data delivery middlewares are described. First a rational for the decision for the exchange services is provided and then DDS as well as MQTT is described.

2.2.2.4.1.1 Rational

The following table shows a comparison of DDS, MQTT, Lean Services, JDSSIN, ZeroMQ/NORM and DisService. All five were chosen as possible candidates for the information exchange mechanism (IEM) within the soldier system. There are reams of middlewares available that are all capable of fulfilling the tasks needed. As /68/ already states, the analysis on pure technical level comparing the features is not sufficient to decide on a middleware. Hence, the technical parameters were just used for guidance if the middlewares are applicable. The most critical part was the therefore the COTS/MOTS/DIY question. /108/ already states, the analysis on pure technical level comparing the features is not sufficient to decide on a middleware. Hence, the technical parameters were just used for guidance if the middlewares are applicable. The most critical part was the therefore the COTS/MOTS/DIY question.

DDS, MQTT, ZeroMQ/NORM and DisService use the Publish/Subscribe principle as an **exchange pattern** and by that provide a name-based information space in which information can be shared. JDSSIN uses Multicast for data exchange on which UDP-Telegrams are send to all network participants that subscribe to the multicast group. Lean Services aim to provide a service-based view on a system which provides a service registry that can be used to request information.

The **type** of application as a middleware leads for DDS, MQTT, ZeroMQ/NORM and DisService to the comfortable situation that the application is disconnected from the network layer, while it is fully involved in JDSSIN. Lean Services use HTTP which aims to abstract the lower layers, but as a common TCP/IP Protocol it may not fully reach this approach. It provides data basically on a request/response pattern.

While ZeroMQ/NORM, DiService, JDSSIN and DDS share a decentralized **topology** approach, since no infrastructure beside the network is needed, MQTT has a centralized Broker and Lean Services have a HTTP-Server. This is especially critical in case of distributed systems that do not have central infrastructure, but in DSS it is common to have at least one computing unit that may host the broker. MQTT also defines the bridging between Brokers, hence a flexible approach with several Brokers is possible. Lean Services uses the same approach for their service registry.

Although it is worth noting that the serverless architecture improves the DSS reliability, both as single soldier and STU, because there is not any single point of failure for data exchange services.

DDS, MQTT and JDSS are capable of identifying if participants left the network or information space or in other words to **determine the liveliness**. Specifically DDS, provides such a check mechanism both at node and single end-point levels, so improving troubleshooting and recovery.

The **updating of late joiners** is handled by every IEM in different ways, except Lean Services that do not provide this ability. Late joiners are communication partners that enter the network after communication has been performed. This is vital in case information need to be synchronized since they have a certain lifetime. For example a measurement of a laser range finder has a life time of a few seconds and only needs to be transferred safely. Tactical Symbols may have a life time of hours or days and thus need to be persistent in the system and should be synchronized in case a new participant joins e.g. a tablet with a BMS application in addition to another EUD. DDS and ZeroMQ/NORM can perform the late joiner update per instance of a topic in case the publisher is still there. MQTT and DisService can provide the last topic provided even in case the participant

is gone. JDSSIN can provide a certain range of messages buffered by the application to the participant, but with no separation of the information. DDS allow to specify the deepness of the history a given publisher shall maintain or a subscriber will request, the two history lengths shall be compatible in order the session to be established. The history allows an application to cope for both high latency network and intermittent network where a subscriber may disconnect for time intervals which is multiple of the data publishing period.

All IEM can **ensure the transmission to all active participants**. DDS also provides for Filtered Contents, where a data is transmitted to recipient(s) only if it matches a given predicate. This could be useful to cope with both communication and computation resources scarcity.

The **data representation** is quite different for all exchange mechanisms. While DDS uses a data model which is brought to a platform specific model, MQTT, ZeroMQ/NORM and DisService do not support anything specific, these middleware's basically forward the information provided to it. JDSSIN uses an XML-Messages as payload and Lean Services use JSON Objects. Both are string representation. Despite some middleware's do not define a data representation all IEMs support a common way of data representation that allows data parsing without defining everything to the BIT-Level (e.g. Bit-Order Big-Endian/Little-Endian). DDS also support variable data types, which cope with both (i) resource scarcity by transmitting only the fields which effectively changed, and (ii) data syntax evolution, guaranteeing the interoperability among different syntactic version of the same information (Topic).

Regarding the **main purpose** DDS is mostly used in distributed systems that are lacking central infrastructure or should not have one or require for high service availability, due to its native support to hot redundancy among information sources, so coping with network branch disconnection. It is highly flexible in configuration and features and also useful for dynamic environments, such as the tactical mobile ad-hoc network (MANET). MQTT is an IoT-Standard of sensor networks that need to connect to a central interaction point (where the broker is installed). By this MQTT has a semi-dynamic approach. It needs a central broker, but the participants of the network are flexible. JDSSIN is mainly used in the tactical environment but has common parts of session layer protocols. DDS and ZeroMQ/NORM, or more specifically the NORM protocol is designed for providing and end-to-end reliable transport over generic IP multicast making it suitable for ad-hoc networking. DisService is designed to be used in tactical networks specially.

Concerning the **environment, the IEMS were designed** for it can be stated, that DDS, ZeroMQ/NORM, DisService as well as JDSSIN were designed for dynamic environments, while MQTT and Lean Service have a centralized broker/server, but no dependencies regarding the participants. Leading to a semi-dynamic communication network.

All IEMs are **applicable to battery driven devices.** This is important, since the DSS is commonly battery driven. DDS, ZeroMQ/NORM and DisService have a little exception, since it is a complex middleware it may not be used on real low power devices. Lean Service are in need of a HTTP-Server and a non-optional compression, which leads to additional power being consumed. Lean Services may use other protocols/middleware such as DDS for transportation, but this would just add another layer. Regarding the DSS that are commonly driven by a battery that is the equivalent to a laptop or smart phone battery, it is certain that using DDS or LSA is feasible. Moreover DDS due to the support of both content filtering and optional data types can strongly reduce the computing power needs.

It is also important that the IEM for the DSS is capable to be used on devices with very limited resources such as micro controllers, so if they are **applicable to micro controllers**. Here DDS can only be used in a minimal configuration, since the resources such as computing power and memory are not available. This reduces the list of features provided by DDS greatly. MQTT was designed for such systems and is therefore by definition applicable. JDSSIN can also be run in such an environment. Lean Services introduce a great overhead due to HTTP and the

compression or just an additional overhead in case another transport protocol is used. As power consumption is critical, Lean Services may not be used.

Regarding the DSS domain personal area networks such as Bluetooth are common and may be used. Hence, it is important to see if the proposed IEMs are **suitable for personal area network communication**. While MQTT was designed exactly for usage in WIFI or Bluetooth, it can only be guessed with a certain confidence that JDSSIN, having a look on the protocol itself, is suitable for the communication. Usage of DDS over Bluetooth is feasible provided that an UDP layer is available, the point to point communication is solved by the DDS features of static address assignment. Usage of Lean Services over such communication means is unclear. Both ZeroMQ/NORM and DisService rely on UDP multicast and can be used over Bluetooth if the operating system supports UDP over the Bluetooth radio.

The identification of instances is also an important feature, since only in case the middleware is aware that instances of objects can be separated by certain attributes, it is capable of differ between instances and thus to handle instances in different ways. For example, DDS is capable of handling one topic with several instances. Hence, it is possible that DDS as one Topic named “Blueforce” on which different blue forces elements can be assigned separated instance identifier. MQTT and LSA are not capable of doing so, the separation of instances needs to be done via topic names. For MQTT this is possible, since MQTT allows wildcards in the subscription and thus to transfer the identification into the topic name. JDSSIN and ZeroMQ/NORM leave this matter to the application, they can only differ between messages.

The **complexity** varies greatly between the IEMs. DDS is extremely powerful and rich in features, which leads to a high complexity. ZeroMQ/NORM and MQTT do not have a lot of features and in the case of MQTT a centralized broker reducing the complexity greatly, but also the “luxury” it provides to the user. DisService and JDSSIN is in the middle, it is not very complex, but leaves also things to the application. Lean Services gain in complexity due to the usage of HTTP and compression but are still less complex than DDS.

Regarding the buy or build decision as well as the credibility of the standard, the question **COTS/MOTS/DIY** should be considered. It is very useful to consider software that can be bought from the shelf. This reduces development costs, but also improves the accordance to standards, since the COTS approach will be used in interoperable environments. It is especially interesting if the COTS middleware’s have a high degree of distribution. Additionally, it lowers the barrier to enter the standard and thus allows also smaller companies and research institutes to provide software or equipment according to the standard. By this the standard is not reduced to the big players, but also offers chances for SME’s. MOTS can serve the same purpose with a reduced number of software vendors. DIY may result in different interpretations of the standard and by that to incompatibility. DDS as well as MQTT can be bought from the shelf and are highly distributed. ZeroMQ and NORM are available as open source and open specification. JDSSIN is available as “NATO Open Source”. Lean Services and DisService are currently for most companies a Do-it-yourself Protocols, what results in high development costs and possible interoperability issues.

To **conclude** DDS is the most comprehensive IEM from the proposed for handling complex information in a distributed system. Hence, it is a good candidate for the communication in the DSS. Especially in such C4I Functional Areas where is requested highly reactive, rich content and robust data exchange such as the Network-centric Battlefield Management System (NEC-BMS), Situational Awareness (SA) and System Management (SYS) where it is requested to manage an high number of instances of different topics whose composition and relationships change dynamically at an high rate. The publish/subscribe paradigm and the ability to identify object instances on IEM level improves the usability for more advanced methods such as sensor data fusion. Which may lead at JDSSIN to higher efforts e.g. in case a certain information is needed to provide a matching between different sensor values. Currently DisService has no open specification and therefor is no candidate for the DDS. MQTT does not provide a sufficient set of features to support these complexity as well as Lean Services.

DDS seems less suitable for the PAN communication as well as for low power devices. The same accounts for DisService and ZeroMQ/NORM. The PAN domain could be suited by MQTT as well as JDSSIN and Lean Services. Thinking of DDS as the “backbone” IEM it is not useful to introduce another multicast protocol, what DDS basically does on lower level, to the DSS domain. The additional multicast protocol will only transfer the information to a single point where it is translated. Hence, it is more useful to provide a centralized gateway that translates the information to DDS. This suits mostly to MQTT since it has a centralized broker or Lean Services with the possibility to see the DSS as one system with all its peripherals. MQTT serves the publish/subscribe principle as DDS does and it is payload agnostic, allowing a simple translation between DDS and MQTT, while Lean Services force the payload into a JSON Object and do not serve the publish/subscribe principle. Hence MQTT should be chosen for this particular use cases.

Properties	DDS	MQTT	JDSSIN	LSA	ZeroMQ/NORM	DisService
Type	Middleware	Middleware	Protocol	Service Based	Middleware	Middleware
Exchange Pattern	Publish/Subscribe	Publish/Subscribe	Multicast	Request/Response	Pub/Sub	Pub/Sub
Topology	Decentral	Central Message Broker	Decentral	Centralized	Decentral	Decentral
Determine Liveliness[2]	Yes	Yes	Yes	No	No	?
Updating Late-Joiners	Per Instance, With History	per Topic	Just a certain window of messages	No	Per instance with current configuration	Configurable per topic
Ensure Transmission to active participants	Yes	Yes	Yes	Yes	Yes	Yes
Data Representation	Defined by Data model and Named	N/A	XML	JSON	N/A	N/A
Main Purpose	(Critical) Distributed Systems	Sensor Networks	Tactical Radio	N/A	Unreliable networks	Tactical networks

[2] Identify the absence of a participant by means of the exchange mechanism. Additional means on application layer are not considered.

Environment designed for (Dynamic/Static)	Dynamic	Semi-Static	Dynamic	Semi-Static	Dynamic	Dynamic
Applicability to battery driven devices	Depends	Yes	Yes	Depends	Yes	Yes
Applicability to microcontrollers (low power/resource devices)	Reduced set of features	Yes	Yes	No	No	No
Suitable for personal area network communication	No	Yes	Yes	No	Maybe	Maybe
Identification of instances	Topic[3] Data Type Fields	By Topic	No[4]	By Topic	No, left to the application	?
Complexity	High	Low	Medium	Medium	Low	Low
COTS/MOTS/DIY	OMG Standard, COTS	COTS	DIY or use NATO Open Source	DIY, No open reference implementation known	Open source / open specification	Open source

Table 2-12 – Rating of middlewares

[3] Each Instance is uniquely identified via a set of Topic data type fields selected at Design Time.

[4] Application based

2.2.2.4.1.2 Data Distribution Service

2.2.2.4.1.2.1 Data-Centric Publish-Subscribe

The DDS specification describes a Data-Centric Publish-Subscribe (DCPS) model for distributed application communication and integration. This specification defines both the Application Interfaces (APIs) and the Communication Semantics (behaviour and quality of service) that enable the efficient delivery of information from information producers to matching consumers.

- The purpose of the DDS specification can be summarized as enabling the “Efficient and Robust Delivery of the Right Information to the Right Place at the Right Time.”

The expected application domains require DCPS to be high-performance and predictable as well as efficient in its use of resources. To meet these requirements it is important that the interfaces are designed in such a way that they:

- Allow the middleware to pre-allocate resources so that dynamic resource allocation can be reduced to the minimum,
- Avoid properties that may require the use of unbounded or hard-to-predict resources, and
- Minimize the need to make copies of the data.

DDS uses typed interfaces (i.e., interfaces that take into account the actual data types) to the extent possible. Typed interfaces offer the following advantages:

- They are simpler to use: the programmer directly manipulates constructs that naturally represent the data.
- They are safer to use: verifications can be performed at compile time.
- They can be more efficient: the execution code can rely on the knowledge of the exact data type it has in advance, to e.g., pre-allocate resources.

It should be noted that the decision to use typed interfaces implies the need for a generation tool to translate type descriptions into appropriate interfaces and implementations that fill the gap between the typed interfaces and the generic middleware. QoS (Quality of Service) is a general concept that is used to specify the behaviour of a service. Programming service behaviour by means of QoS settings offers the advantage that the application developer only indicates ‘what’ is wanted rather than ‘how’ this QoS should be achieved. Generally speaking, QoS is comprised of several QoS policies. Each QoS policy is then an independent description that associates a name with a value. Describing QoS by means of a list of independent QoS policies gives rise to more flexibility.

2.2.2.4.1.2.2 Real Time Publish Subscribe

The Real-Time Publish Subscribe (RTPS) protocol found its roots in industrial automation and was in fact approved by the IEC as part of the Real-Time Industrial Ethernet Suite IEC-PAS-62030. It is a field proven technology that is currently deployed worldwide in thousands of industrial devices. RTPS was specifically developed to support the unique requirements of data-distributions systems. As one of the application domains targeted by DDS, the industrial automation community defined requirements for a standard publish-subscribe wire-protocol that closely match those of DDS. As a direct result, a close synergy exists between DDS and the RTPS wire-protocol, both in terms of the underlying behavioural architecture and the features of RTPS. The RTPS protocol is

designed to be able to run over multicast and connectionless best-effort transports such as UDP/IP. The main features of the RTPS protocol include:

- Performance and quality-of-service properties to enable best-effort and reliable publish-subscribe communications for real-time applications over standard IP networks.
- Fault tolerance to allow the creation of networks without single points of failure.
- Extensibility to allow the protocol to be extended and enhanced with new services without breaking backwards compatibility and interoperability.
- Plug-and-play connectivity so that new applications and services are automatically discovered and applications can join and leave the network at any time without the need for reconfiguration.
- Configurability to allow balancing the requirements for reliability and timeliness for each data delivery.
- Modularity to allow simple devices to implement a subset of the protocol and still participate in the network.
- Scalability to enable systems to potentially scale to very large networks. • Type-safety to prevent application programming errors from compromising the operation of remote nodes.

The RTPS also support the dynamic discovery among the DDS entities belonging to the same DDS domain.

2.2.2.4.1.3 Message Queue Telemetry Transport

MQTT is an open machine-to-machine information exchange protocol that uses the publish/subscribe principle. It was standardized 2013 by the Organization for the Advancement of Structured Information Standards (OASIS). It is usually used for Internet-of-Things purposes in slow sensor networks.

In different to DDS MQTT introduces a central component, the “broker” that handles communication between publisher and subscriber. The centralized broker reduces the efforts for publishers, since the broker holds the information for late joiner and handles the ensured message transfer to the subscribers. This matter serves the common usage of MQTT and is applicable on Soldier Systems as well. In accordance to the chosen system busses, that also introduce centralized infrastructure their self it is possible to host the MQTT-broker on these performant system bus hosts and have minimal client implementations in the devices.

In case a second MQTT-Broker needs to be integrated into a system the bridging function can be used. Bridged broker share the subscribed topic between each other so that information are openly shared between the two.

For low performant sensor networks MQTT-SN is specified. While MQTT is using TCP to hold the connection MQTT-SN is using UDP. This is for different reasons. UDP is easier to implement and serves a connectionless communication model. Hence, it is not necessary to keep a connection open and serve keep-alive requested by the lower protocol. This reduces resource usage and communication efforts significantly.

2.2.2.4.2 Streaming

2.2.2.4.2.1 RTP

See section 2.2.2.2.1.

2.2.2.4.2.2 RTSP

See section 2.2.2.2.3

2.2.2.4.2.3 H.323

See section 2.2.2.2.2

2.2.2.4.2.4 SIP / SDP

The Session Initiation Protocol is commonly used in Voice over IP applications to establish and control a communication session. As SIP is not used to carry data, RTP is used for the transmission. Hence, both protocols are coupled. As it is widely used in Voice over IP Application it can be routed and provide infrastructure roles such as “redirect server” in order to work in highly meshed networks. Hence, it is also applicable to different use cases in a soldier system as well as in digital radio communication.

SIP uses the Session Description Protocol to describe the streaming media communication parameters. (See also sections 2.2.2.2.4 and 2.2.2.2.5)

2.2.2.4.2.5 STANAG 4609

Motion Imagery (MI) is a valuable asset for commanders that enable them to meet a variety of theatre, operational and tactical objectives for intelligence, reconnaissance and surveillance. STANAG 4609 is intended to provide common methods for exchange of MI across systems within and among NATO nations. STANAG 4609 is intended to give users a consolidated, clear and concise view of the standards they will need to build and operate motion imagery systems. The STANAG includes guidance on uncompressed, compressed, and related motion imagery sampling structures; motion imagery time standards, motion imagery metadata standards, interconnections, and common language descriptions of motion imagery system parameters.

STANAG 4609 mandates that all visible light MI systems used by participating nations shall be able to decode all MPEG-2 transport streams with MPEG-2 compressed data types (Standard Definition, Enhanced Definition, High Definition) up to and including MISM Level 9M and all H.264 compressed data types up to and including MISM Level 9H, but each Nation may choose to ORIGINATE one, two or all data types. Levels 9M and 9H are defined in the Motion Imagery System Matrix (MISM) as found in AEDP-8.

Likewise, STANAG 4609 mandates that all Infrared MI systems used by participating nations shall be able to decode all MPEG-2 transport streams with MPEG-2 compressed data types up to and including MISM Level 8M and all H.264 compressed data types up to and including MISM Level 8H, but each Nation may choose to ORIGINATE either compression type at whatever level it chooses. The levels of the IR System Matrix are found in Edition 3 of AEDP-8. The objective of STANAG 4609 is to provide governance so as to allow participating nations to share MI to meet

intelligence, reconnaissance, surveillance and other operational objectives with interoperable MI systems.

2.2.2.4.3 Tactical Data Delivery

2.2.2.4.3.1 Variable Message Format

The Variable Message Format (VMF) Military Standard (MIL-STD) provides military services and agencies with Joint interoperability standards, including message, data element, and protocol standards. These standards are essential for the design, development, test, certification, fielding, and continued operation of automated tactical data systems (TDSs) which support the requirement to exchange timely, critical, command and control information across Joint boundaries.

VMF applies to all developmental and operational TDSs that are required to interoperate with one or more other service TDSs using VMF over any media. It contains message and data element standards for implementation on inter-service VMF interfaces.

VMF complies with basic Joint Forces policies and has been developed in consonance with the following concepts:

- Tactical command and control, and communications systems standards are developed only for systems and equipment applicable to functional areas in which the need for interoperability and compatibility has been validated as essential by the Joint Chiefs of Staff.
- VMF apply to operational and future tactical systems and use system characteristics previously approved for Service use where such characteristics meet the Joint requirements.
- VMF establishes certain standards and criteria for message formats and transmission characteristics that will be used in the design and/or procurement of systems and equipment. Additionally, these standards will be used in computer program development and when new system designs are implemented within existing systems.
- An interface between tactical systems should exploit the maximum capability of sensors and processors to provide precise information exchange in support of tactical operations.
- VMF Message format standards and information exchange criteria are designed to support established doctrine and known requirements.

2.2.2.4.3.2 Joint Dismounted Soldier System Interoperability Network

Joint Dismounted Soldier System Interoperability Network (STANAG 4677) has the aim to provide an interoperable communication exchange between C4 for systems of different NATO Partners. To achieve this it "*describes how an interoperability network between national dismounted soldier networks operating in a coalition environment is established. This is achieved through:*

- *The use of a standardised data message format derived directly from the Multilateral Interoperability Programme's (MIP) Joint Command Control and Consultation Information Exchange Data Model (JC3IEDM) STANAG 5525*
- *An Information Exchange Mechanism (IEM) tailored to the tactical radio environments found at the dismounted soldier level*

- *The setting up of a radio network across the coalition boundary with all member nations using a designated type of radio system, hereby called the "Loaned Radio". Described an interoperability network " (Source /14/ page 16)*

Therefore it defines all aspects needed to achieve this goal. Namely:

- Security concept
- Data Model
- Loaned Radio concept
- Information Exchange Mechanism
- Network access

Figure 2-4 shows how the different aspects interconnect with each other leaving out the security as it is an overall approach.

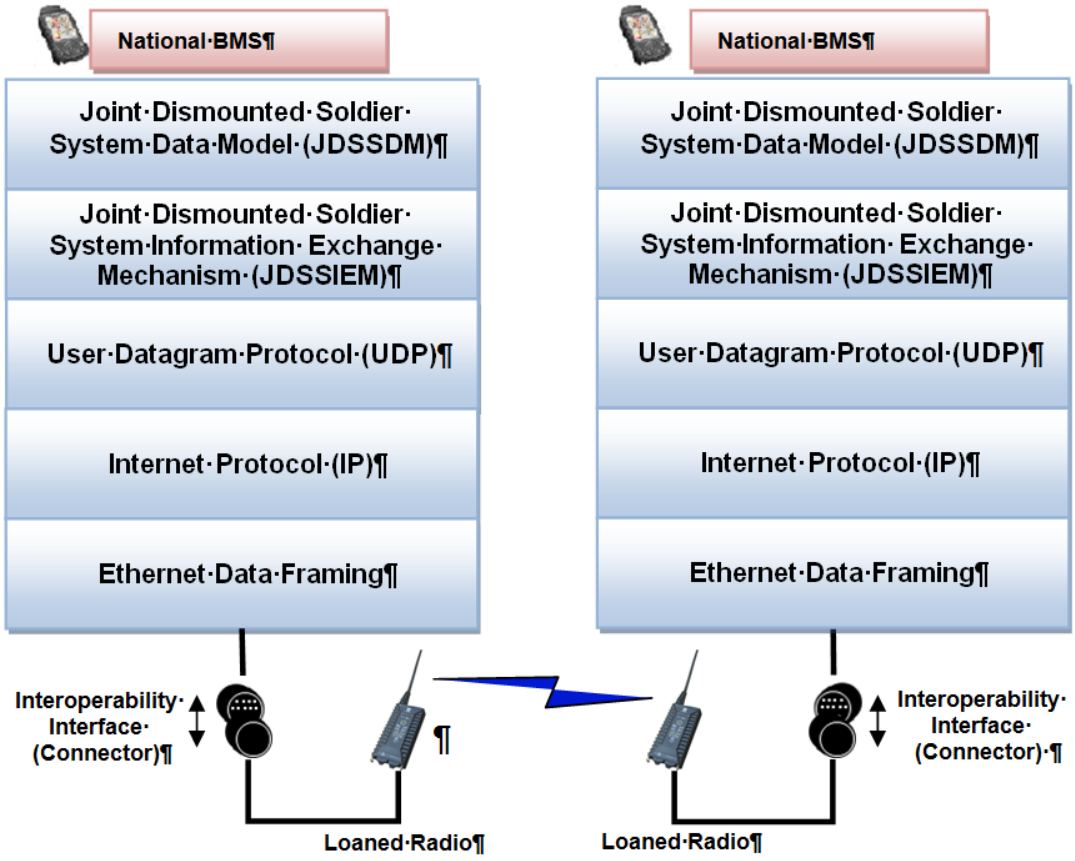

Figure 2-4 – JDSS Dismounted Soldier System C4 Interoperability Solution (Source: /14/)

Since JDSS is a well-defined and already deployed standard it is a valid input for interoperability purposes on all domains. So it is not only used for the Joint Domain, but also for other domains and as a useful input for the GOSSRA C4I Data model.

2.2.2.4.3.3 Rationale

Variable Message Format as well as STANAG 4677 are both well accepted standards in the NATO and thus valid for implementation. The goal was to provide standards that can be used for delivery of tactical data on different levels. These standards are recommendations to use. Hence, implementation is optional and could be avoided. Nevertheless the probability to have multinational missions especially with European forces is increasing. Hence, a suggesting stands can help as guidance for implementation.

The table below shows the considered standards or implementations.

Regarding the **main purpose** DDS is mostly used in distributed systems that are lacking central infrastructure or should not have one. It is highly flexible in configuration and features and also useful for dynamic environments. MQTT is an IoT-Standard of sensor networks that need to connect to a central interaction point (where the broker is installed). By this MQTT has a semi-dynamic approach. It needs a central broker, but the participants of the network are flexible. JDSSIN is mainly used in the tactical environment but has common parts of session layer protocols. ZeroMQ/NORM, or more specifically the NORM protocol is designed for providing and end-to-end reliable transport over generic IP multicast making it suitable for ad-hoc networking. DisService is designed to be used in tactical networks specially.

The **type** of application as a middleware leads for DDS, MQTT, ZeroMQ/NORM and DisService to the comfortable situation that the application is disconnected from the network layer, while it is fully involved in STANAG 4677 and VMF. On the other hand are STANAG 4677 and VMF actual standards and thus providing not only communication patterns, but also data model and physical data links

DDS, MQTT, ZeroMQ/NORM and DisService use the Publish/Subscribe principle as an **exchange pattern** and by that provide a name-based information space in which information can be shared. STANAG 4766 uses Multicast for data exchange on which UDP-Telegrams are send to all network participants that subscribe to the multicast group.

While ZeroMQ/NORM, DiService, STANAG 4677 and DDS share a decentralized **topology** approach, since no infrastructure beside the network is needed, MQTT has a centralized Broker. This is especially critical in case of distributed systems that do not have central infrastructure, and thus be critical for inter-DSS communication. MQTT also defines the bridging between Brokers, hence a flexible approach with several Brokers is possible, but lacking discovery mechanisms so bootstrapping in a decentralized environment is impossible if the standard is strictly followed.

All candidates can **ensure the transmission to all active participants**.

The **data representation** is quite different for all exchange mechanisms. While DDS uses a data model which is brought to a platform specific model, MQTT, ZeroMQ/NORM and DisService do not support anything specific, these middleware's basically forward the information provided to it. STANAG 4677 uses an XML-Messages as payload and VMF an own proprietary implementation. Despite some middleware's do not define a data representation all IEMs support a common way of data representation that allows data parsing without defining everything to the BIT-Level (e.g. Bit-Order Big-Endian/Little-Endian).

The **complexity** varies greatly between the candidates. DDS is extremely powerful and rich in features, which leads to a high complexity. ZeroMQ/NORM and MQTT do not have a lot of features and in the case of MQTT a centralized broker reducing the complexity greatly, but also the "luxury" it provides to the user. DisService and STANAG 4677 is in the middle, it is not very complex, but leaves also things to the application. VMF actually gaining complexity by its competitive and huge data model. While STANAG 4677 is made and mostly used for dismounted soldiers and this describing their narrow minded needs, VMF describes the whole battlefield.

Regarding the buy or build decision as well as the credibility of the standard, the question **COTS/MOTS/DIY** should be considered. It is very useful to consider software that can be bought from the shelf. This reduces development costs, but also improves the accordance to standards, since the COTS approach will be used in interoperable environments. It is especially interesting if the COTS middleware's have a high degree of distribution. Additionally, it lowers the barrier to enter the standard and thus allows also smaller companies and research institutes to provide software or equipment according to the standard. By this the standard is not reduced to the big players, but also offers chances for SME's. MOTS can serve the same purpose with a reduced number of software vendors. DIY may result in different interpretations of the standard and by that to incompatibility. DDS as well as MQTT can be bought from the shelf and are highly distributed. ZeroMQ and NORM are available as open source and open specification. STANAG 4677 is available as "NATO Open Source". DisService and VMF are currently for most companies a Do-it-yourself Protocol, what results in high development costs and possible interoperability issues.

To **conclude** MQTT is not suitable for the tactical domain in inter-DSS communication as it cannot serve the decentralized approach. ZeroMQ/NORM and DisService were compared against DDS and STANAG 4677 and it was shown, that STANAG 4677 can outperform these two or is at least on the same level. Hence, STANAG 4677 is already ratified and serves more than just information exchange it is a valid standard for inter-DSS communication. The same comparison showed, that DDS is not suitable for tactical networks in a configuration that provides greater benefits than the other candidates. As STANAG 4677 only provides tactical data on lower level VMF can be used to complete the communication on the whole spectrum of the tactical domain.

Thus STANAG 4677 and VMF are chosen for tactical data. DDS can be used for non-tactical data in medium performant radio networks and thus may not be used in the tactical domain. Since STANAG 4677 and VMF do not provide file exchange other protocols are suggested in the system view.

Properties	DDS	MQTT	STANAG 4677	VMF	ZeroMQ/NORM	DisService
Type	Middleware	Middleware	Standard	Standard	Middleware	Middleware
Main Purpose	Distributed Systems	Sensor Networks	Tactical Communication	Tactical Communication	Unreliable networks	Tactical networks
Exchange Pattern	Publish/Subscribe	Publish/Subscribe	Multicast	Unicast/ Multicast/ Broadcast	Pub/Sub	Pub/Sub
Topology	Decentral	Central Message Broker	Decentral	Decentral	Decentral	Decentral
Ensure Transmission to active participants	Yes	Yes	Yes	Yes	Yes	Yes
Data Representation	Defined by Data model	N/A	XML	Binary	N/A	N/A
Provides Data Model	No	No	Yes	Yes	No	No
Environment designed for (Dynamic/Static)	Dynamic	Semi-Static	Dynamic	Dynamic	Dynamic	Dynamic
Complexity	High	Low	Medium	High	Low	Low
COTS/MOTS/ DIY	COTS	COTS	DIY, Reference Implementation available as open source from Dutch MoD	DIY, Reference Implementation available as open source from Dutch MoD	Open source / open specification	Open source

Table 2-13 – Rating of inter-DSS communiation standards

2.2.2.5 Transport Service

2.2.2.5.1 Optimized Link State Routing Protocol

The **Optimized Link State Routing Protocol** (**OLSR**)is an IP routing protocol optimized for Mobile Ad-hoc Network (MANET), which can also be used on other wireless had hoc network. OLSR is a proactive link-state routing protocol, which uses *hello* and *topology control* (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

2.2.2.5.2 Internet Protocol

The internet protocol is the fundamental protocol for the internet, as well as for routed networks. It adds an addressing layer to the transport protocols and thus allows also to route the information between networks. Hence, it is a very important protocol for the Personal Domain of the DDS but even more important for the STU, Inter-Vehicle and Coalition and Joint domain. Wikipedia defines the IP Protocol as follows:

"The Internet Protocol is responsible for addressing host interfaces, encapsulating data into datagrams (including fragmentation and reassembly) and routing datagrams from a source host interface to a destination host interface across one or more IP networks. For these purposes, the Internet Protocol defines the format of packets and provides an addressing system.

Each datagram has two components: a header and a payload. The IP header includes source IP address, destination IP address, and other metadata needed to route and deliver the datagram. The payload is the data that is transported. This method of nesting the data payload in a packet with a header is called encapsulation.

IP addressing entails the assignment of IP addresses and associated parameters to host interfaces. The address space is divided into subnetworks, involving the designation of network prefixes. IP routing is performed by all hosts, as well as routers, whose main function is to transport packets across network boundaries. Routers communicate with one another via specially designed routing protocols, either interior gateway protocols or exterior gateway protocols, as needed for the topology of the network."[5]

The internet protocol version 4 was first deployed in 1983 with an address space of 32 Bit, introducing a limit of 4.294.967.296 unique hosts. It is possible to create private networks, so that not each of the computers need to be connected to the internet. Thera are three blocks for private networks namely 10.0.0.0/8, 172.16.0.0./12 and 192.168.0.0/16 allowing networks with up to 16.777.216 unique hosts. These hosts can then connect to the internet via a router that routes between the private and public network and performs network address transition. In IP-based systems usually the private ranges are used.

Due to the growth of numbers of computers in the internet, the address space is nearly exceeded today. Therefore IPv6 was created as a successor for IPv4. It integrates not only an enhanced address range of 128 Bit, but also some optimizations. The IPv4 header included information and fields to provide capabilities that are usually handled by other protocols above using IP. Hence, it

[5] Source: https://en.wikipedia.org/w/index.php?title=Internet_Protocol&oldid=927055788

was decided to mitigate the additional header overhead introduced to the wider range of addresses by removing these fields. Due to the high address range it is possible to assign a unique IP to every computer and this identify it with this IP.

2.2.2.6 Application

The NATO Generic Vehicle Architecture consists, in the current version (see /9/ till /13/), of 7 Volumes, each describing different aspects of the architecture.

2.2.2.6.1 Architecture

Volume one of the NATO Generic Vehicle Architecture (See /9/) describes the architectural approach and gives an introduction to the standard. Additionally it describes the key drivers and updates the benefits of the architecture.

2.2.2.6.2 Power Infrastructure

Volume two of the NATO Generic Vehicle Architecture (See /10/) describes the power infrastructure and is defining different connectors, pinning and requirements for power distribution. Hence it is a valid source for integration of dismounted soldiers in a NGVA-Vehicle. Since power support for soldiers is one of the main use cases for a soldier connection to the vehicle, the defined interfaces should comply with it.

2.2.2.6.3 Data Infrastructure

Volume three of the NATO Generic Vehicle Architecture (See /11/) defines the data infrastructure and this the basic exchange for information within the vehicle. It defines Ethernet in combination with the Data Distribution Service as the basis of the information exchange. Since mounted soldiers may also exchange information with the vehicle it is extremely important to also link to this volume.

2.2.2.6.4 Data Model

Volume five of the NATO Generic Vehicle Architecture (See /12/) describes the data model and the settings of the data distribution service middleware necessary to actually connect between two DDS instances and that define the features used of DDS. The data model defines the data structures shared in the bus. The data structured are derived form a domain class diagram using the MDA approach and a set of translators. To be able to update the data model independently from the STANAG it is only described how to reach and modify it.

The data model, in combination with the previous sections describes everything needed for communication within the NGVA and enter the Network in a NGVA-Compliant manner.

2.2.2.7 Audio Exchange

2.2.2.7.1 Analog 4W

Analog 4-WIRE or four-wire circuit is a two-way communications system where the two paths are arranged so that the respective signals are transmitted in one direction by only one single path of the circuit. In intercom channels, there are four wires, which are divided into 2 sets of two conductors used to create complete electrical circuit for one path.

The 4-wire circuit gets its name from the fact that a balanced pair of conductors was used in each of two directions for full-duplex operation with low crosstalk. 4-wire systems can be 4-wire balanced or 4-wire unbalanced, which means that the circuits can consist of two conductors of the same type with equal impedance or different, unequal impedance conductors. Example: digital matrix, cameras, third party systems, etc.

2.2.2.7.2 USB Audio

USB Audio is a digital audio connection used to send digital sound between computers. The following table provide the USB-IF standards for USB Audio:

USB-IF Audio Device Class Definition Rev. 3.0 https://www.usb.org/document-library/usb-audio-devices-rev-30-and-adopters-agreement	USB-IF: USB Device Class Definition for Audio Devices
	USB-IF: USB Device Class Definition for Basic Audio Functions
	USB-IF: USB Device Class Definition for Audio Data Formats
	USB-IF: USB Device Class Definition for Terminal Types

Table 2-14 – USB-IF standards for USB Audio

2.2.2.7.3 USB Eth. VoIP G.711/G.726

Voice over IP (VoIP) or IP Telephony is a group of protocols and technologies for delivering audio exchange over the Internet Protocol (IP). The VoIP standards are covered by the following standards:

- RTP, SRTP and RTCP, described in Section 2.2.2.2.1
- H.323, described in Section 2.2.2.2.2
- RTSP, described in Section 2.2.2.2.3
- SIP, described in Section 2.2.2.2.4
- SDP, described in Section 2.2.2.2.5

2.2.2.7.4 Bluetooth

Bluetooth is described in Section 2.2.2.1.3.

2.2.2.8 Communication Components

This paragraph reports the communication standards over radios typically used in the current tactical domains. For each waveform, categorized as LOS or BLOS, the main characteristics are provided, such as operative frequencies, bandwidth, modulation, typical range, WF nature (Broadcast or MANET), EPM capability and supported traffic.

Other wireless standards specific for machine-to-machine, IoT and sensors communications, adopted by civilian market, such as 802.11(Wi-Fi) family or LoRa (Long Range), could be potentially applicable to the DSS domain. Such technologies are potentially suited for operational scenarios and contexts where DSS needs to communicate with sensors in close proximity; they will not be treated in this document.

2.2.2.8.1 Line-of-Sight (LoS)

With the term “legacy” radio for DSS communications are identified all those legacy Combat Net Radios available mainly for Dismounted and Vehicular domains, as specified by the NATO STANdardization AGreement (STANAG) documents.

Other proprietary “legacy” radio communication solutions such as national-only or not standardized are not considered in this section.

Both LoS and BLoS radio communication standard systems applicable for all DSS roles are considered.

2.2.2.8.1.1 STANAG 4204 / 4205

VULOS is a VHF-UHF Line Of Sight WF capable to provide basic standard analogue voice and data communications to ensure interoperability of land, air and maritime single channel V/UHF radio equipment.

- Frequency Bands: 30-88 / 225-400 MHz with 25 KHz bandwidth
- Modulation: AM,FM, ASK,FSK
- Operative Scenario: Ground Communications, G-A-G
- Security: NATO / National Restricted
- Voice uncoded
- Data Troughput: 16 kbps
- Range: tens of kilometres
- broadcast nature (no relay capability)

2.2.2.8.1.2 STANAG 4246 (HQ I/II)

HAVE QUICK (also HAVEQUICK, or HQ) is an ECM resistant / frequency-hopping system used to protect Ground-Air-Ground radio communications. HQ WF adopts a VINSON COMSEC solution. It will be included and superseded by the next version of SATURN WF.

- Frequency Band: 225-400 MHz with 25 KHz bandwidth
- Modulation: AM
- Operative Scenario: G-A-G
- Security: up to NATO Secret
- EPM: Frequency Hopping

- Only Voice mode
- Range: tens of kilometres
- broadcast nature (no relay capability)

2.2.2.8.1.3 STANAG 4372 (SATURN ed.4)

Second generation Anti-jam UHF Radio for NATO (SATURN) is a UHF EPM WF providing plain and secure Voice and Data communications, as it further improves the jamming resistance of the Have Quick II, by means of Fast Frequency Hopping and Digital Modulation Techniques.

- Frequency Band: 225-400 MHz with 25 KHz bandwidth:
- Modulation: MSK,
- Operative Scenario: G-A-G
- Security: up to NATO Secret
- EPM: Fast Frequency Hopping
- Voice and Data mode (16kbps)
- Range: tens of kilometres
- broadcast nature (no relay capability)

2.2.2.8.1.4 STANAG 5630 Series (NATO NB ed.1)

The NATO NB is designed with an essential goal, achieving coalition interoperability within lower tactical levels. There was and currently is no ratified interoperable Combat Net Radio STANAG available that enables security and supports network centric coalition operations.

NB WF is a waveform with self-forming and self-healing capability, it is able to build a meshed networking for being mainly used in mobile sub-segment of tactical communications scenarios regardless of soldier, land vehicles or maritime vessels communications contexts. A wide set of mission parameters and configuration options enables NATO NB to be used in most missions, taking benefit of the low spectrum usage and simultaneous NB networks coexistence in battlefield.

This very high inherent versatility makes NATO NB ed.1 the convenient candidate for upgrading former communications and replacing fielded legacy radios, although some important feature, such as EPM, is not available.

- Frequency Band: 30-88 / 225-400 MHz (extendible up to 520 MHz) with 25/50 KHz bandwidth
- Modulation: CPM
- Operative Scenario: Ground Communications
- Security: NATO / National Restricted / SCIP-voice native transport
- EPM: No
- Voice (Voice Group Call management) and Data mode (up to 80 kbps)
- Range: up to 50 kilometres
- MANET: relay capability

2.2.2.8.2 Beyond Line-Of-Sight (BLoS)

2.2.2.8.2.1 "HF Home" Suite

Over the last decades the wide deploy of satellite communications relegated HF military communications as back-up technology in the same application domains, wherever the satellite resource wasn't available or un-accessible.

Modern EW makes austere environment easy to build, that's way in the last years HF coming back as an affordable and resilient way for long and very long communications (up to thousands kilometers) to provide voice and small data services at any hierarchical level. Communications nodes start from typically special role DSS up to vehicular/rotary wing/aircraft/vessel.

A set of STANAGs and mil-standard specifications as subset of "HF-Home" mil-standard description are the de-facto standard in HF transmission.

"HF Home" WFs support voice and low data-rate services

- STANAG 4285: HF Modem WF provides various Single Tone PSK Modulations up to 3.6kbps
- STANAG 4539: HF Modem WF provides various Single Tone PSK/QAM Modulations up to 12.8 kbps
- MIL-STD-188-141C: 2G ALE Automatic Link Establishment
- STANAG 4538: 3G ALE Automatic Link Establishment
- STANAG 5066: IP over HF, Data Link Layer capability for TCP/IP applications enabling applications to directly connect the HF modems

2.2.2.8.2.2 SATCOM Dedicated Ch. / DAMA

Satellite communications offer great advantages for military applications including wide (geo-stationary-satellite) area coverage with distance-insensitive cost, communication to remote areas, rapid extension to new locations; highly flexible networking, large capacity; reliable long range service to moving platforms like ships, aircraft, and vehicles up to DSS nodes.

UHF MILSATCOM has a long history enabling beyond line-of-sight communications across the battlespace and it continues to provide assured access under disadvantaged weather conditions and coverage.

Non-processed narrowband services are currently provided via transponders on selected USA UHF Follow-on and Fleet Satellites and in the last decades by several satellite fleet by other NATO and European nations.

UHF SATCOM capable radio (WF and antenna kit) is generally reserved to special role DDS member.

- SATCOM Dedicated Channel: support one voice or data up to 16 kbps
- Demand Assigned Multiple Access (DAMA) support TDMA access the satellite channel with: up to 5 voice call.

The following mil-std specifications can be considered as de-facto standards:

SATCOM Dedicated Channel / DAMA: MIL-STD-188-181A, MIL-STD-188-182A, MIL-STD-188-183

2.2.3 Standards Related to "Security View"

This section shows the standards related to the security view. They are not only used in the security view, but shall also give an idea of applicable standards to security.

Security Scope	Standard	Ref.
Information Technology — Security Techniques — Information Security Risk Management	ISO/IEC 27005	Third edition - 2018
Security Risk Assessment	MAGERIT Methodology	Version 3.0
Risk Management Framework	NIST Special Publication 800-37	National Institute of Standard and Technology - Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach
Recommended Security Controls	NIST Special Publication 800-53	National Institute of Standard and Technology - Security control selection guidance for non-national security systems
Security Controls Assessment	NIST Special Publication 800-53A	National Institute of Standard and Technology - Security control assessment procedures for security controls defined in NIST Special Publication 800-53
Information Technology -- Security Techniques -- Evaluation Criteria for IT Security	ISO/IEC 15408	Common Criteria (Vol. 1, 2, 3)

Table 2-15 – IT-Security Standards

2.3 NTV-2 Technical Standards Forecast

The purpose of the Technical Standards Forecast subview (NTV-2) is to identify **emerging**, **obsolete** and **fragile** standards, and to assess their impact on the architecture and its constituent elements.

2.3.1 Electronics Technical Standards Forecast

Service	Forecast		
	Short Term (1 Year)	Medium Term (3 Years)	Long Term (5 Years)
Data Bus (Wired)	Display Port		
	USB-C	USB 4.0	
	ISB 2.0		
	Thunderbolt 3		
Data Link (Wired)	802.3 1000BaseT		
Data Link (Wireless)	Wi-Fi 6	Wi-Fi >6	

Table 2-16 – NTV-2 Data Link Standards Forecast

2.3.1.1 Integrated Sensor Bus (ISB 2.0)

The Integrated Sensor Bus protocol has been developed as part of a research project (3DTAG and BASE) projects both funded by the Netherlands Ministry of Defence) to find a solution for the drawbacks that were identified with USB2.0 when applied to DSS systems.

- As it is expected that future DSS systems need to become capable of handling streaming sensory data with extremely low latencies (audio, video, tactile), a protocol is needed with small data packets.
- Power efficiency is crucial for DSS systems and need therefore to be a core driver in the design of the protocol.
- Instead of a tree structure as in USB 2.0, a bus structure is preferred.

The ISB2.0 protocol description is made available as open source under the GNU (LGPL) conditions which means that it is available for third parties. The protocol suite is depicted in Figure 2-5 and comprises in fact three main parts. One part is built upon LVDM that allows for power efficient, high-bandwidth data exchange with extensions to various COTS protocols to easily connect to audio, video or generic streaming channels. Another part deals with the USB 2.0 stack and handles initialisation and configuration tasks with low bandwidth requirements and one part is

responsible for power management and uses the PD (Power Delivery) functionality of USB3.1. For the connector, the USB-C is chosen, allowing for a sufficient number of concurrent connections.

Compared to USB the latency of ISB is much lower and Electro Magnetic emissions are lower.

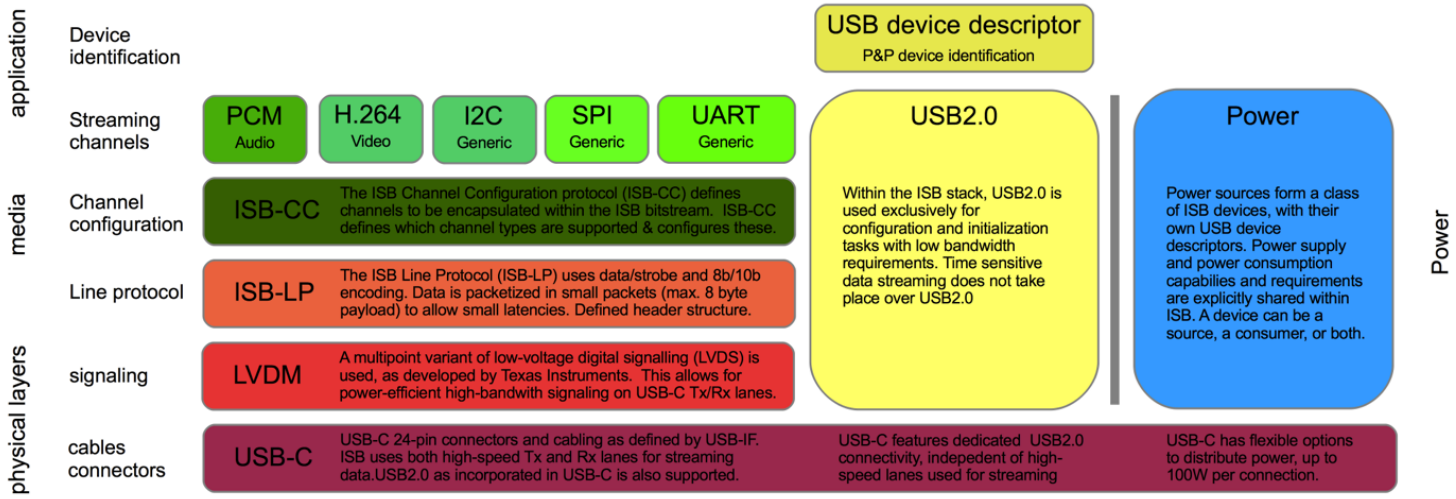

Figure 2-5 – Protocol suite of ISB2.0

2.3.1.2 DisplayPort

DisplayPort is a standard which specifies a digital interface for displays, including connectors. The latest iteration of the DisplayPort standard is version 1.4 of which initial products with support appeared on the marked in Q2 2016, whereas version 1.2a has reached widespread market availability as of Q2 2016. Due to the timing of this report, we will consider the features of version 1.4. Note that 1.4 remains backwards compatibility with respect to earlier DisplayPort standards. In practice, DisplayPort is already widespread, but has a smaller market share than HDMI. Both connectors are often seen on laptops, displays and televisions.

DisplayPort features support for resolutions up to 8K@60Hz compressed, and 8K@30Hz uncompressed. Moreover, the standard supports transporting multiple video streams over a single connector, allowing delivery to multiple display devices over a single cable. It is also possible to send DisplayPort signals over USB-C instead of over a DisplayPort cable. DisplayPort's transmission protocol is based on packets, and therefore is able to not only carry video, but also audio, USB and Ethernet data as well.

DisplayPort 1.4 supports adapters to VGA, HDMI and DVI, thereby allowing interoperability with more display devices. In a mode known as Dual-mode DisplayPort, the source device can detect the presence of a HDMI sink, and automatically adjust the output accordingly.

The DisplayPort standard was published as a royalty-free standard, however MPEG-LA claims to have patent claims to the underlying technologies. These claims are yet to be verified. The MPEG-LA license requires the payment of $0.20 per produced unit for manufacturers. Aside of the MPEG-LA claims, any manufacturer is required to become a member of VESA which will cost at least $5000.00 annually.

In a DSS, DisplayPort is suitable as an interface to displays, especially those with high resolutions. It may be beneficial to support DisplayPort in order to increase the interoperability with other

interfaces as well. Furthermore, the option to carry multiple types of signals over a single cable offers design options for a DSS where total the amount of cables can be reduced if this is desired.

2.3.1.3 Ethernet (IEEE 802.3)

Ethernet or the IEEE 802.3 is a collection of LAN (Local Area Network) standards for cabled (i.e. copper or fibre) media that define the physical layer, the data link and its MAC sublayer. The Ethernet IEEE standardization working group commenced in the early 1970s and has constantly issued updates to keep pace with improving technology and the growing user needs. A well-defined nomenclature is used, allowing for a unique identification.

The IEEE 802.3 supports the network architecture, described by IEEE 802.1. The MAC sublayer method is CSMA/CD which means that the access is not based on fixed time slots and collisions may occur during simultaneous transmission attempts. As a result, the protocol may effectively imply (re)transmission delay for low rates. Therefore, specifically for DSS application, a high rate is preferable.

The designator for describing the different forms of Ethernet consists of a three parts:

- The first number (typically one of 10, 100, or 1000) indicates the transmission speed in Mbit/s;
- The second term indicates transmission type: BASE = baseband; BROAD = broadband;
- The last number indicates segment length. A 5 means a 500-meter (500-m) segment length from original Thicknet. In the more recent versions of the IEEE 802.3 standard, letters replace numbers. For example, in 10BASE-T, the T means unshielded twisted-pair cables. Further numbers indicate the number of twisted pairs available. For example in 100BASE-T4, the T4 indicates four twisted pairs.

Different releases and variants of the standard are then designated by different designated letters after 802.3. Some recent examples may be relevant for a future wired DSS PAN (a PAN actually is described in 802.15):

- **802.3az (2010):** Energy-efficient Ethernet. This standard uses LPI (Low Power Idle), which is actually a low energy consumption state that can be used during periods where there is no link utilization.
- **802.3bq (June 2016):** 25G/40GBASE-T for 4-pair balanced twisted-pair cabling with 2 connectors over 30 m. The question for DSS application is how resilient this would be against physical deformation and wear and tear.
- **802.3bp (June 2016):** 1000BASE-T1 – Gigabit Ethernet over a single twisted pair, automotive & industrial environments, which might be more feasible for a wired DSS PAN.
- **802.3bt (2017):** Power over Ethernet enhancements up to 100 W using all 4 pairs balanced twisted-pair cabling, lower standby power and specific enhancements to support IoT applications (e.g. for DSS reading sensors or activating the weapon).

Altogether, a fibre medium may be less likely for a DSS.

IEEE 802.3 are open standards.

2.3.2 Software Technical Standards Forecast

Service	Forecast		
	Short Term (1 Year)	Medium Term (3 Years)	Long Term (5 Years)
Data Exchange Services			Information-Centric Networking Research Group (ICNRG) [/38/]
		DDS for Time Sensitive Network (DDS-TSN)	
Networking			IPv6-only

Table 2-17 – Software Technical Standards Forecast

2.3.2.1 Information-Centric Networking

Information-centric networking (ICN) is an approach to evolve the Internet infrastructure to directly support this use by introducing uniquely named data as a core Internet principle. Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication. The expected benefits are improved efficiency, better scalability with respect to information/bandwidth demand and better robustness in challenging communication scenarios. These concepts are known under different terms, including but not limited to: Network of Information (NetInf), Named Data Networking (NDN) and Publish/Subscribe Networking.

ICN concepts can be applied to different layers of the protocol stack: name-based data access can be implemented on top of the existing IP infrastructure, e.g., by providing resource naming, ubiquitous caching and corresponding transport services, or it can be seen as a packet-level internetworking technology that would cause fundamental changes to Internet routing and forwarding. In summary, ICN is expected to evolve the Internet architecture at different layers.

This family of protocols support design patterns which are critical for battlefield scenarios which involve highly dynamic and disrupted network conditions and where implementations over the TCP/IP architecture have struggled. The most relevant design patterns are: host-independent abstractions, multicast communication, pervasive network-accessible storage, opportunistic communication, namespace synchronization as transport, and data-centric security.

2.3.2.2 DDS for Time Sensitive Network (DDS-TSN)

DDS for Time Sensitive Network specifies a Platform Specific Module (PSM) of DDSI-RTPS for Time Sensitive Network transport.

This specification will improve the robustness and the effectiveness of Data Exchange Services based on the DDS protocols.

DDS-TSN is currently in the Draft status.

2.3.3 Radio Communication Technical Standards Forecast

This paragraph reports the emerging standards which will most probably be affirmed in the short and medium term period. For each waveform, categorized as LOS or BLOS, the main characteristics are provided: network sizing, traffic profile and security issues.

2.3.3.1 Line-on-Sight (LoS)

Emerging NATO and Multinational operatives scenarios such as Federated Mission Networking (FNM) framework, it is clearly stated the need of both Narrowband and Wideband LoS waveform to support the tactical domain operativity in the modern and future ORBAT.

2.3.3.2 NB Waveform

2.3.3.2.1 STANAG 5630 ed.2 Series (NATO NB ed.2)

The Edition 2 is the evolution of NATO NB ed.1 mainly with added EPM capability. For its definition, the first step will be a comprehensive update of user, operation and technical requirements as stated in the /41/.

The requirements for a NBWF cover four broad areas

- Improvement in tactical communications interoperability and flexibility of mobile land forces;
- Integration of the waveform(s) with support of NATO information assurance standards;
- To operate in contested EM environments including spectrum availability limitations and the effects of electronic warfare;
- Enhancement to Combat Identification through RBCI techniques.

The scope and level of ambition of NATO NB ed.2 is a good reference for multinational operative scenarios including the possibility of using platoons from different nations within the same company, for which communications interoperability must be assured at the platoon level. Even for different nations' companies co-located within the same battalion, DSS special role need to be able to communicate at the company level.

The NBWF requirements summarized below represent the capabilities fulfilled by NATO NB Ed.1 and define a level of ambition for Ed.2.

These requirements overcame a pure squad platoon domains giving to a DSS systems the capability to communicate within a wide set of national and multinational organizations.

NBWF Edition 1 provides:

- A secure and resilient narrowband waveform to operate on SWaP constrained platforms (e.g. hand-held radio) supporting:
  - Secure simultaneous voice and data services
  - Friendly force tracking (FFT)
  - Integration with NATO crypto and IA standards.
- Supporting multinational command, control and coordination down to company level (with an ambition to extend usage down to platoon level to allow more comprehensive subunit de-confliction between co-located multinational units)

- Operating ground to ground, air ground air and ground sea ground
- Dynamically operating on a single RF channel of 25 or 50 kHz for C2 services
- Support ranges up to 50 km
- Providing basic networking capabilities optimised to support approximately 15-20 nodes, but with possibility to support higher numbers with degraded performance

NBWF Edition 2

Base level of ambition should provide:

- All the features of Ed.1
- Operates in a moderate EM threat environment as defined in /42/
- Uses modern cryptographic standards (STaC-IS) SCIP-214.6
- Data rate capability similar to Ed.1 Fixed Frequency
- The NBWF will support the situational awareness (SA) in embedded way designed into the transport layer framing.

Enhanced level of ambition should provide:

- Operates in a severe EM threat environment as defined in the /42/.
- Provide modes/profiles with greater capacity and lower latency than Ed.1 for short range scenarios;
- Support an RBCI capability. As much as possible compatible with future RBCI standardization effort.

2.3.3.2.2 NB WF Supportable Traffic Estimation

The Ref /41/ provides supplementary information regarding the number of nodes in different nets of a brigade and the services required to support a typical military deployment. It offers an estimation of network size, typical used platforms, operative ranges and other main features in the tactical organizations including some typical traffic profiles with their attributes (latency, frequency and average size of messages).

Out of “NATO Multinational Brigade Command Net” (first column), other radio nets, starting from Battle Group (Multinational Brigates), may involve portable platforms (manpack and HH) available for DSS radio communication equipment for all roles down to the basic one.

	NATO Multinational Brigade Command Net	Battle Group Net	Battalion Net (Bt Cdr + Coy Cdrs)	Coy Net (typical 20 nodes Coy Cdr + Pt Ldrs + support)	Platoon Net	Amphibius Readiness Group Net
NB WF Operative framework						
No of Nodes	30	30-40	30-40	30-40	15-20	40
Type of Radio	Vehicle	Veh/Man	Veh/Man	Veh/Man	Veh/Man/HH	Plat/Man/HH
Area of Operation	30-50 km	20-30km	5-20 km	5-10km	1-3km	20-30km
Terrain (for channel model)	Fading	Fading	Fading / multipath	Fading / multipath	Fading / multipath	Littoral
NB WF Traffic profiles						
Voice (% of channel use)	VP3 (90%)	VP1 (50%)	VP1 (50%)	VP1 (50%)	VP3 (90%)	VP1 (50%)
SA Periodic Time Interval (one per node) - 60-bytes max - Latency < 5s	every 15min (900s)	every 5min (300s)	Variable 60-300s	variable 30-300s	variable 10-300s	variable 60-300s
SA (Aggregated/Consolidated) Latency < 10s	-	1 every 15min	1 every 60 - 100 seconds	1 every 120-300s	-	-
Chat - 100-bytes - Latency < 10s	Network Radio	Network Radio	Yes	Yes	Yes	1 message/ 120 sec
Email + attachment -Latency < 120s	Network Radio	Network Radio	Yes	Yes	No	Yes - infrequent
File transfer -Latency < 120s	NATO FMN Core Services	NATO FMN Core Services	Spiral 5 FMN Tactical	Special to types	Special to types	50kBytes infrequent

Table 2-18 – Basic dimensioning and information exchange requirements supportable by NB WF (/41/)

2.3.3.2.1 NB WF Supportable Network Dimensions

A waveform does not exist in a military deployment as only one instance. The waveform has to coexist with multiple instances as well as many other radio services that are in use. For a VHF radio system used for command and control the likely number of nets required depends on the deployment echelon. National nets (applying different waveforms organically) and NBWF nets (for interoperability) could coexist. NBWF is used on nets where different nations contribute to the same command level. E.g. a battalion net, if there are one or more companies from different nations.

Typical figures for all NBWF Networks deployment are expressed in cumulative way in the following bullets:

- Platoon: One VHF command net.

- Company: Approximately 10 nets: four platoons, company command, logistic support, reconnaissance, medical etc.
- Battalion: Approximately 30 nets: three or four companies
- Brigade: Approximately 120 nets: three or four battalions.

Worst Case: Number of NBWF Nets and National nets in the same amount of spectrum, same frequency set, 50 Watt in a 10x10 km area: 120 nets

2.3.3.2.2 NB in European Framework

The above requirements are also expected to be the input for a new NB waveform development in the European context, currently under definition.

For this reason such European NBWF is a candidate to be proposed as a NB EPM WF STANAG for NATO interoperability purposes.

2.3.3.3 WB Waveform

The intent of a WideBand Waveform (WBWF) is to focus on ground to ground, ground to air to ground and littoral communications. It is meant to complement NATO tactical airborne communication systems (i.e. SATURN STANAG 4372) and the NATO NB WF Ed.1 and Ed.2.

The WBWF should be optimized to provide interoperability between armed forces from different nations at Command Post and combat unit levels.

The WBWF does not stand alone (one waveform does all) but instead has to be considered as part of the overall architecture of a Multinational Brigade C2 and O&I (Operational and Intelligence) deployed system. In general, only special role DSS should be capable to support it. In the Tactical domain, the WBWF and the NBWF should be complementary at all echelons.

The requirements for a WBWF, as stated in the /43/, cover four broad areas:

- Improvement in tactical communications interoperability and flexibility of mobile land forces (including air and naval forces in support)
- Integration of the waveform(s) with support of NATO information assurance standards
- To operate in contested EM environments including spectrum availability limitations and the effects of electronic warfare
- Specifically, to deliver networked and internetworked FMN (Federated Multinational Networks) Services where the capabilities of the NBWF are not able to satisfy the volume and/or latency requirements

The NATO WBWF will be defined and implemented width a dual editions approach, as to the NB WF, WB Edition 1 should provide:

- A secure and resilient wideband waveform to operate on SWaP constrained platforms (e.g. vehicles, low-speed aircraft) supporting:
    - Secure simultaneous FMN Spirals 1-3 Services
    - Support modularity for future FMN Spirals 4-5 Services
    - Friendly force tracking (FFT)
    - Integration with NATO crypto and IA standards.
- Supporting multinational command, control, planning and coordination down to company level
- Operating ground to ground, low-speed ground-air-ground and ground sea ground (littoral)
- Support ranges up to 50 km (with intra-network relaying)
- With basic networking capabilities optimised to support approximately 150 nodes but with possibility to support higher [i.e. large or dense Area of Operation, up to 200 nodes] or lower [i.e. sparse, dispersed nodes within the Area of Operation] numbers with degraded performance
- Operates in a moderate EM threat environment as defined in /42/
- Uses modern cryptographic standards (NINE, STaC-IS)
- Frequency ranges: 225-400 MHz
- Voice services over I
- User data throughput up to 1Mbps

The enhanced level of ambition for Edition 2 should provide, other than edition 1:

- Operates in a severe EM threat environment as defined in /42/

- Provide modes/profiles with greater capacity, higher spectral efficiency and lower latency than Edition 1;
- Improved SWaP characteristics.
- A reduced waveform capability e.g. man-pack, UAS supporting:
- Secure simultaneous voice and limited FMN services
- Chat, interface to PLI
- Integration with NATO crypto and IA standards
- Supporting multinational operation down to platoon, and lower where justified for specialized users only
- Extended Frequency ranges: 175-520 MHz and future up to 2.5 GHz

2.3.3.3.1 WB WF Supportable Traffic Estimation

Table 1 reports the FMN user tactical services for NATO coalition operations remised in /43/. These services are consumed by National troops in the execution of NATO coalition missions.

User tactical services	Description	User level
Voice service	Voice service at the required mission classification level. Available at all level of coalition deployed forces as well as capable of connecting the team or platoon leader up to the chain of command. It can rely on a gateway to bridge different communications infrastructures.	From Battle Group commanders to team level, and across national borders. The gateway connects up the chain of command, e.g. to NATO Multinational Brigade level or above.
Tactical chat/ message service	Secure chat or messages capability on tactical devices (e.g. PDAs.) and on command component workstations. It can rely on gateway to bridge different communications infrastructures.	From Battle Group commanders down to platoon level and across national borders to enable transfer of orders and progress reports.
Video teleconference service	Video conference capability to enhance C2 of Higher level command. Secure and non-secure	Battle Group (or company) level and above, depending on their role and need. Potentially connect to elements outside the coalition forces (news media centers, etc.).
Common Operating Picture (COP) service	Single identical display of relevant operational information shared by more than one command unit.	Battle Group level and above, depending on role and need. Collect info from all different units.
Automated locations and identification service	Reports the position of every elementary units to a central repository. Can be connected to the COP.	The users are the command post staffs. The information must be collected from every elementary units, typically vehicle-size.
Targeting service	This service provides real time targeting information to dismounted soldiers, Air support or special forces.	Command post staffs, to provide targeting information to special functions such as Forward Air Controller (FAC), Special Operation Forces (SOF), platoon and dismounted soldiers. Available across national borders.
Shared ISR service	This service shares in near-real time sensor data or products to facilitate targeting or dynamic reaction to the development of the operation.	Command post staff.
Cooperative Identification service (coalition combat ID)	It enables last second cooperative identification with friendly forces in the proximity of the target area. Must be enabled across national borders.	Weapon delivery systems on ground or Air. Platoon and dismounted soldiers. Available across National borders
Combined network fires service	Ensure sufficient interoperability to permit weapon systems pairing between brigades of different Nations, and automated or semi- automated clearance of fires.	Brigades or Command Component HQ. Available across National borders

Table 2-19 – User tactical service for NATO coalition operation (Source: /43/)

2.3.3.3.2 ESSOR HDR OC1

The above requirements are covered (and mostly inherited) by the ESSOR HDR OC1 European wideband waveform which is currently under the process to be released as a WBWF STANAG for NATO interoperability purposes.

2.3.3.4 Beyond Line-Of-Sight (BLoS)

2.3.3.4.1 WB-HF

In the last years de-modulations techniques and growing digital processing capabilities allowed the specification and the implementation of higher speed modems to enrich the “HF family” modems. The reference specifications are the:

- MIL-STD-188-110D Appendix D, for Very High Data Rate modems. Single tone carrier with variable modulation and symbol rate, resulting in a variable bandwidth from 3 up to 48 KHz (up to 240kbps).
- MIL-STD-188-141D: ALE 4G

Wideband HF (WB-HF) is a mode which allows to support, when the link quality is sufficient, more than a simple voice call or very short message transferring.

This WB-HF mode is in the process to be ratified as a STANAG specification (STANAG 5069).

2.3.3.4.2 SATCOM Integrated Waveform (IW)

Integrated Waveform is an evolution of DAMA. It provides system enhancements that allow to exploit the same channels of DAMA with an increase of simultaneous voice calls, improvement of voice quality and data throughput thanks to new modulations/coding schemes.

IW standards are defined from the following MIL-STD-188-181C/182B/183B series.

Incoming ratification of STANAG specification is identified by:

The IW waveform is in the process to be ratified as a STANAG specification (STANAG 4681).

As reference performance, a single satellite channel could be configured to provide up to twenty voice communication or three 16kbps data logical channels.

2.3.3.4.3 SATCOM IW in European Framework

UHF SATCOM communications enable users to conduct secure communications under all weather conditions and cover, with usage of portable terminals suitable for DSS (with portable umbrella antenna).

Current DAMA and IW terminal solutions implies that specific US HW components must be used, unless currently restricted information was provided.

A more open and interoperable TACSAT-IW based (STANAG 4681) solution should be instead available and fully SW implementable, without any restriction.

For the above reasons an European program is going to specify and implement an European IW-Based Waveform, compliant with the open STANAG 4681. It will include an additional OrderWire (OW) encryption mode for communications up to secret.

2.3.4 Human Interface Devices Standards Forecast

2.3.4.1 Biometric Credential Standards

The more the complexity of a system grows, the more important is to grant its services only to qualified, identified and authorised personnel. The widespread approach to assess the user's identity on a single device basis, which relies on a locally installed application using locally stored PINs and passwords, is hardly sustainable for the DSS.

This is why, in addition to position tracking and health monitoring systems biometric technologies are expected to play a major role in authentication services in the near future (see /44/).

If the DSS is seen as an ecosystem of several devices, each of them possibly requiring authentication more than once during the mission, then a system to collect, assess and manage biometric credentials should be foreseen. Regardless of the system, security and privacy matters arise when dealing with sensitive information like biometrics. For example, compromised passwords can be reset, whilst compromised biometrics cannot. Once compromised, biometrics credentials can be used by anyone.

Two standard systems are the most promising for the near future, which will be briefly described in this section.

The Biometric Open Protocol Standard (see /45/, /46/) provide a mechanism to authenticate biometrics by storing data in encrypted form. Not only biometrics is encrypted, but also it is checked in encrypted form. In fact, BOPS supports fully homomorphic encryption (FHE, see /47/, /48/) so biometrics data remain encrypted during the whole authentication process (see /49/). BOPS is a vendor independent identity authentication solution specifically designed for biometrics that provides identification, access control, authentication, role gathering and auditing. BOPS is open, sharable, scalable and enables interoperability between biometric products. The protocol defines an end-to-end identity authentication platform and access control infrastructure, integrating front and backend systems and including rules that govern secure communications within those environments. Private biometrics as implemented in a system that conforms to /46/ satisfies the privacy requirements of the US Department of Defense Standard Trusted Computer System Evaluation Criteria (TCSEC).

An alternative solution is the one provided by the Fast IDentity Online Alliance (FIDO Alliance). The FIDO standard is managed by an alliance of member vendors that was formed to address the lack of interoperability among strong authentication device. In particular, the FIDO Alliance has published three sets of specifications for authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) and the Client to Authenticator Protocols (CTAP). CTAP is complementary to the W3C's Web Authentication (WebAuthn) specification; together, they are now known as FIDO2.

However, the FIDO specifications (see /50/) do not define a true end-to-end authentication infrastructure as the focus is on vendor inclusion through API specifications (see /51/) and so it looks less appealing than BOPS for GOSSRA based DSS.

3 Integrated Dictionary

3.1 Abbreviations and Acronyms

AC	Alternating Current
ACELP	Algebraic CELP
ACPI	Advanced Configuration and Power Interface
ADPCM	Adaptive differential PCM
AECTP	Allied Environment and Climate Test Protocols
AEP	Allied Engineering Publication
AES	Advanced Encryption Standard
ALE	Automatic Link Establishment
AM	Amplitude Modulation
API	Application Programming Interface
ASK	Amplitude-Shift Keying
AVC	Advanced Video Coding
BASE	Backbone Architecture for Sensory Enhancement
BLE	Bluetooth Low Energy
BLOS	Beyond Line Of Sight
BMS	Battery Management System
BOPS	Biometric Open Protocol Standard
BROAD	Broadband
BW	Band Width
CD	Coalition Domain
CE	Conformité Européenne
CELP	Code-excited linear prediction
COMSEC	Secure Communications
COP	Common Operational Picture
COTS	Commercial off-the-shelf
CPM	Continuous Phase Modulation
CPU	Central Processing Unit
CRC	Ciclic Redundancy Check
CS-ACELP	Conjugate Structure ACELP
CSMA/CD	Carrier sense multiple access with collision detection
CTAP	Client To Authenticator Protocols
CTLS	Contactless
DC	Direct Current
DCPS	Data-Centric Publish-Subscribe
DDS	Data Distribution Services
DEU	Deutschland (Germany)
DIN	Deutsches Institut für Normung
DIY	Do It Yourselve
DLEP	Dynamic Link Exchange Protocol
DNV GL	Det Norske Veritas Germanischer Lloyd (NLD)

DSS	Dismounted Soldier System
DVI	Digital Visual Interface
EBML	Extensible Binary Markup Language
EC	European Comission
ECM	Electronic Counter Measures
EDA	European Defence Agency
EEC	European Economic Community
EM	Electro Magnetic
EMC	Electromagnetic Compatibility
EPM	Electronic Protective Measures
ESP	Spain
ESSOR	European Secure SDR
ET	Ejercito de Tierra
ETSI	European Telecommunications Standards Institute
EU	European Union
EUD	End User Device
EW	Electronic Warfare
FAC	Forward Air Controller
FFT	Friendly Force Tracking
FHE	Fully Homomorphic Encryption
FIDO	Fast IDentity Online Alliance
FLAC	Free Lossless Audio Codec
FM	Frequency Modulation
FMN	Federated Mission Networking
FNM	Federated Mission Networking
FSK	Frequency-Shift Keying
GFSK	Gaussian Frequency-Shift Keying
GIF	Graphics Interchange Format
GNU	General Public License
GOSSRA	Generic Open Soldier System Reference Architecture
GSM	Global System for Mobile communications
HDMI	High-Definition Multimedia Interface
HDR	High Data Rate
HEVC	High Efficiency Video Coding
HF	High Frecuency
HH	Hand Held
HQ	Headquarters
HTTP	HyperText Transfer Protocol
HW	HardWare
IA	Authentication mechanisms
ICN	Information-Centric Networking
ICNRG	Information-Centric Networking Research Group
ID	Identification
IDL	Interface Definition Language
IEEE	Institute of Electrical and Electronic Engineers
IEM	Information Exchange Mechanism

IEMS	Integrated Element Management System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IR	Infrared
IS	Imaging Services
ISB	Integrated Sensor Bus
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific and Medical
ISOBMFF	ISO Base Media File Format
ISR	Intelligence Surveillance and Reconaissance
IT	Information Technology
ITA	Italy
ITU	International Telecommunication Union
IW	Integrated Waveform
JDSS	Joint Dismounted Soldier System
JDSSIN	Joint Dismounted Soldier System Interoperability Network
JFIF	JPEG File Interchange Format
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
LAN	Local Area Network
LCG-DSS	Land Capability Group – Dismounted Soldier Systems
LEV	Light Electric Vehicle
LGPL	Library General Public License
LIPS	Lithium-Ion Power Systems
LOS	Line Of Sight
LPC	Low Power Consumers
LPI	Low Power Idle
LSA	Lean Services Architecture
LVDM	Texas instrument multipoint LVDS
MAC	Medium Access Control
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MANET	Mobile Ad hoc Network
MCU	Multipoint Control Units
MDA	Model Driven Architecture
MDE	Ministerio de Defensa de España
MIL	Militar
MIP	Multi Interoperability Program
MISM	Motion Imagery System Matrix
MKV	Matroska
MOS	Mean Opinion Score
MOTS	Military off-the-shelf
MPEG	Moving Picture Experts Group
MQTT	Message Queuing Telemetry Transport
MSK	Minimum Shift Keying
NAK	Negative Acknowledgment

NATO	North Atlantic Treaty Organization
NAV	NATO All View
NBWF	Narrowband Waveform
NCIA	NATO (NCI Agency) Communications and Information Agency
NCV	NATO Capability View
NDEF	NFC Data Exchange Format
NDN	Named Data Networking
NEC	Network Enabled Capability
NFC	Near Field Communication
NGVA	NATO Generic Vehicle Architecture (STANAG 4754)
NISP	NATO Interoperability Standards and Profiles
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
NW	Nett Warrior
OASIS	Organization for the Advancement of Structured Information
OHSAS	Occupational Health and Safety Assessment Series
OLSR	Optimized Link State Routing
OMG	Object Management Group
ORBAT	Order of Battle
OSI	Open Systems Interconnection
OW	OrderWire
PADR	Preparatory Action on Defence Research
PAN	Personal Area Network
PC	Payload Control
PCM	Pulse-code modulation
PD	Power Delivery
PLI	Position and Location Information
PNG	Portable Network Graphics
POL	Poland
POTS	Plain Old Telephone Service
PRT	Portugal
PSK	Phase-Shift Keying
PSM	Platform Specific Model
PSTN	Public Switched Telephone Network
PU	Public
QAM	Quadrature Amplitude Modulation
QSIG	Q-Signaling protocol
RBCI	Radio-Based Combat Identification
RF	Radio frequency
RFC	Request For Comments
RGB	Red Green Blue
RGBA	Red Green Blue Alpha

RTCP	Real Time Control Protocol
RTP	Real-Time Transport Protocol
RTPS	Real Time Publish Subscribe
RTSP	Real Time Streaming Protocol
SA	Situational Awareness
SATCOM	SATellite COMmunications
SATURN	Second generation Anti-jam UHF Radio for NATO
SBDS	Smart Battery Data Specifications
SBS	Smart Battery System
SCIP	Secure Communication Interoperability Protocol
SDP	Session Description Protocol
SIG	Special Interest Group
SIP	Session Initiation Protocol
SN	Sensor Network
SOF	Special Operations Forces
SRTCP	Secure RTCP respectively
SRTP	Secure RTP
STANAG	Standardisation Agreement (NATO)
STU	Small Tactical Unit
SW	Software
SWE	Sweden
SysML	System Modelling Language
TACSAT	Tactical Satellite
TC	Technical Coordinator
TCP	Transmission Connection Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TDMA	Time Division Multiple Access
TIFF	Tag Image File Format
TLS	Transport Layer Security
TS	Transport Stream
TSN	Time Sensitive Network
UAF	Universal Authentication Framework
UAS	Unmaned Aircraft Systems
UDP	User Datagram Protocol
UHF	Ultra-High Frequency
UK	United Kingdom
UML	Unified Modelling Language
UN	United Nations
US	United States
USA	United States of America
USB	Universal Serial Bus
VESA	Video Electronics Standards Association
VGA	Video Graphics Array
VHF	Very High Frequency
VMF	Variable Message Format
VULOS	VHF-UHF Line Of Sight

WB	WideBand
WBWF	WideBand Waveform
WF	Waveform
WP	Work Package
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/ NATO AEP-4754, NGVA, Volume 1, Architecture Approach, EDITION 1, January 2018.

/10/ NATO AEP-4754, NGVA, Volume 2, Power Infrastructure, EDITION 1, January 2018.

/11/ NATO AEP-4754, NGVA, Volume 3, Data Infrastructure, EDITION 1, January 2018.

/12/ NATO AEP-4754, NGVA, Volume 5, Data Model, EDITION 1, January 2018.

/13/ NATO AEP-4754, NGVA, Volume 7, Verification and Validation, EDITION 1, January 2018.

/14/ NATO AEP-76, VOL. 1 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security (STANAG 4677) Edition A

/15/ NATO AEP-76, VOL.2 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) Data Model (STANAG 4677) Edition A

/16/ NATO AEP-76, VOL.3 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Loaned Radio (STANAG 4677) Edition A

/17/ NATO AEP-76, VOL.4 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism (STANAG 4677) Edition A

/18/ NATO AEP-76, VOL.5 Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access (STANAG 4677) Edition A

/19/ DefStan 23-09 Generic Vehicle Architecture, Draft Issue 3, part 5 - Data Model, October 2011

/20/ Object Management Group (2015), “Real-Time Data Distribution Services”, Issue 1.4, 04/ 2015

/21/ OMG, “The Real-time Publish-Subscribe Wire Protocol DDS Interoperability Wire Protocol Specification – version 2.2” , 11/2014

/22/ Extensible and Dynamic Topic Types for DDS Specification, Version .1.2, September 2017

/23/ Interface Definition Language, Version 4.2, March 2018

/24/ Schulzrinne, H., Casner, S., Frederick, R. and V. Jacobson,"RTP: a transport protocol for real-time applications", RFC 1889, January 1996.

/25/ MIL-STD-6017 – Variable Message Format

/26/ www.omg.org/mda - OMG Model Driven Architecture

/27/ www.omg.org/uml - OMG Unified Modeling Language

/28/ ITU, H.323, "Packet Based Multimedia Communications Systems" , Feb 1998

/29/ H. Schulzrinne, A. Rao, R. Lanphier, et al., "Real Time Streaming Protocol (RTSP)", RFC 7826, December 2016

/30/ M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, RFC2543, "SIP : Session Initiation Protocol", March 1999

/31/ MoD UK, “Lean Services Architecture Specification”, V2, June 2015

/32/ J. Postel, “Transmission Control Protocol”, RFC 793, September 1981

/33/ J. Postel, “User Datagram Protocol”, RFC 768, August 1980

/34/ J. Postel, “Internet Protocol”, RFC 791, September 1981

/35/ T. Clausen, C. Dearlove, P. Jacquet, U. Herberg, RFC 7181, “The Optimized Link State Routing Protocol Version 2”, April 2014

/36/ S. Ratliff, S. Jury, D. Satterwhite, R. Taylor, B. Berry, RFC 8175, “Dynamic Link Exchange Protocol (DLEP)”, June 2017

/37/ S. Deering , R. Hinden , RFC 8200, Internet Protocol, Version 6 (IPv6) Specification, July 2017

/38/ Information-Centric Networking Research Group (ICNRG), https://irtf.org/icnrg

/39/ van Wijngaarden, Lessons learned from National Technology Project BASE (Backbone Architecture for Sensory Enhancement), internal GOSSRA presentation, 2018

/40/ Net Warrior Interconnect Architecture White Paper, NWPAN-WP-01112013 (2017)

/41/ AC/322(CP/1)N(2019)0027: Requirements for a Coalition Tactical Radio Waveform (Narrow Band Waveform -NBWF)

/42/ NCIA NCIA/TR/2018/NCB012810/ 02: Electronic Warfare Threats to Radio Communication Systems in VHF and UHF Bands, CASINI Enrico, OZEN Serdar, LTC LOFFREDI Fabio, PENNEL Bruce, March 2019

/43/ AC322(CP1)N(2019)0028: Op Requirements for a Coalition UHF Tactical Radio Waveform (WideBand Waveform -WBWF) STANAG xxx Series (NATO NB ed.2)

/44/ Global Biometrics and Mobility Report, market Analysis and Forecasts 2016-2022, ed. 2017

/45/ Biometric Open Protocol Standard (BOPS), IEEE 2410-2016 ed. 2017

/46/ BOPS III, IEEE 2410-2018

/47/ Private Biometrics (link: https://en.wikipedia.org/wiki/Private_biometrics, last accessed June 2019)

/48/ Homomorphic Encryption (link: https://en.wikipedia.org/wiki/Homomorphic_encryption, last accessed June 2019)

/49/ Streit, et al. – Privacy-Enabled Biometric Search (2017)

/50/ Fast IDentity Online Alliance (FIDO Alliance) (web site link: https://fidoalliance.org/, last accessed June 2019)

/51/ Hoyos Labs – Identity Authentication white paper (2015)

/52/ MIL-DTL-38999 Rev. M

/53/ USB 3.2 Specification (September 2017)

/54/ USB 2.0 Specification (December 2018)

/55/ BLUETOOTH CORE SPECIFICATION Version 4.2 (or Higher)

/56/ NFC Logical Link Control Protocol Technical Specification

/57/ NFC Simple NDEF Exchange Protocol Technical Specification

/58/ ITU H.264 (Version 13) Advanced video coding for generic audiovisual services (2019)

/59/ ITU H.265 (Version 6) / ISO/IEC 23008-2: High efficiency video coding (2019)

/60/ ISO/IEC 14496-14 (2003)

/61/ Matroska Specification (https://www.matroska.org/technical/index.html)

/62/ Free lossless audio codec specification (https://xiph.org/flac/format.html)

/63/ ISO/IEC 13818 (2000)

/64/ ITU-T G.711 (2000)

/65/ ISO/IEC 10918-5 (1994)

/66/ IETF RFC 2083 (1997)

/67/ TIFF Specification Revision 6.0 (1992)

/68/ Luminact and 2iC: Supporting the development of the Australian Generic Soldier Architecture: 005 - Middleware Study, Version 2.0, 2019

/69/ Asaduzzaman, Chidella and Mridha: A Time and Energy Efficient Parking System Using ZigBee Communication Protocol, 2015

/70/ OASIS: MQTT Version 5.0, 2019

/71/ IETF: RFC 4566 - SDP: Session Description Protocol