GOSSRA

Generic Open Soldier System Reference Architecture

Collaborative Project

PADR_FPSS_A_2017_800783

GOSSRA Architecture for Standardisation - Vol. 3

Operational View (NOV)

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.

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

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

1 Overview and Summary Information

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

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

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

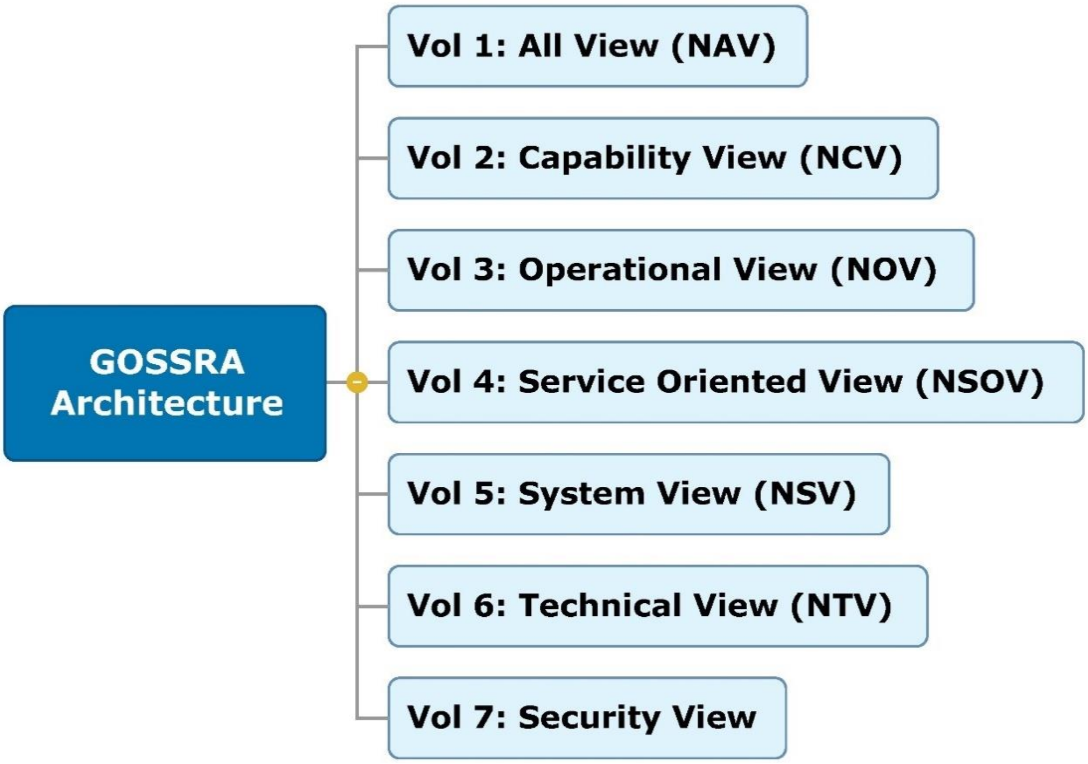
GOSSRA Architecture
Vol 1: All View (NAV)
Vol 2: Capability View (NCV)
Vol 3: Operational View (NOV)
Vol 4: Service Oriented View (NSOV)
Vol 5: System View (NSV)
Vol 6: Technical View (NTV)
Vol 7: Security View

Figure 1-1 – GOSSRA Document Structure

This for Soldier Systems was developed based on following assumptions:

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

1.1 Architecture Scope

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

This Reference Architecture comprehensively focuses on:

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

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

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

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

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

1.2 Identification

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

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

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

Following are the GOSSRA project team members:

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

  - Mazzulli Vanessa (Technical Expert)
  - Zamburru Lorenzo (Technical Expert)

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

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

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

Special thanks for their feedback and contributions.

2 Operational View

2.1 NOV-1 High Level Operational Concept Description

2.1.1 Dismounted Soldiers in the Battlefield

The purpose of the High-Level Operational Concept Description sub-view, depicted at Figure 2-1, is to provide a quick, high-level description of operations, and its context to the architecture to senior-level decision makers. The underlying concept is that, at every level, the boots on the ground using modern soldier systems provide the cutting edge to any force, which may be the difference between defeat and victory.

The operational environment depicted is in terms of operational elements involved, geographic regions, nodal connectivity, types of forces, etc. which provides a description of the key operational elements and their interactions. Operational elements imply internal or external systems, organisational units, weapons systems, or other resources.

The concept of simultaneity of operations at different theatres of operations enabled through the conduct of NCO and the common entity of the infantry soldier is depicted to highlight the universality of ultimately having boots on the ground or the contact with the enemy to ensure support or complete any operation.

The illustration depicts operations during day or night, in varied weather and terrain conditions such as:

- desert areas with extremely hot temperatures by day and below zero by night,
- arctic and/or mountainous areas with permanent snow /frost, high intensity winds or storms,
- humid areas like moors, forests, rainforests, coastlines and rivers
- urban areas with its street canyons predestined for ambush attacks, and
- moving and fighting by night, which requires night vision equipment to enable orientation and reconnaissance.

Various types of terrain require different mobility means, which are shown in the illustration as:

- Ground vehicles (wheeled or tracked),
- Amphibious vehicles (capable of flotation/hover)
- Rafts, boats or assault boats,
- Aircraft, helicopters or drones,
- Skis, sledges, etc.

Besides the enemy, other factors may also be posing a threat to the dismounted soldier such as:

- dangerous animals
- insects,
- bacteria and viruses
- weather / air pollution

The **High-Level Operational Concept** illustrates that firstly, NCO/joint operations are conducted simultaneously at all levels – strategic, operational and tactical, however, at each level the decisive component are the troops engaged in combat, troops whose fighting efficiency and effectiveness can be enhanced by providing them with a state-of-the-art soldier system.

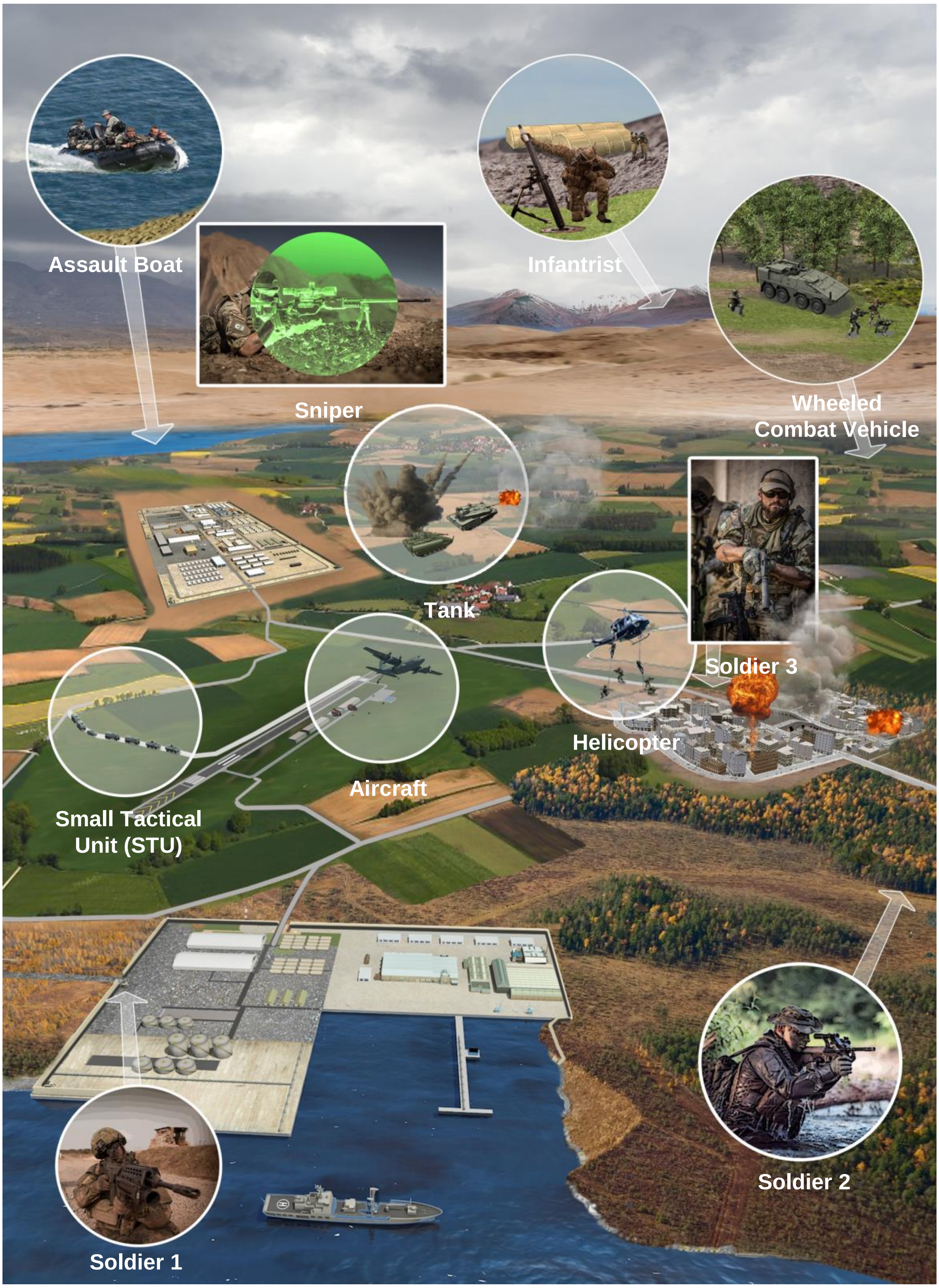

Figure 2-1 – High Level Operational Concept Description

2.1.1.1 Illustration of Dismounted Soldiers in MOUT (Military Operations in Urban Terrain)

Dismounted Soldier Systems (DSS) are employed traditionally outside of cities but, during the last century, soldiers are increasingly drawn into missions inside big cities. Fighting inside cities is extremely challenging, Figure 2-2 illustrates the activities of urban warfare referred to as MOUT and its operational requirements for a DSS.

The Figure depicts a combined tactical force of infantry and mechanised elements of two companies (one held in reserve and the other deployed in platoon and STU combat teams) attacking the enemy in an urban area. Leading the attack are three light tanks which provide the fire power and protection to the follow-on mechanised infantry in infantry fighting vehicles (IFVs) and the dismounted infantry. The soldiers of the infantry are fighting dismounted using the protection of tanks and IFVs and when mounted in their IFVs can move quickly against light opposition. In certain scenarios of high risk to the infantry, the platoon may fight partly mounted and partly dismounted with the ability to switch when necessitated by operational circumstances.

The configuration of a built-up area allows the enemy multiple opportunities to surprise own forces either through carefully laid ambushes with obstacles like mines, IEDs covered by anti-tank and /or sniper fire or through lures into narrow defiles and then neutralising or immobilising the leading tank to halt progress and inflict casualties. It is for this reason that situational awareness in real time or near real time becomes an important operational requirement.

In case of a multi-national force it is imperative that radio systems, data protocols and syntax are compatible for sharing the Common Relevant Operational Picture (CROP), which is critical to ascertain own and enemy positions and identify friend and foe in order to prevent fratricide of own troops and collateral damage to property / innocent civilians, who may be hostage or in close vicinity of enemy targets.

The operational capabilities and functions required while fighting in built up areas have been shown in the boxes in the Figure, however “reliable and fast radio communication”, “automatic blue-force tracking’’ and “sensors for intelligence and reconnaissance” are top level operational functionalities leading to system and hardware requirements in a DSS.

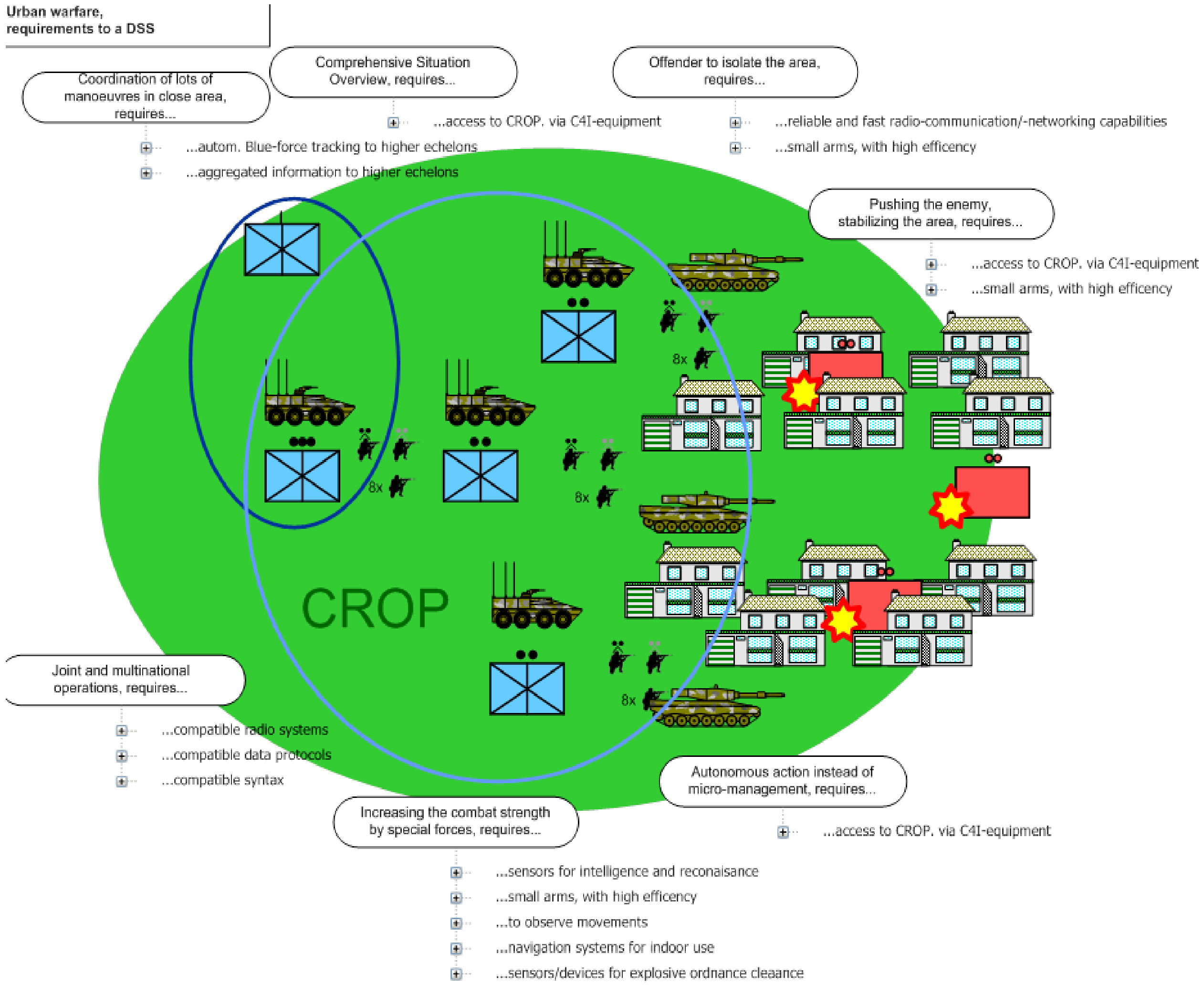
Urban warfare, requirements to a DSS
Coordination of lots of manoeuvres in close area, requires...
...autom. Blue-force tracking to higher echelons
...aggregated information to higher echelons
Comprehensive Situation Overview, requires...
...access to CROP. via C4I-equipment
Offender to isolate the area, requires...
...reliable and fast radio-communication/-networking capabilities
...small arms, with high efficency
Pushing the enemy, stabilizing the area, requires...
...access to CROP. via C4I-equipment
...small arms, with high efficency
8x
8x
8x
8x
8x
CROP
Joint and multinational operations, requires...
...compatible radio systems
...compatible data protocols
...compatible syntax
Autonomous action instead of micro-management, requires...
...access to CROP. via C4I-equipment
Increasing the combat strength by special forces, requires...
...sensors for intelligence and reconaisance
...small arms, with high efficency
...to observe movements
...navigation systems for indoor use
...sensors/devices for explosive ordnance cleaance

Figure 2-2 – Operational Concept of DSS in Urban Terrain: Dismounted Motorised/Mechanised Infantry Supported by Tanks and Infantry Fighting Vehicles

2.1.1.2 Applicability of Dismounted Soldiers to Infantry, Mechanised Infantry and Special Forces

The intensity of infantry soldiers' activities with arms impacts his / her vulnerability, due to the nature of operations he/she has to undertake. It is therefore important to empower and protect them with a state-of-the-art soldier system.

Soldier systems are primarily used by the infantry or mechanised infantry or special forces of the military and police. As an example, in Germany, the forces which use a complete modern soldier system are:

- **Infantry:** The branch of a military force that fights on foot. As the troops who are intended to engage, fight, and defeat the enemy in face-to-face combat, they bear the brunt of warfare and typically suffer the greatest number of casualties.
- **Mechanized Infantry:** infantry equipped with Armoured Personnel Carriers (APCs) or infantry fighting vehicles (IFVs) for transport and combat.
- **Airman Infantry:** The purpose is ground based defence of air force bases and installations, as well as capturing and securing enemy air installations.
- **Naval Infantry (Marines):** Force that specializes in the support of naval and army operations on land and at sea, as well as the execution of their own operations.

Assuming that the majority of branches - already equipped and to be equipped in future - are the light and the mechanized Infantry, the architecture focusses on the mission related requirements of these two branches. Mission-related commonalities and differences between both branches are described in Figure 2-3 and Figure 2-4 respectively.

LIGHT INFANTRY
(FOOT/AIR ASSAULT/AIRBORNE)

- EMPLOYED IN INACCESSIBLE /ALL TYPES OF TERRAIN
- PARACHUTE DROPPED BY AIRCRAFT INTO BATTLEZONE
- HELICOPTER TRANSPORTATION AND RAPPEL
- MARCH/VEHICLE TRANSPORTED TILL FORWARD ASSEMBLY
- LACK HEAVY WEAPONS AND ARMOUR
- RAPID ACTION TO SEIZE AND HOLD KEY TERRAIN
- SENSITIVE TO WEATHER CONDITIONS
- LACK SUPPLIES FOR SUSTAINED OPERATIONS
- PROVIDE PSYCHOLOGICAL ADVANTAGE BY VERTICAL ENVELOPMENT OF DEPLOYED ENEMY
- SUCCESSFUL IN WWII, VIETNAM, AFGHANISTAN, RRF

Figure 2-3 – Characteristics & Role of Light Infantry

MECHANISED INFANTRY

- ARMOURED PERSONNEL CARRIER(APCs) OR INFANTRY FIGHTING VEHICLES (IFVs) BASED
- APC/IFV HAS HARD PROTECTION (AGAINST SMALL ARMS/SPLINTERS)
- USE ANTI-TANK MISSILES / MOUNTED GUN
- POSSESS HIGH CROSS COUNTRY MOBILITY AND FIRE POWER
- CAN FIGHT IN THE DISMOUNTED OR MOUNTED ROLE
- USUALLY SUPPORT MECHANISED FORCES IN COMBAT GROUPING IN BATTLE
- PROVIDE PROTECTION TO FOOT INFANTRY IN MOUT OPERATIONS

Figure 2-4 – Characteristics & Role of Mechanised Infantry

Depending on the conflict, operations may also be asymmetric which implies perfidious attacks in unknown terrain and attrition. Light Infantry (LI) would normally be employed in no-go areas for tracked or wheeled vehicles. This implies that, mobility of LI in such terrain should not be hampered by vehicle dependent bulky components or high Size, Weight and Power (SWaP) requirement DSS.

Other operational requirements could be the need to provide air and sea worthiness, augmented strength and mobility to the LI Soldier Systems to enable small tactical units to achieve greater mobility even when they operate self-contained and have to carry all necessary equipment in man-portable loads or assault boat loads.

2.1.2 Underlying Concepts of Military Operations

2.1.2.1 Doctrinal Levels of War

At the outset of obtaining a NATO Operational View of the architecture for a dismounted soldier system, it is important to understand the concept of military operations at all its doctrinal levels – Strategic, Operational and Tactical and the forms of warfare therein. Figure 2-5 below depicts the three doctrinal levels of network - enabled military operations of a national/multi-national force which are elaborated in the succeeding sections.

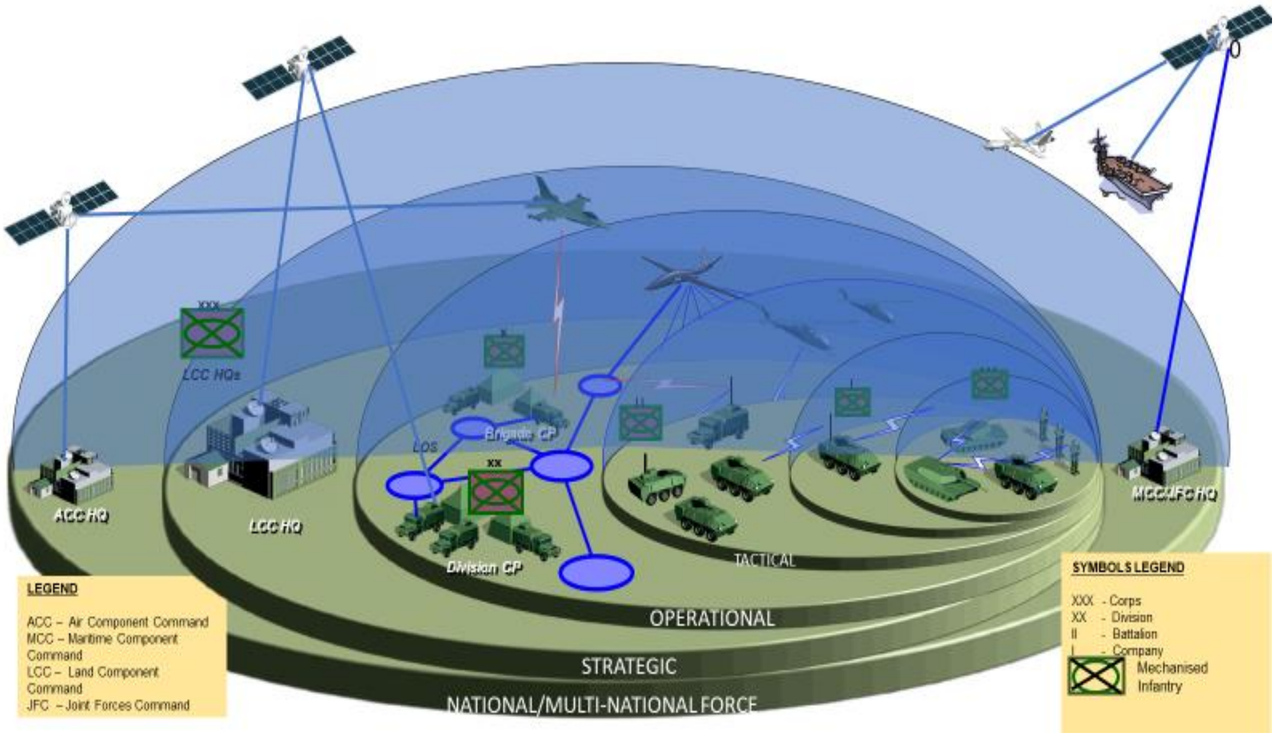

Figure 2-5 – Doctrinal Levels of Network-Enabled Joint MNF Operations

2.1.2.2 Strategic Level

Operations at the strategic level implies the strategy (planning, coordination and direction) adopted by a joint multi-national or national force to achieve the overall political and military objective. Military Strategy is usually at the level of at least a Command, generally comprising all Service components (Army, Air Force, Navy and Special Forces/Marines). Each Service, may comprise all arms components e.g. in an Army Command the arms components are Infantry and Armoured Corps/Divisions; support arms components are Artillery, Air Defence, Signals, Engineer Regiments and services components are Ordnance, Supply, Repair and miscellaneous logistic services battalions /units.

Similarly, strategic depth implies the depth attainable through operations by a Theatre (Command) sized or equivalent force level to maintain sufficient distances between the front lines of battle and the industrial core areas, capital cities, heartlands and major population centres.

2.1.2.3 Operational Level

The operational level of war is the level at which campaigns and major operations are conducted and sustained to accomplish strategic objectives within theatres or areas (Corps or Division area of operations). It links the tactical employment of forces to strategic objectives.

A major operation is a series of tactical actions (battles, engagements, strikes) conducted by various combat forces of a single or several services, coordinated in time and place, to accomplish operational, and sometimes strategic objectives in an operational area. These actions are conducted simultaneously or sequentially under a common plan and are controlled by a single commander.

The focus at this level is on operational art, the use of military forces to achieve strategic goals through the design, organization, integration, and conduct of theatre strategies, campaigns and major operations. The force level is generally a Corps (2-4 Division) or Division (2-4 Brigades) and/or an independent Brigade (2-4 Regiments/Fighting Units).

2.1.2.4 Tactical Level

A tactical engagement is a small tactical conflict between opposing forces, usually conducted at brigade level and below. Engagements are usually short in minutes, hours, or a day. Tactics is also the realm of close combat, where friendly forces are in immediate contact and use direct and indirect fires to defeat or destroy enemy forces and to seize or retain ground.

Exposure to close combat separates Army forces from most of their counterparts. Army forces fight until the purpose of the operation is accomplished. Because of this, they are organized to endure losses, provided with combat service support (CSS) to generate and sustain combat power, and trained to deal with uncertainty.

The result of a tactical battle may outweigh the size of the conflicting forces and small tactical gains achieved, often result in strategic outcomes. It is in this realm of dismounted soldier combat that DSS would be utilised most often and hence, also the reason that the infantry soldier’s exposure to risk is minimized and his chances of victory optimized by providing him/her with a capable DSS.

2.1.2.5 Network Centric Operations

The linkages between the three levels of strategic, operational and tactical operations is obtained through the operational concept of Network Centric Operations (NCO). The linkages between the three levels of military operations is obtained through the operational concept of Network Enabled Capability (NEC), which is related to the US concept of network-centric warfare (NCW) – later renamed as Network-Centric Operations (NCO) to encompass operations other than war (e.g. Peace Keeping). NCO has three domains – Physical, Information and Cognitive, which describe the implicit multi-dimensional relationship between all entities of the Force, wherein the DSS would be fielded as an entity in the battlespace.

The Physical Domain implies that all elements of the Force are robustly networked achieving seamless connectivity & interoperability;

The Information Domain implies that the Force has the capability to share, assess & protect information to a degree that it can maintain information advantage over an adversary through the process of correlation, fusion and analysis; and;

The Cognitive Domain means that the Force has ability to develop high degree of awareness and share it; Cognitive also implies development of a shared understanding, including the commander’s intent.

NCO allows simultaneity or enables simultaneous operations to be carried out at the strategic, operational and tactical levels; and through it, delivers increased synergy. In the context of the DSS, connected as an operational entity, it empowers the dismounted soldier or the key element of "boots on the ground," to deliver success through the benefits of better synchronised effects in the battle space; greater speed of command; increased lethality, survivability & responsiveness; resultantly, diminishing the adversaries' courses of action.

2.1.2.6 Multi-national Operations

Multi-national operations are conducted within the structure of an alliance (the result of formal agreements between two or more nations for broad, long-term objectives which further the common interests of the members) or a coalition (an ad hoc arrangement between two or more nations for common action).

Military alliances, such as the North Atlantic Treaty Organization (NATO), may afford participating nations time to establish formal, standard agreements for broad, long-term objectives. Alliance members strive to field compatible military systems, establish common procedures, and develop contingency plans to meet potential threats in a fully integrated manner. A multinational force commander faces many complex demands. These may include dealing with cultural issues, interoperability challenges, and an immature theatre C2 organization. Commanders may also be required to address different national procedures, the sharing of intelligence, and theatre support functions.

Since coalition operations are not structured around standing agreements, a preliminary understanding of the requirements for operating with a specific foreign military may occur through peacetime military engagement. These developmental activities include, but are not limited to, ongoing personal contacts, pre-positioning of equipment, exercises, exchange programs, and humanitarian assistance.

Commanders have to accommodate differences in operational and tactical capabilities among multinational forces. For example, not all armies have the staff structures or means to process, reproduce, or rapidly disseminate plans and orders. Decision authority delegated to staffs and subordinate commanders also varies among armies.

The commander's intent and concept of operations must be clearly and simply articulated to avoid confusion resulting from differences in doctrine and terminology. Integrating indirect fires, naval surface fires, close air support, interdiction, and information operations requires common manoeuvre and fire support coordinating measures (FSCMs). All elements of the force must fully understand and strictly adhere to them. Detailed war-gaming, planning, and rehearsals help develop a common understanding of the operation plan and control measures. Operational and tactical plans address recognition signals, FSCMs, air support, communications, and liaison.

The collection, production, and dissemination of intelligence are major challenges in a multinational operation. There are many instances in which direct access to finished intelligence, raw data, source information, or intelligence systems is not allowed outside national channels. Multinational partners also normally operate separate intelligence systems to support their own policy and military forces. These national systems may vary widely in sophistication and focus. However, at a minimum, each nation contributes valuable human intelligence to the multinational effort. Commanders establish systems that maximize each nation's contribution and provide an effective intelligence picture to all units. Commanders arrange for the rapid dissemination of releasable intelligence and the use of available intelligence assets by all partners. A multinational intelligence staff at the headquarters facilitates integration of intelligence efforts.

Mission assignments of multinational units should reflect the capabilities and limitations of each national contingent. Some significant factors are relative mobility and size; intelligence collection assets; and long-range fire, Special Operations Forces (SOF), and organic Combat Support Services (CSS) capabilities. The ability to contribute to theatre air and missile defence, training for operations in special environments, and preparing for defensive operations involving weapons of mass destruction is also important. Rapport with the local population, language considerations, and special skills should be considered as well. Multinational commanders may assign host nation forces home defence or police missions, such as rear area and base security. They may also entrust air defence, coastal defence, or a special operation to a single member of the multinational force based on the special capabilities of that force. The national pride of multinational partners is an important intangible factor that is considered when assigning missions. Commanders analyse the mission's peculiar requirements so they can exploit the advantages and compensate for the limitations of a multinational force.[1]

In summary, some of the key operational issues warranting coordination in NCO are mentioned below:

- **C4ISTAR**: The theatre or joint theatre C4ISTAR is generally not so well developed and fine-tuned. Different nations have different C4ISTAR structures and resources. Even if coordination has happened during peace the system is not really tried out until exposed to the vagaries of an active operation. Decision authority delegated to staffs and subordinate commanders also varies among armies.
- **Intelligence:** Multinational partners also normally operate separate intelligence systems to support their own policy and military forces. These national systems may vary widely in sophistication and focus. However, at a minimum, each nation contributes valuable human intelligence to the multinational effort. Commanders establish systems that maximize each nation's contribution and provide an effective intelligence picture to all units.
- **Operational & Tactical Capability**: Differences in organisational resources, operational and tactical capabilities like means to process, reproduce, or rapidly disseminate plans and orders need to be identified and understood by the Joint Forces Commander (JFC). Mission assignments of multinational units should reflect the capabilities and limitations of each national contingent. Some significant factors are relative mobility and size; intelligence collection assets; and long-range fire, Special Operations Forces (SOF), and organic Combat Support Services (CSS) capabilities
- **Commander’s Intent**: Commander’s intent and concept of joint multinational operations must be clearly and simply articulated using joint terminology
- **Integrated Fire Support**: Integrating indirect fires, naval surface fires, close air support, interdiction, and information operations requires common manoeuvre and fire support coordinating measures (FSCMs).
- **Joint Training**: Detailed war-gaming, planning, and rehearsals help develop a common understanding of the operation plan and control measures. Operational and tactical plans address recognition signals, FSCMs, air support, communications, and liaison.

The national pride of multinational partners is an important intangible factor that is considered when assigning missions. Every multinational operation is different. Commanders analyse the mission's peculiar requirements so they can exploit the advantages and compensate for the limitations of a multinational force.

[1] https://www.globalsecurity.org/military/library/policy/army/fm/3-0/ch2.htm#par3-1; NATO JP 3-16.

2.1.2.7 Swarming Operations

2.1.2.7.1 Definition and Concepts

The rise of advanced information operations will bring swarming to the fore, establishing a new pattern in conflict. This concept derives insights from examples of swarming in nature and in history. Both areas are plenty of examples of omnidirectional yet well-timed assaults. From ants and bees and wolf packs, to ancient Parthians and medieval Mongols, swarming in force, or of fire, has often proven a very effective way of fighting.

From a military conflict viewpoint, swarming can be defined as a seemingly amorphous, but deliberately structured, coordinated, and strategic way to strike from all directions simultaneously, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions.

Swarming will work best, and perhaps will only work, if it is designed mainly around the deployment of myriad, small, dispersed, networked manoeuvre units which also act as sensory organization in the battlespace and provides for stealthy ubiquity.

It depends completely on nimble information operations enabling swarm forces communication and coordination.

This puts a premium on robust, adaptive communications that help with both the structuring and distribution of information which enable swarm force to engage the enemy most of the time—a key aspect of swarming.

2.1.2.7.2 Swarming Operations Tenets

Swarming has two fundamental operational needs:

- **Sustainable pulsing,** which is the capability to strike at an adversary from multiple directions, via a large number of small units of manoeuvre that are tightly *networked*—i.e., that can communicate and coordinate with each other at will, and are expected to do so.
- **Ubiquitous sensing,** which is the additional capability for a swarm force to provide the surveillance and synoptic-level observations necessary to the creation and maintenance of "top-sight."

These two fundamental requirements may necessitate creating new approach to (i) Information Operations, and (ii) systems for command, control, communications, computers, and intelligence (C4I), as described below.

Sustainable Pulsing

If the informational needs of a swarming military force can be fulfilled, then it will be possible to undertake the "signature" act of a swarm: the "sustainable pulsing" of forces and/or their fire. This essential notion consists of the ability of swarms, who take their positions in a dispersed fashion, to repeatedly strike the adversary—with fire or force—from all directions simultaneously, then to separate from the attack, re-disperse to blanket the battlespace, and repeat the cycle as battle conditions require.

Command & Control Delegation

Sustainable pulsing requests for the devolution of a great deal of command and control (C2) authority to a large number of small manoeuvre units. These units will be widely dispersed throughout the battlespace and will likely represent all the various sea, air, and ground services—putting a premium on inter-service coordination for purposes of both sharing information and combining in joint "task groups."

C2 delegation requires for a communication system which is adaptive, decentralized, and interoperable.

Stealthy Ubiquity

The swarm force will be stealthier, since its order of battle will be characterized by amorphousness, at least to the eyes of the enemy. The small size and dispersed deployment of its units of manoeuvre will help to convey an image simultaneously stealthy and ubiquitous—a kind of "stealthy ubiquity." Thus, the force will be largely unseen and undetectable, but it will be able to congeal and strike decisively anywhere in the battlespace—with no limitation imposed by lines or fronts. Indeed, there may be no "front" per se. This is the potential of a swarming force, whose basic tenets must be to pursue centralized strategic control while at the same time decontrolling tactical command, dispersing units, and redesigning logistics.

Ubiquitous Sensing

To perform a sustainable pulsing and obtain stealthy ubiquity, the swarm units must not only be networked with each other, but also must coordinate and call upon other assets in the area. To achieve this, swarming depends upon the operation of a vast, integrated sensory system that can selectively distribute both specific targeting information and overall top sight about conditions in and around the battlespace. The swarming will turn the military into a “sensory organization" consisting of networked operational units.

As sensory organization, the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) system may generate so much information that it will be necessary to come up with new ways to segregate the often time-urgent need of the operational unit from the higher command's need to retain clear "top-sight"—a "big picture" view of what is going on.

2.1.3 Trends in Operational Scenarios

To be able to envisage the current and likely future operational needs required to be incorporated in the DSS architecture, it is imperative that we keep abreast of operational trends. The current and near future security environment and conflict scenarios would be characterised by the following operational trends:

- Shift from large scale conventional conflicts requiring air power, artillery, tanks, mechanised vehicles etc. to asymmetric conflicts requiring small mission oriented tactical teams and STUs in predominantly infantry like roles.
- Operations would be short, swift, efficient (minimal use of force), effective (increased lethality), with minimum collateral damage (accurate intelligence /precision strike) and of rapid intensity at the battle space level.
- The battle space environment will be dynamic and unpredictable, where simultaneous engagement may be necessary at different levels (Strategic, Operational, and Tactical) as well as simultaneity of air land and sea-based operations.
- Combined and mixed operations using multi-national military, police, civilian experts, NGOs, media and other international observer and relief organisations would be the norm.
- Asymmetric or Hybrid warfare will entail fighting an invisible enemy (merged with the local civilian population) with no clear boundaries of conflict. Soldiers using DSS would be faced with a myriad of asymmetric threats like IEDs, Human Bombs, Civilian Population Shields, Terror, or perfidious attacks in unknown terrain from unknown sources and environment.
- Unmanned Warfare would be the trend using a variety of unmanned sensors, unmanned ground/water/under-water systems, unmanned aerial vehicles (UAVs) and unmanned aircraft systems (UAS).

2.1.4 Trends in Threats to a Dismounted Soldier in the Battle Space

The spectrum of threat likely to be faced by the dismounted soldier during operations include the following:

- Increased lethality and precision of ordnance, ammunition and smart munitions;
- Minefields/reactive minefields, trip wire initiated directional anti-personnel mines, and obstacles designed to hinder mobility - covered by enemy fire;
- Unmanned ground sensors, unmanned armed platforms, unmanned aircraft systems or small unmanned aircraft system (UAS) like swarm UAVs with improvised explosive devices (IEDs);
- Tactical CBRN, DEW (Laser / Heat Energy) Weapons Systems
- Electronic Warfare and Cyberwarfare (resulting in loss of data and/or access to own tactical and communications networks or GPS);
- Asymmetric threats like IEDs, human bombs, civilian population shields, terror, etc.;
- Battle stresses due to fear of death/permanent disability/serious injury, fear of the unknown, being attacked any time, seeing comrades become casualties, noise, inclement weather, loneliness, etc.;
- Getting disoriented and lost, disconnected or separated from comrades and not knowing what to do next;
- Psychological warfare waged by adversary governments through bought out media, propagating the uselessness of fighting wars for political and not reasons of national interest.
- Threat from aggressors who mingle and merge with innocent civilian population, thereby preventing engagement by keeping own forces in a doubt or dilemma.

2.1.5 Missions Types and Intensity

The types of mission, role of the dismounted soldier and intensity of infantry soldiers' activities during operations varies from safeguarding of say installations / facilities, camps and personnel, to attacking the enemy with a platoon or STU - to a hand-to-hand combat. The dismounted soldier unit may be deployed in a variety of missions, whose intensity would vary depending on the nature and type of the mission.

Broadly speaking, the types of military missions in order of intensity may be categorised into *Combat*, *Humanitarian* and *Permanent Missions,* as mentioned below:

2.1.5.1 Combat Missions

Combat Missions may be offensive or defensive in nature and generally involve exchange of fire and/or contact with the enemy and carry a high risk of injury / death.

Offensive Combat Missions listed in the US Field Manual 100-5 are:

- Movement to Contact (Closing in with the enemy to establish contact and engagement);
- Hasty/Quick Attack (A hastily / quickly planned attack with available resources);
- Deliberate Attack (A well planned and rehearsed attack integrating all resources required to assure victory);
- Exploitation (Follow up operations to seize an opportunity or weakness of the enemy); and;
- Pursuit (Deliberate and planned operations to not allow the enemy to run away or reorganise*)*.

Defensive Combat Missions types are:

- Area Defence (Quick Defence/ Deliberate Defence, to hold or guard ground of tactical importance);
- Mobile Defence (with a holding element to draw in the enemy and a strike element to destroy it); or;
- Retrograde Operations (which includes Withdrawal, Delay and Retirement operations – all of which are meant to minimise risk and to engage the enemy at a time of own choosing).

Combat mission may also be overseas missions/mission in another country; national and alliance combat operations (offensive, defensive, or retrograde); special operations; anti/counter terrorism; counter insurgency; or common military operations like patrolling, raids, ambush, cordon and search, etc.

2.1.5.2 Humanitarian Missions

These include peace operations; search and rescue; CIMIC missions like - aid to civil authorities, disaster relief; etc. These types of missions are listed in the NATO MNF SOP and include numerous missions such as:

- Combat operations in small-scale contingencies,
- Stability operations,
- Peace Operations (PO) - which includes peace building, peacekeeping, peace enforcement, and peace-making,
- Foreign Humanitarian Assistance (FHA),
- Military Assisted Non-combatant Evacuation Operation (NEO),
- Search and Rescue (SAR) /Personnel Recovery (PR), and
- Foreign Internal Defence (FID).

2.1.5.3 Permanent

These missions include safeguarding installations, camp security, training for combat, enhancing individual physical and combat skills, collective training, joint exercises, etc.

The role of all forms of infantry in these operations include tactical operations like *Patrolling, Ambush, Infiltration, Raids, Cordon and Search, Road Opening, Holding Delay Lines, Quick Attack, Attack by Infiltration, Area Defence,* etc. Each of these mission types have specific stages and roles for the dismounted soldier/soldier STU which needs to be analysed in order to arrive at the operational needs required to be fulfilled by a modern soldier system.

The intensity in each of these types will depend upon the stage of operation. For example, in an attack operation the stages of insertion/infiltration; establishment of a firm base; move to the forming up place; forming up for an attack, actual attack under fire, hand to hand combat / capture of defences; exploitation; and; reorganising defences for a counter attack; have varying levels of intensity. It is not feasible to specifically design DSS for each and every mission type and intensity but an understanding of the common operational needs in most missions can make the architecture relevant and robust.

2.1.6 Operational Needs Common to All Types of Mission

The operational needs desired for a DSS, which are required to accomplish most mission types are enumerated below:

2.1.6.1 Situational Awareness & Battle Space Transparency

For all missions, units usually operate together with forces of other branches or in coalition with other nations which needs to be carefully planned and coordinated. It is important for decision making, effective engagement, mobility, protection and survivability, sustainability and logistics to achieve a high situational awareness and keep it current during the operation. Fast and comprehensive messaging is the necessity for current and correct assessment of the situation.

Exchanging graphics and sketches with exact values of position, time and numbers are required to achieve a good common situational awareness. Gathering and processing of information is therefore a major operational task in all types of missions.

2.1.6.2 Timely and Actionable Intelligence

Intelligence is the key to all operational planning. Actionable intelligence is the key to all operational actions and involves the time assessment and dissemination of focused intelligence. Real time or near-real time intelligence enables precision strike with minimal collateral damage and enhances the pace and momentum of operations. Intelligence may take several forms like analysis of enemy order of battle (ORBAT), location and activity data, change detection through satellite imagery or even electronic support measures to gain intelligence through enemy communication networks.

Monitoring of open intelligence means like WhatsApp and Facebook or Twitter or Faxes or mobile telephony of suspected targets can also yield important intelligence. This factor is especially important in MOUT and anti – terrorism operations where the enemy merges with neutral civilian population.

Establishment of multi-national intelligence centres for focus and coordination is an important factor for MNF operational success. The ability of the DSS to link to such centres would therefore greatly enhance a clearer CROP and better decision support. Similarly, denying actionable intelligence, especially radio / electronic intelligence through configurable means such as reduced power, brevity of transmissions, and directional antennas in the communications architecture design in the DSS would help.

2.1.6.3 Dynamic Planning

The fast paced and fluid battlespace demands frequent alterations in plans during its execution, as well as contingency plans for less likely courses of action of the enemy to deny him the benefit of tactical surprise. This necessitates that the DSS should be able to receive instant updates in the CROP as well as concurrent decision support information. This would in turn entail that the processes of planning and execution would get merged in future battle space management system networks.

2.1.6.4 Information Operations - Speed of Decision Making & Dissemination

Military operations at all levels depend on information and information systems for many simultaneous and integrated activities. Information Operations (IO) integrate the employment, during military operations, of information-related capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. Dissemination of decision support information with speed is an operationally critical activity for the DSS.

2.1.6.5 Protection from Current & New Dimensions of Threat

Advances in technology and ingenuity of the adversary force would bring in new dimensions of threat like robotic soldiers, swarm UAVs, small unmanned aircraft system (sUAS), tactical CBRN, directed energy weapons, etc. For example, the current approach to countering sUAS is on detecting RF transmissions used by sUAS or their operators and jamming the command and control links and GPS signals of individual sUAS. However, this may not work in the future as sUAS can operate without RF command and control links by using automated target recognition and tracking, obstacle avoidance and other software enabled capabilities. The design of the DSS should therefore allow add on capabilities to counter such threats in its current or upgraded versions.

2.1.6.6 Effectors & Fire Control System

The end note for all successful operational activity is the effective reduction, neutralisation or destruction of the enemy using the optimum effector. Since types of missions would keep changing and with it the threats and intensity, the design of the effector (soldier/STU weapon) and its control system should allow firing different calibre and types of munitions (incendiary, air-burst, illuminating, shaped charges, self-homing, etc.) as well as different types of projectiles (rounds, grenades, rockets/missiles, etc.) with minimal changes to the personal/STU support weapon system of the DSS. It may also be necessary to automatically indicate/feed the effective engagement ranges for launch/firing of such effectors. To counter threats like swarm UAVs or robot soldiers it may be necessary to equip DSS with the ability to initiate ECM measures to disrupt targets like swarm UAVs/Robots which are controlled through EM waves.

2.1.6.7 Assessing & Adapting to Mission Types and Intensity

In all types of missions, the soldier/STU would have to configure the DSS to suit the type and intensity of the operation by analysing the intensity of operational needs during different stages of the operational activity. Standard operational plans / special operational plans usually cater for self-containment for a period of 48 – 72 hours. However, the current system of providing standard on weapon scales of ammunition for this duration may change in the future. The battlespace management system/tactical control system software, through predictive algorithms, may be able provide an estimate of likely conflict threats, duration and intensity, to enable the soldier/STU to be optimally equipped and armed.

2.1.6.8 Self-Synchronized Operations by STUs (Small Tactical Units)

The concept of NCO is designed to support self -synchronized operations by STUs, wherein the STU or Soldier has a shared understanding of the situation including the commander’s intent. This enables the soldier, STU or STU to carry on with their operational plan without having to seek frequent approvals for small tactical actions which are part of the operational directive or do not fit the operational plan exactly. Self-synchronised operations is made possible through the cumulative effect of an accurate CROP, speedy decision support, communications, coordination and training.

2.1.7 Multi-national Interoperability

Interoperability as defined by NATO /9/ is the ability to act together coherently effectively and efficiently to achieve allied tactical, operational and strategic objectives. It may be categorised under *Technical, Operational* and *Logistical* Interoperability. The measure of this ability or level of standards achieved by Alliance Forces of NATO to act together are scaled from a minimum of *commonality* to an ideal of complete *interoperability* in twelve capability areas like

- Real Time Position Information and COP Development;
- Digital Interoperability;
- Command and Control;
- Equipment and Training Compatibility;
- Common Symbology, Message Format, and Display Resolution;
- Cyber Security;
- Identification Friend or Foe;
- Targeting and Fire Support;
- Network Capacity, Notification, and Information Management;
- Language;
- UAS; and;
- Sensors.

In order for multi-national units to become interoperable a broad range of aspects ranging from doctrine, techniques, tactics and procedures, a common understanding of information, the ability to connect each other's systems, etc. training and operational logistics must also be aligned.

The following paragraphs identify the interoperability points and needs at different organisational levels of joint / multi-national forces such as adjacent battalions, fire support teams, and combined arms teams.

2.1.7.1 Adjacent Battalions

The NATO/LCGDSS Soldier System Interoperability LCGDSS Over-Arching definition document /13/ provides a set of information exchange needs and component/energy exchange in the form of coalition forces interoperability scenarios. In this document, the first two scenarios (peace support and major combat operations in a non-NATO country) describe needs between two battalions that operate adjacent to each other with a common boundary. A battalion from nation A, and a battalion from nation B. Both are under command of A nation A brigade staff.

This can be depicted schematically as in Figure 2-6 where the yellow rings are the interoperability points between the two nations. As the battalion of nation B is under the command (subordinate) of the nations' A brigade command post, the regular hierarchical information flow from the brigade post to nations' B battalion command post goes through interoperability points 2 and 3 (which will often be implemented by means of one single radio network). Interoperability point 1, it is added in the figure to provide a direct information flow between STUs that operate close to each other in a cross-border situation without dormancy (denoted here as squad-squad information flow, but also possible at platoon level). Note that such a direct flow between two squads might not be very common practice yet. But according to the LCGDSS descriptions, they see valuable information needs at that low level. This has been one of the main background reasons to develop STANAG 4677 (dismounted soldier system C4 Interoperability) within NATO.

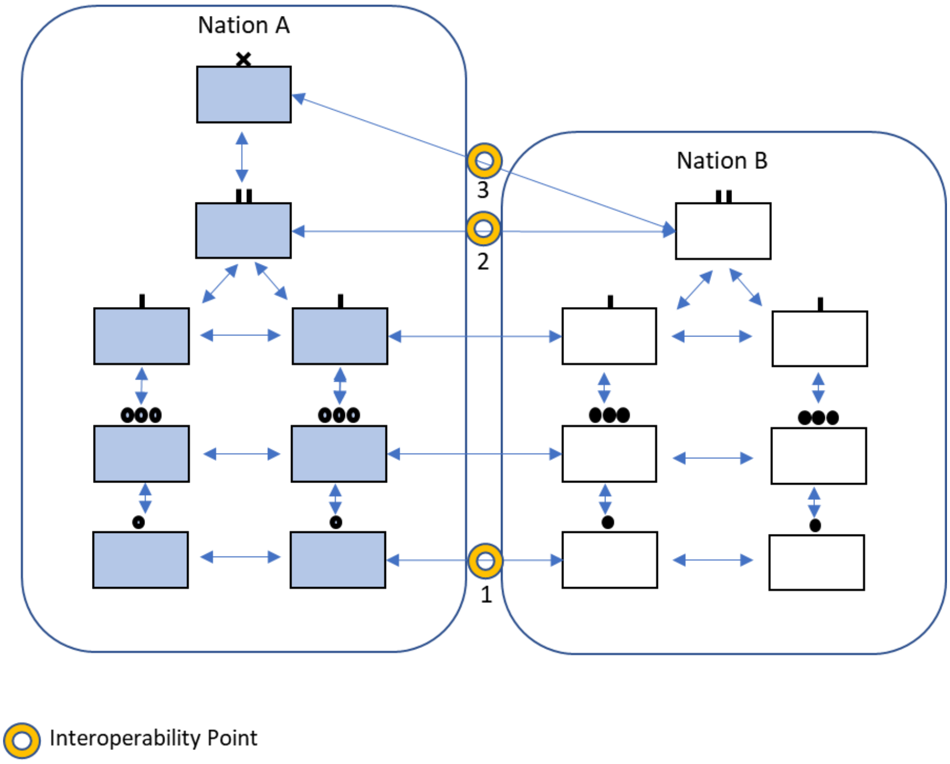

Figure 2-6 – Interoperability points[2] between two battalions operating adjacent to each other with a common boundary

The information needs from the over-arching document /13/ scenarios are summarised at Table 2-1.

Need	Sender/recipients	Related information
Common Operating Picture (COP) Information	STU to STU, and propagation in both nation A and B chain of command.	Icons of STUs (potentially individuals)
Digital Images	STU to STU	Digital picture
Dynamically coordinate between STUs to change a plan in a time sensitive operational action	STU to STU	Standard message formats Sketch May require text message systems with translation capability.
Friend foe identification	STU to STU	Actual positions (via COP exchange or active combat ID systems)
Task assignment through the COP	Unit to unit (multiple levels)	Using standard symbology and/or messaging.
High-res remote sensor imagery	STU to battalion	
Fire support request	Platoon to company	Fire support request report

Table 2-1 – Summary of Adjacent Battalions Information Needs

[2] The figure and the use of interoperability points are inspired by an RTO study from Cassini ea. (SDR-Ready Standardized waveforms for Tactical VHF and UHF Communications for NATO, RTO-MP-IST-092)

2.1.7.2 Fire Support Teams

At company or battalion level, dedicated Fire Support Teams (FST) are often attached that serve as liaisons between the artillery and mortar units on the one hand and close air support from fixed wings and helicopters on the other hand. Forward Observers (FO) and Forward Air Controllers (FAC) are included in such teams. The composition of such units varies per country, some countries have separate forward observer teams and forward air control teams whereas in other nations these specialists are combined into one integrated fire support team.

As both close air support and artillery fire support is located at higher hierarchical levels, it will often happen in coalition operations that the manoeuvre unit, the attached FST (FO/FAC) unit and the artillery/mortar and close air support units are from different nations and in this way these Fire Support Teams are a clear example of multinational interoperability. They operate both vehicle-mounted as well as dismounted/on-foot.

Typical information needs found in Table 2-2.

Need	Sender/recipients	Related information
Situational Awareness Information	FST(FFO/FAC), manoeuvre units, artillery units, aircrafts	FST(FFO/FAC) units need to be aware of the battlefield situation of the unit they are attached to.
Coordination information	FST(FFO/FAC), manoeuvre units, artillery units, aircrafts	Coordination information
Target information, requests for fire support/close air support	FST(FFO/FAC), manoeuvre units, artillery units, aircrafts	Call for fire requests.

Table 2-2 – Summary of Fire Support Teams information needs

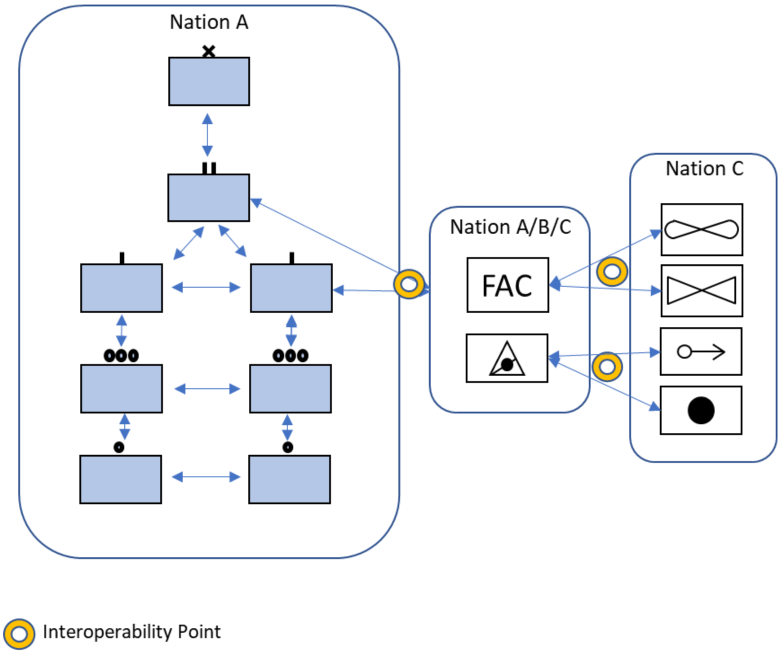

Figure 2-7 – Interoperability Points for Fire Support

2.1.7.3 Combined Arms Team

Traditionally, platoons operate within the context of a company, closely together with neighbouring platoons and without much direct interaction with other combat or combat support units. However, recent operations have shown a more dispersed type of operations of small units where various military capabilities were attached to small units (like platoons) in order to enable these units to operate more independent in the dispersed battlefield. Examples of such units are sometimes denoted as Combined Arms Teams (CAT). Examples of elements/capabilities that can be integrated in small teams are in fact the same capabilities that traditionally can be found only at higher levels (such as brigade):

- Combat Engineering
- Medical Support
- Signal capability
- Fire Support (mortar)
- Reconnaissance
- Electronic Warfare

In multinational coalition operations it is rather likely that these various elements will originate from different coalition partners introducing interoperability points. Additionally, these small units will be supported from units or equipment from higher or different arms units (e.g. artillery, close air support, reconnaissance units/equipment like UAV imagery). Where traditionally the brigade level was the smallest unit where different types of combat and combat support were integrated, the tendency is that the platoon can or will act (under certain circumstances) in the near future as such a smallest integrated unit in order to conduct small scale operations on the dispersed battlefield. This will give rise to the Interoperability Points as depicted below.

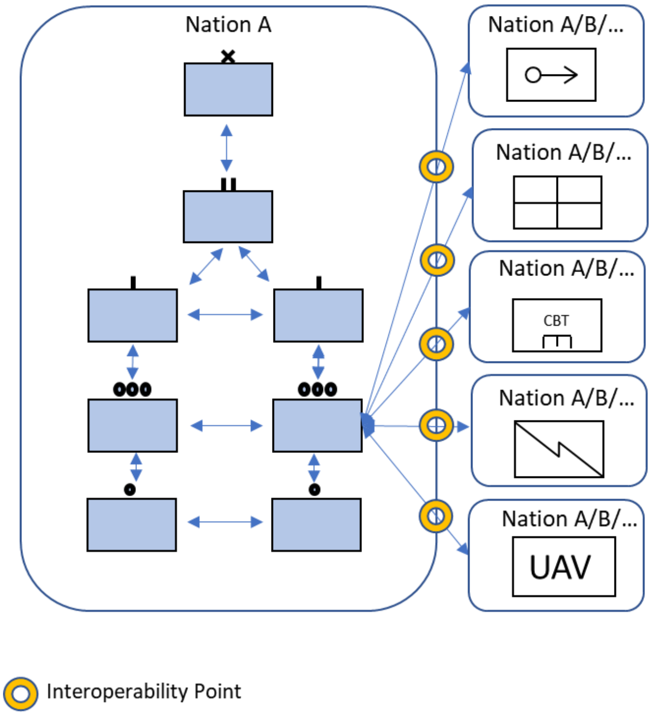

Figure 2-8 – Platoon in the role of smallest integrated unit

2.1.8 Improving Soldier System Effectiveness

In the Operational View, only the operational side of how to improve the DSS effectiveness is addressed.

2.1.8.1 Factors Impacting Soldier System Effectiveness

Improving Soldier System Effectiveness of the DSS from an operational point of view needs an analysis of what areas of the military/operational capability or decision-making cycle need improvement in effectiveness in the current SoA DSS. The operational issues are categorised as under:

- **Critical Operational Issues** (Project Proposal PADR-FPSS-01-2017 GOSSRA):
    - Multi-national interoperability
    - Adaptability to Missions Types and Intensity
    - Less Predictable Dynamic Environment
    - Improved Soldier System Effectiveness
    - Usability with special attention to low size, weight, power consumption and user interfaces
- **The extent to which the Operational Capability Categories are achieved** (CG) 1 to 8 described in the NATO Capability View (NCV):
    - CG 1: Command, Control, Communication, Computing (C4)
    - CG 2: Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR).
    - CG 3: Effective Engagement
    - CG 4: Mobility
    - CG 5: Protection and Survivability
    - CG 6: Sustainability and Logistics
    - CG 7: Education and Training
    - CG 8: Multi-National Interoperability
- **Operational Decision-Making Cycle**: The ability to outpace the enemy while making operational decisions:
    - Boyd‘s OODA: Observe, Orient, Decide and Act;
    - EU/German:
        - Observation and Acquisition of Situation
        - Assessment and Decision Making
        - Operation Planning
        - Order Production and Dissemination
        - Execution

2.1.8.2 Measures to Improve Operational Effectiveness of the Soldier System

Correlating the Future Development Document (FDD) Analysis of Identified Gaps and Promising Technologies and Trends in Soldier System Effectiveness in relation to Infantry Operational Needs can be used as a tool to evaluate measures which can improve effectiveness as well as estimate the increase in effectiveness in each of the areas. This has been shown at Table 2-3.

FDD Analysis Categorisation	Measures to Improve Effectiveness of Soldier System	Operational Cycle Effectiveness Area (Infantry Operational Capability Need)

Power Interfaces & Data Exchange	• Standardise power and data connectors between USB, Ethernet and CRB, and Power Distribution Network (DCI
	• Design & standardise wireless/ better wired connection between helmet and weapon integrated in the vest.
	• Standardise DSS power quality for safety including battery safety allowable voltages
	• Standardise Frequency Ranges for DC/DC Converters to minimize impact on radio communications.
	• Improve power generators and energy harvesting techniques
	• Standardise interfaces between different DSS Modules (DCI and additional DCI, DSS and Weapon, Accessory Rail and DSS).
	• Modular plug-and-play architectures and network-enabling and interconnection capabilities (Improved data storage, interface and automated distribution between soldiers, different sensors and systems).
	• Improve human-machine interface capability and ergonomics to display information to the soldier and avoid overload (continue EDA MUMSIS study). Explore see-through HMD Augmented Reality technology.
	• Improve cyber and data security by mandating the use of crypto graphical (quantum-) secure algorithms, auditing the security of a proposed DSS standard on a specification level and ensuring security on the system level as well as the component level.
		Interoperability;
		Protection & Survivability;
		Sustainability and Logistics;
		C4ISTAR

Technologies (Sensors, Unmanned Systems Weaponry & Equipment)	• EW:
	  ○ Active protection measures, including directed energy weapons (such as HPM or lasers) integrated on vehicles;
	  ○ Passive measures include efficient counter jamming (of radio, GPS) techniques (e.g. using Galileo Public Regulated Service [PRS]) as protection against jamming and spoofing.
	• Use advanced materials for soldier's clothing to significantly reduce multispectral signatures, exploit e-textiles and exoskeletons.
	• Integrate CBRN sensors into DSS
	• Utilise biometric technologies to improve security and monitor soldier vital systems.
	• Integrate and improve fusion of sensors as well as Sensor-C2-Effector linkages.
		Observe, Orient, Decide and Act (OODA)
		C4:
		Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR);
		Effective Engagement;

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

	o Synthetic Aperture Radar (SAR) will allow higher resolution, better discrimination between different types of targets, have improved all weather surveillance capability, will be capable of foliage penetration and will be effective against many camouflaged and certain underground targets. o o Electro-optic and radar sensors will become smaller, lighter and consume less power, therefore even small unmanned platforms (such as UAV) will be able to carry them. • Develop / Improve UAV Counter Measures in terms of: o Detection: through acoustic sensors and spectrum monitoring without depending on stationary platforms like IR, video and radars. o Passive Countermeasure: using a beacon or pointer that would temporarily blind the UAV, keeping it from capturing relevant imagery and information. o Active Countermeasures: Applicable approaches identified are: ▪ Electronic Spoofing: force the UAV to land or return to the launch site – leading to it's or it's operator's capture. ▪ Kinetic Countermeasure would be in form of another UAV that would either crash into the offending vehicle, or use a net and parachute to bring it to the ground. • Weaponry and Related Systems: o Network small arm weapons and fire control on battlefield (NIAG228); o Incorporate advanced RBCI features o Explore feasibility of cyber-attack as a weapon o Investigate active protection measures, including directed energy weapons (such as High-Power Microwave [HPM] or Fibre or Solid-State Lasers with up to 60/100 kW power) integrated on vehicles and associated trade-offs (applications in full range of environment or limited, e.g. excluding urban). • Integrate UxVs within DSS or its platforms: • Integrate nano-UAVs within DSS (individually or at the STU level) because they are highly portable, easily deployable, and currently available in the market and provide enhanced vision to soldiers both during day and night in multiple environments. • Improve heat management system of the DSS.	Protection & Survivability;
Communications	• Increase communication bandwidth and reduce size and numbers of communication equipment to make voice, image and data communication easier including "Videoconferencing in the field" between commanders and individual soldiers.	C4ISTAR: Protection & Survivability;

	• Develop reliable and robust networks established by unmanned vehicles such as UAVs (communication relay drones) to provide backup modes of communication. • Incorporate EMP capabilities to allow Low Probability Detection (LPD) in radio sets/links (e.g. in Covert operations) • Replace current loaned radio solution by a Coalition/EU wave form, • Evolve a common Wave Form SDR architecture allowing wider procurement options to nations.	
Operational/ Training	• Increase computing power, advance software algorithms (e.g. image processing and analysis) and communications / data fusion from increased number and type of sensors to improve decision support and C4ISTAR. • Allow chain-building of DSS-allowing individual soldiers to function as sensors. • Effectors: Need to investigate active protection measures, including directed energy weapons (such as High-Power Microwave [HPM] or Fibre or Solid-State Lasers with up to 60/100 kW power) integrated on vehicles and associated trade-offs (applications in full range of environment or limited, e.g. excluding urban). • Develop integrated training facility within system with external monitoring capability • Develop training packages using modelling and simulation using AI and Augmented Reality	This would have a cross-cutting impact on all operational capability areas.

Table 2-3 – Measures to Improve Soldier System Effectiveness

The envisaged current and likely future operational needs for different missions and mission intensities needs add-on systems in the table above, which are integral or modular in design. Care should be taken in standardisation of the architecture to ensure that continuous R&D and innovation is not hindered.

2.1.8.3 Improving Soldier System Effectiveness Linked to Interoperability Areas

Another approach to improving soldier system effectiveness is to address the in section 2.1.6 identified interoperability capability areas.

2.1.9 Command & Control Concepts

2.1.9.1 Legacy Command and Control

Legacy C2 use linear processes, which are strongly optimized but cannot manage the complexity nature of Information Age conflicts.

Legacy military organizations use simple, often linear command and control mechanisms. That is, they decompose the battlespace, phase (decompose over time) their operations, use specialization, optimization, and centralized planning to make their actions efficient, and employ decentralized execution and cyclic processes[3] to ensure that their efforts are flexible and responsive to the operating environment. Their goal is adaptive control pressure to control selected features of the battlespace (casualty ratios, territorial control, etc.) by adjusting their actions as the situation changes. This is an important (but incomplete) step toward the agility needed by Information Age forces.

The optimized, C2 processes cannot easily adapt to the uncertain nature of the future conflicts.

Legacy militaries have, as a result of their size, the way they are organized, and their approach to command and control, developed a “battle rhythm” that cannot easily be changed. Yet many of today’s missions may require a faster speed of command than is typical of these work processes.

The principles underlying traditional command and control are:

- **Decomposition**, which stems from a “divide and conquer” mentality to solve any problem;
- **Specialization**, which requires for the development of professional specialties as a direct result of the decomposition approach.
- **Hierarchy**, which is the organizational consequence of specialization. The efforts of highly specialized entities need for a middle management layer, who coordinates them by synchronising their actions to achieve the goals of the organizations they support.
- **Optimization**, which is the goal of mission management and requires for operations complexity to be transformed into a collection of simple, manageable tasks and problems, which can be (locally) optimized.
- **Deconfliction**, which is a prerequisite of any feasible (local) optimization process, which assumes well known circumstances, i.e. optimal operating environment.
- **Centralized Planning**, which became a crucial part of Industrial Age command and control because it enabled commanders to arrange forces and events in time and space so as to maximize the likelihood of success (mission accomplishment). Given the limits of Industrial Age communications, plans are the key mechanisms by which military commanders create the conditions necessary for success.

2.1.9.2 Interoperability in Legacy Military Organizations

Legacy military organizations have evolved into many-layered hierarchies populated with stove-piped organizations where information exchange is based on centralized planning processes, via static, predefined information exchange requirements, i.e. legacy approach to interoperability is based on the belief that it is possible to specify the information exchanges and collaborations that are needed in advance, by creating fixed seams that prevent information from being brought to bear, i.e. they prevent diversified information integration effects.

[3] The popularity of the OODA loop (Observe, Orient, Decide, Act) among professional militaries is a reflection of their recognition of this cyclic process

In dynamic, less predictable operational environment, it is often not possible to know who may need what piece of information, when it will be needed, and who may need to work with whom.

2.1.9.3 Agility in Legacy Military Organizations

Legacy forces belief in optimization and centralized planning. Optimization inherently involves trade-offs. Given a choice between an option that yields the best result, and another option that may not be as good as the optimum, but maintains its value over a larger range of conditions, Legacy organizations systemically have chosen to go with the global optimum for a given problem. This is due the decomposition approach, which is based on very narrowly framed decisions taken by specialists.

It is worth to note such an approach systematically forced out of consideration the complexity and uncertainty inherent in real world situations, as consequence, this fixation on optimality often results in the selection of an option that sacrifices agility, i.e. an option that maintains its value over a larger range of conditions, in the hopes of achieving the best possible result in the current, specific case.

From the above consideration stems that centralized planning is antithetical to agility because it (1) is relatively slow to recognize and respond to changes in the situation, (2) results in ill-informed participants, and (3) places many constraints on behaviour.

2.1.9.4 Drawbacks of Legacy Military Organisations

For what described in the previous paragraphs, the Legacy approach to warfare has many drawbacks with respect to the current and emerging conflicts. The more relevant ones are listed below:

- As a result of their size, and the way they are organized, a Legacy approach to command and control, develops a “battle rhythm” that cannot easily be changed. Yet many of today’s missions may require a faster speed of command than is typical of these work processes.
- Because of the complexity of the security challenges faced, modern militaries need to (1) bring all of their information to bear to make sense of the situation and (2) be able to employ all of their assets to effectively respond to the situation. The Legacy principles and practices of decomposition, specialization, hierarchy, optimization, and deconfliction, combined with command and control based on centralized planning, will not permit an organization to bring all of its information (and expertise) or its assets to bear.
- In addition, legacy organizations are not optimized for interoperability or agility. Thus, solutions based upon these assumptions and practices will break down and fail in the Information Age.

2.1.9.5 Command and Control of Information Age Warfare

The command and control of Information Age warfare can be represented as the interaction of top-down and bottom-up effects. The Deliberate Planning is a typical top-down approach, which is appropriate when ample time is available for the consideration of a number of alternative courses of action by either “side” and a course of action can be chosen that is considered to be, in some sense, optimal. On the other hand, Rapid Planning is bottom-up, it is appropriate when time is short and expert decision making under stress leads to a pattern-matching approach.

Military missions are complex activities. Ashby’s Law of Requisite Variety [/10/] indicates that to properly control such a system, the variety of the controller must match the variety of the combat system itself. The C2 system itself, in other words, has to be complex.

The essential idea is that: a number of interacting units, behaving under small numbers of simple rules or algorithms, can generate complex behaviour.

As part of this careful choice, there is the need to ensure that the potentially chaotic behaviour generated by the interaction of these simple rules is ‘damped’ by a top-down C2 structure which remains focused on the overall, high level, mission objectives. An Information Age C2 architecture will be based on two main C2 segments:

- The C2 Tactical Segment, which is the lower-level interaction of simple rules or algorithms that generate the required system variety. It acts at lower levels of command and will consist of a stimulus/response mechanism. In cybernetic terms, this is *feedback control*.
- The C2 Cognitive Segment, which is the controlling intelligence, which guides the system towards a particular operative goal. It focuses on mission objectives and provides the overall goal to the C2 Tactical Segment. It acts at the higher level, a broader (cognitive-based) review of the options available to change the current mission plan (if necessary) to be carried out. In cybernetic terms, this is *feed-forward control* since it involves the use of a ‘model’ to predict the effects of a particular system change. The C2 Cognitive Segment typically include a Decision Support System, which processes by appropriate algorithms the Big Data gathered from C2 Tactical, and then provides the human operator both the analytics outcome and different alternatives among which to choose the command(s) to issue to the C2 Tactical elements.

The overall C2 system can be outlined as in [/11/]: within a broad intent and constraints available to all the forces, the local C2 Tactical force units self-synchronise under mission command of C2 Cognitive in order to achieve the overall intent.

This C2 synergic process is enabled by the ability of the forces involved to be robustly networked and loosely coupled. C2 loose coupling property allows capturing the local freedom available to the units to prosecute their mission within an awareness of the overall intent and constraints imposed by high-level command. This also emphasises the looser correlation and asynchronous relationship between inputs to the system (e.g., sensor reports from networked DSS STUs) and outputs from the system (e.g., orders from C2 Cognitive). In this process, information is transformed into “shared awareness,” which is available to all via the Global Data Space which provides a solution for selective information sharing. As described below, C2 Tactical loose coupling leads to units that self-organise in clusters by opportunistically linking up with other units, which are either local in a physical sense or local through (for example) an information grid (self-synchronisation), but here it is worth noting that C2 loose coupling property allows capturing the local freedom available to the units to prosecute their mission within an awareness of the overall intent and constraints imposed by high-level command. This also emphasises the looser correlation and asynchronous relationship between inputs to the system (e.g., sensor reports from networked DSS STUs) and outputs from the system (e.g., orders from C2 Cognitive).

Self-organisation in this context is taken to mean the coming together of a group of individuals to perform a particular task. They are not directed by anyone outside the group. It is the group members themselves who choose to come together, who decide what they will do and how it will be done. A feature of these groups is that they are informal and often temporary. Self-organising systems can, as their name implies, develop local organisation within the system in order to evolve towards an attractor. A possible scenario follows.

The C2 Cognitive issues a directive for tuning the behaviour of a STU of soldiers (the soldiers coordinate via C2 Tactical rules). Each of them is able to self-organise to compose clusters suited to perform the C2 Cognitive command. It is worth noting that a (group of) soldier(s) can in turn issue commands to unmanned vehicles, this implies that the C2 Tactical is able to generate hybrid clusters composed by both human and (swarm of) autonomous nodes. It is worth noting that as the self-organising and clustering properties are based on a given degree of autonomous decision making, a high degree of autonomy provides many advantages, but on the other hand, also raise non-trivial challenges in the interaction with humans, who need to cooperate with or command & control STU of UxVs.

2.2 NOV-2 Operational Node Connectivity Description

The term Small Tactical Unit (STU) was chosen in order to describe a group of soldiers while not specifically referring to Section, Squad or Team, etc. as the organisation of such groups are different in different nations. STU recognizes the need to not only specify and address an individual soldier but also a soldier group (STU) because inside a STU there are soldiers with different roles/specialist equipment and also shared equipment, which otherwise would not have been considered in the architecture.

2.2.1 Dismounted Soldier Node Internal Connectivity

Figure 2-9 presents internal associations between the nodes (or *blocks* in SysML) of an individual DSS. The associations shown in the figure describe an interaction and do not necessarily represent a wired connection. Besides information, transported via wired or wireless connections, it describes also the physical flow of materiel and/or energy.

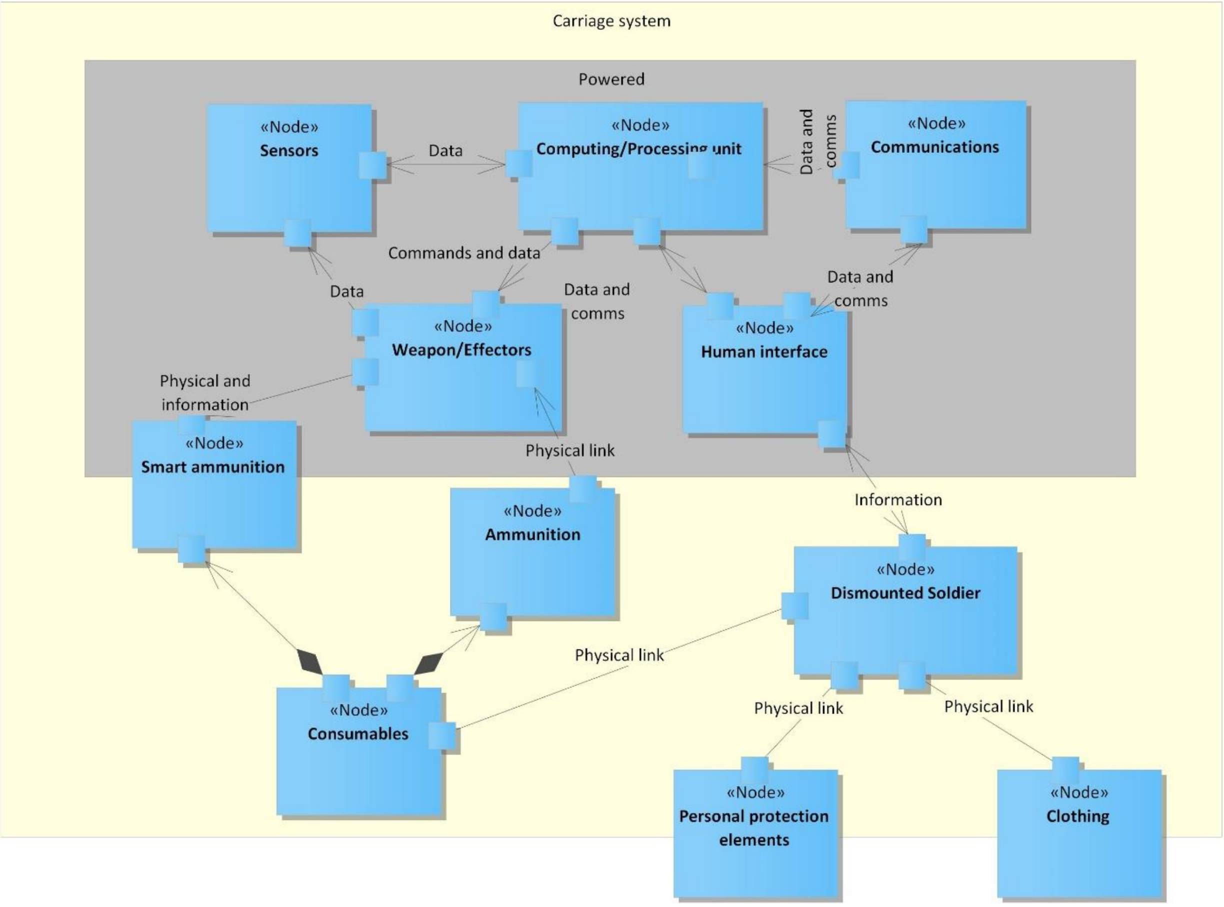

Figure 2-9 – Dismounted Soldier Node Internal Connectivity

2.2.1.1 Sensors

Sensors in the individual soldier context refer to smaller sensor systems, which represent devices or equipment, used for acquiring data and especially tactical data. Such sensor systems typically use electro-optical, acoustic, or RADAR technology.

Sensors may have associations with the block “**computing/processing”** for further processing in the computer or data distribution to other soldiers and with the block “**weapon/effectors”** for delivering better aiming data to the weapon. The Sensors may also be directly attached to the **weapon/effectors** and therefore may have a physical association to it.

2.2.1.2 Computing/Processing

The block “**computing/processing”** has associations to the blocks “**Communication”, “Human Interface”, “Weapon/Effectors”, “Orientation/Navigation”** and “**Sensors”** and represents only digital data exchange as the computing block is receiving, storing, processing and forwarding data according to its software.

In the ISTAR process this block is mainly responsible for the extraction of **Intelligence** from the **Surveillance, Reconnaissance, and Target Acquisition** data.

2.2.1.3 Communication

The block “**Communication”** with its capability to receive and transmit information from/to other DSS and/or communication nodes using voice and/or data has associations to blocks “**Human Interface”** and “**Computing/Processing”**. The association represents digital and/or analogue data exchange.

2.2.1.4 Human Interface

The block “**Human Interface”** represents the systems output to the **Soldier** and the systems input from the **Soldier**, which can be performed by using suitable human senses, e.g. optical, audio, tactile, etc. Block **Human Interface** transforms digital or electrical information to human senses and vice versa. Therefore, it is associated with the Soldier as well as block “**Communication”** and “**Computing/Processing”**.

2.2.1.5 Weapon/Effectors

The block “**Weapon/Effectors”** has associations to block **“Sensors”** and “**Computing/Processing”**. An additional association is required when using “**Smart Ammunition”**. This is to transmit data and/or programme the ammunition prior to shooting.

2.2.1.6 Smart Ammunition

An example of **Smart Ammunition** is munition which can be programmed for air burst or to increase accuracy of a bullet's trajectory prior to shooting. For this capability, an association to a suitable **Weapon/Effector** is necessary.

2.2.1.7 Consumables

The block **"Consumables"** mainly has associations to the **Soldier**, because the **Soldier** needs nutrition (food, water) or replacement of discharged batteries as well as supply of ammunition for the **Weapon/Effectors.**

2.2.1.8 Personal Protection

The block "**Personal Protection"** has associations to the **Soldier** only. The association is mainly of ergonomic nature because of the passive armour. In future, the association might become additionally electrical for reactive armour.

2.2.1.9 Clothing

The block "**Clothing"** has associations to the **Soldier** but, with smart materials which are coming up now, may also be associated with the **Data Management and Data Infrastructure**. Such materials may enable data transfer, power distributions, and may even incorporate some processing power or just work as an antenna. Also devices might be incorporated, e.g. active cooling devices or adaptive camouflage.

Smart textiles for data transmission

Smart Textiles or intelligent textiles refer to materials that include additional functionality into textiles or clothing, other than protecting the body. The area of smart textiles is a strong growing market and is definitely of interest for future combat soldier equipment. Among other topics it includes miniaturized, integrated sensors, which enable monitoring of the body or of parameters in the environment. Smart textiles also include flexible printed circuit boards, flexible antennas and even flexible batteries. These developments are of interest in the soldier system area for reasons of lowering the weight of equipment, while increasing wearing comfort.

Flexible textile antennas

Since about 5 years, in the USA and Europe civil research is performed on embroidered body-worn antennas using conductive fibers, called E-fibers. These research activities are since approx. 2012 specifically stimulated by IoT developments (mainly for health monitoring applications) and bring the integrated, body-worn antennas beyond the military application domain. Military R&D in this field started around 2006 and has mostly considered frequencies from about 1.5 GHz (e.g. Pharad and Wearable Antenna Technologies Inc.). Civil interest in this topic may generate a spin-off for the military market, especially for DSS biometrical applications.

The lower the radio frequency is, the more body loss effects and restricts transmission of signals. However, present state-of-the art indicates that embroidered multiple dipoles as low as 600 MHz are feasible (using e.g. highly flexible silver-coated Amber strand fibers by Syscom Advanced Materials, Inc.). The loss is acceptable and the azimuth coverage is omnidirectional, which is important to provide a dismounted solider with the desired wireless connectivity and range.

A number of antenna structures such as inverted F antennas and low-profile micro strip antennas are applied for higher radio frequencies and higher bandwidths accordingly.

2.2.1.10 Carriage System

The block "**Carriage System"** currently has associations to the **Soldier** only. The association is mainly of ergonomic nature because it is the interface between human and equipment. In case electrical devices are carried inside or attached to the backpack (e.g. power generators) electrical connections would be necessary.

2.2.1.11 Power

The block “**Power”** is associated to the equipment which has electric/electronic functions. Power (-infrastructure and -management) can be organized centralized and/or decentralized as described in the previous STASS study I. Associations are the flow of energy and can be added with power related information/data exchange.

2.2.2 Small Tactical Unit (STU) Internal Node Connectivity

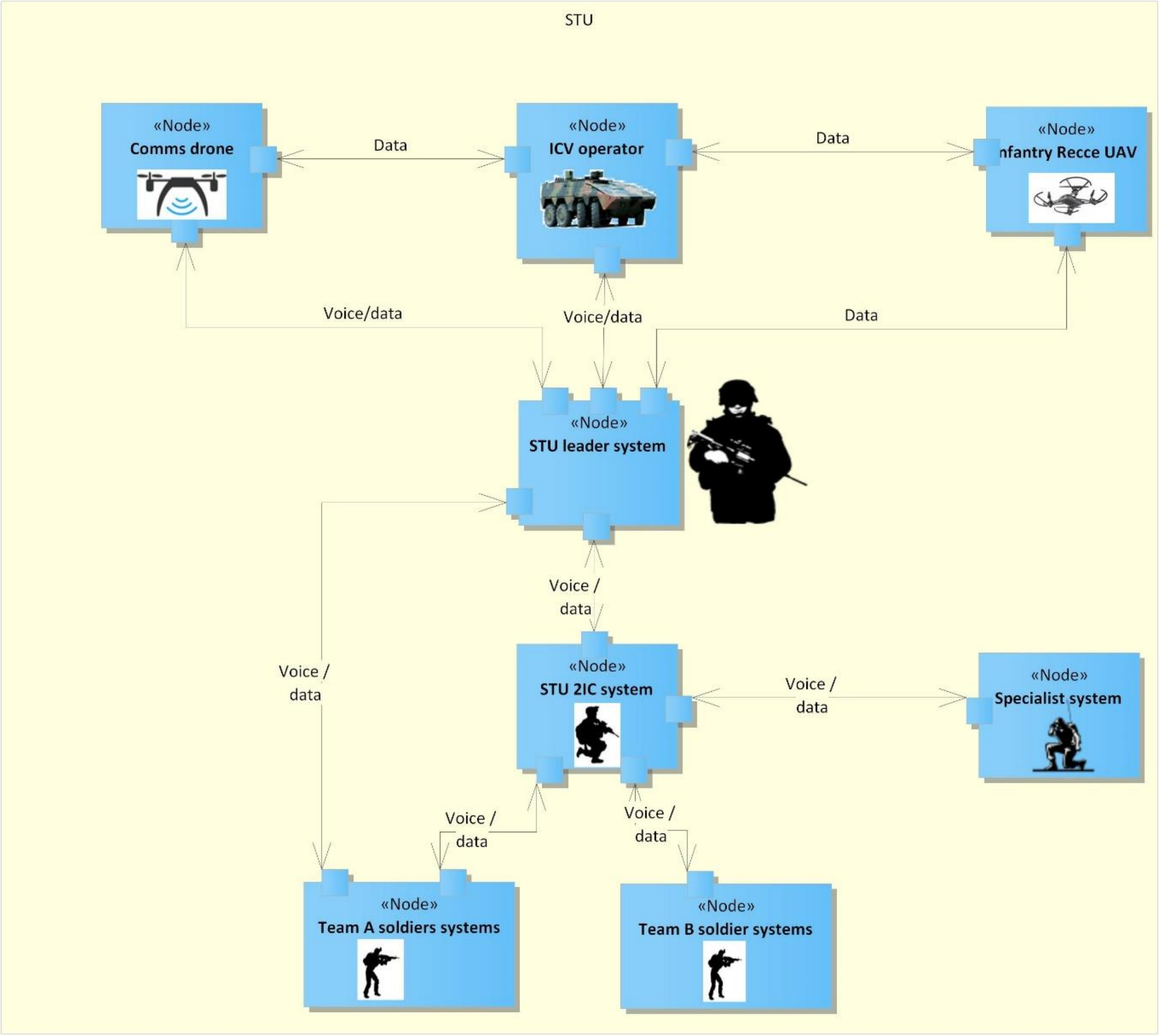

Figure 2-10 – STU Internal Node Connectivity

Figure 2-10 above depicts the STU Internal Node Connectivity. The voice and data links are wirelessly connected between each individual of the STU. Data links exist between the integral Reconnaissance UAV to the ICV and the Base Station (generally with the Section Leader or the Section 2IC) and a Wi-Fi Repeater Drone (when necessary) to enable wireless voice and data WAN connectivity to all members of the STU. Additional links, like a portable common charging station/unmanned ground sensor, etc. may also be part of the connectivity through wired / wireless links.

2.2.2.1 STU /Section Leader System

The STU Leader, through his/her system, commands and controls the STU and is linked wirelessly for voice and data communication with other members of the STU. The STU Leader through the mission network (E.g. the Federated Mission Network {FMN}), which would be designed differently for different missions, gets the relevant COP and is seamlessly and securely connected to all members of his STU as well as the Platoon Commander through the Platoon Commander System.

2.2.2.2 STU /Section 2IC System

The Second in Command of the STU (through Section 2IC System) gets near real time reconnaissance information, through a data link from the STU Reconnaissance UAV (either through the ICV or from the UAV Base Station) and has voice and data link with the STU Leader and all other members of the STU. In case of the STU Leader or Section Leader System becomes a casualty, the 2IC system should be able to take over all functions of the STU Leader.

2.2.2.3 STU /Specialist System

The Specialist Node should be linked via data and voice to the Section 2IC System, who directly controls such personnel like the Mortar Bomber or the Medium Machine Gun (MMG) Operator or the UAV Controller. It should also have da ta and voice links with the rest of the Section Leader System, and other STU members systems. Specialist systems may also need to be connected with UAGS or other shared devices at the STU level.

2.2.2.4 Individual Soldier System

The individual soldier system would have voice communication and data links with all other Individual systems as well as the rest of the STU members. Not all members need to have the complete COP, which should be available on a need basis.

2.2.3 Small Tactical Unit (STU) Node External Connectivity

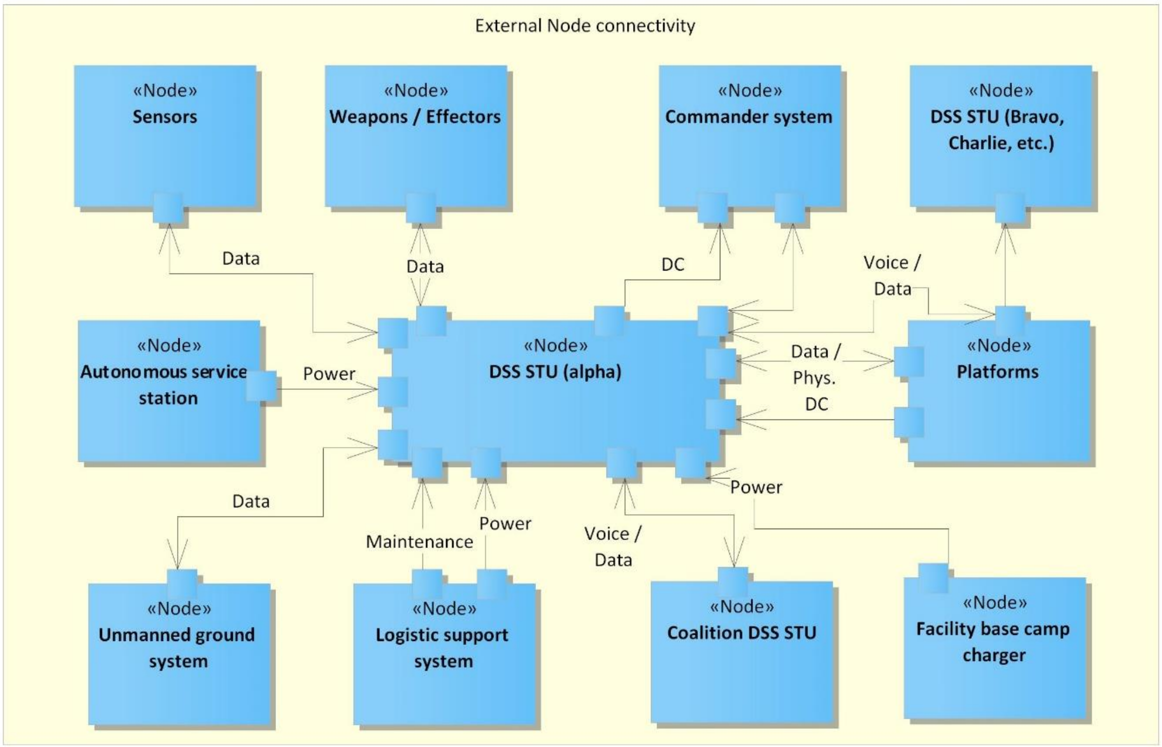
External Node connectivity
«Node» Sensors
«Node» Weapons / Effectors
«Node» Commander system
«Node» DSS STU (Bravo, Charlie, etc.)
Data
Data
DC
Voice / Data
«Node» Autonomous service station
Power
«Node» DSS STU (alpha)
Data / Phys. DC
«Node» Platforms
Data
Power
Maintenance
Voice / Data
Power
«Node» Unmanned ground system
«Node» Logistic support system
«Node» Coalition DSS STU
«Node» Facility base camp charger

Figure 2-11 – STU Node External Connectivity

Besides information, transported via wired or wireless connections, Figure 2-11, also shows physicals-based flows, e.g. for material and energy between a **DSS Soldier-STU** and its surrounding elements.

Ports and blocks are design elements of the System Modelling Language SYS-ML.

2.2.3.1 STU

The **Soldier-STU** here is seen as a unit of soldiers, being its composition dependent on the branch, mission and task. Each soldier can be equipped with material/devices according to their specific roles and capabilities but also material/devices which are shared inside the STU.

The Soldier STU operates as the **DSS-STU** which represents all their equipment as a comprehensive, modular system.

STUs can be sub-divided in teams. STUs (Sections/Squads) are organized in platoons, subordinated to the platoon commander.

2.2.3.2 DSS STU

The **DSS Soldier-STU** here is seen as equipment/material that provides services to the **Soldier-STU** enhancing their individual capabilities. It provides shared awareness through a Common Relevant Operational Picture (CROP) which may be available to some or all soldiers depending on the national preference.

The **DSS Soldier-STU** provides basic equipment, including sensors, effectors, computers, and communication equipment, to each individual soldier according to the branch and mission. For the interconnection with additional/external effectors, sensors and communication equipment additional ports shall be made available.

The **DSS Soldier-STU** provides also equipment which is tailored to the specific STU and can be allocated to one or more specific soldier(s) according to their task and/or role.

To maintain the platoon commanders DSS, which may be used more extensively, a port is useful to transport electrical energy from another DSS. This can be done for example by physically exchanging batteries or fuel or use a wired connection to feed in DC power.

The possibility to exchange energy within the **DSS Soldier-STU** is useful to maintain the abilities of a DSS which runs out of energy. Depending on the personal equipment and its usage, different power consumption will occur. Soldiers with charged batteries should be able to exchange them with soldiers with chargeless batteries.

2.2.3.3 Commander System

The **Platoon Commander System** provides services to the commander to support the enhanced challenges of command, control, communication, planning and preparation of a platoons’ mission.

The connection between the **Platoon Commander System** and the **DSS Soldier-STU** establishes voice and data exchange via radio frequencies (RF) without preventing face-to-face communication. Here the Platoon Commander is a higher-level functionary of the Soldier Section / Squad referred to as a STU.

If energy is running out, power supply may be maintained by another DSS.

2.2.3.4 Platforms

Platforms can be ground, air and navy vehicles, which may belong to the STU or are provided specifically for an operation. They can serve as transport, protection, fire support and supply of the STU/Team and its DSS-equipment. Some platforms provide all these services within one single platform, others just provide transport.

Fully integrated vehicle/DSS-systems act as a mothership for the **DSS Soldier-STU**. Points of interaction are the provision and/or transport of electrical energy and nutrition, the exchange of information and the utilization of the vehicle infrastructure, e.g. for long range communication.

When mounted on STU vehicle or helicopter, the DSS is connected, e.g. with a cable, in order to receive energy but also to be able to communicate by voice and exchange data. Empty fuel cartridges can be refuelled or replaced by new ones.

In some nations, the vehicle energy supply does not allow draining its own battery and will provide just enough power for the electrical and electronic devices (in case not enough power is available for charging). Thus, discharged batteries are replaced by charged batteries and recharged using a dedicated charger on the vehicle. In other nations, the batteries of the DSS are also charged when connected to the vehicle (if enough power is available from the vehicle).

Often neglected are the ergonomic aspects of the physical integration of soldiers and their equipment. It must be taken into account that certain branches always carry the DSS-equipment strapped on; especially mechanized infantry rapidly changing from mounted to dismounted roles and vice versa.

2.2.3.5 Coalition DSS STUs/Teams

The **Coalition DSS STUs/Teams** are units of allied forces deployed in the same mission area (in their assigned specific area of responsibility) when organized in multi-national forces. To establish and maintain a close cooperation of STUs/teams of different nations, a common communication service is necessary.

STANAG 4677 suggests to provide an “Interoperability Radio” with a standardized interface to the STUs. Exchange of tactical data, especially Blue Force, Contact and Sighting, and NBC Information between multi-national STU DSS’s is then enabled. Of course, the exchange of energy could also be possible if required.

2.2.3.6 Unmanned Ground Systems

Unmanned Ground Systems (UGS) are small driving robots which can be carried and deployed when needed, mainly used for surveillance and reconnaissance tasks. Larger driving robots may be used to accompany dismounted soldiers to carry out different tasks, e.g. load carrying.

Such UGS’s may be autonomous, semi-autonomous, or just remote controlled. Either system needs some points of interaction with the **DSS-Soldier-STU** and is considered in the previous diagram (Figure 2-11).

2.2.3.7 Logistic Support System

The **Logistic Support System** is an organization that provides adequate supply of material, maintenance, personnel to the STU/team on mission, directly or via the platoon.

Points of interaction are of varied range and may be simply the storage and provision of energy and nutrition up to the replacement of LRU’s on demand, as well as remote advisory or remote control for self-repair.

2.2.3.8 Sensors

Sensors in the STU context rather refers to sensor systems which represent devices or equipment used for acquiring data and especially tactical data as Surveillance, Reconnaissance and Target Acquisition part of the ISTAR process. Such sensor systems typically use electro-optical, acoustic, or RADAR technology and could, especially at STU level, include a complete platform such as a reconnaissance UAV or a ground /amphibious reconnaissance vehicle (tracked or wheeled).

2.2.3.9 Weapons/Effectors

Weapons/Effectors are devices or material as part of the DSS that provides the capabilities to the **Soldier-STU** to achieve the desired effect as defined within the mission.

All soldiers are normally equipped with a weapon, with a size and type, which differs depending on the individual role. The weapon may be equipped with additional aiming devices, e.g. electro-optics, in order to increase first-hit probability and/or aiming when unexposed to the enemy.

A connection between Weapons/Effectors and DSS Soldier STU could be used for data exchange, e.g. a push-to-talk command while keeping the hands at the weapon. Specific applications may also inform about rounds of ammunition available in the weapon or may even display virtual reality markers in the aiming device.

2.2.3.10 Autonomous Service Station

The node **Autonomous Service Station** represents a sub system or device which can be carried by the infantry STU or which is provided for long term autonomous missions. It may be deposited at a base camp or hiding place where the STU or the team can return after an intensive mission.

The Autonomous Service Station provides an energy harvesting device or a mobile power generator with recharger capabilities. It may also store ammunition, a long-range communication device, water/food, dry clothes etc.

Local stores or the environment shall be also considered under this node.

2.2.3.11 Facility Base Camp Charger

Base Camp Chargers can be used to recharge empty batteries before and after mission.

2.3 NOV-3 Operational Information Requirements

The purpose of the Operational Information Requirements sub-view is to identify and describe all information exchanges that make up all information lines between operational nodes.

NOV-3 sub-view identifies which information shall be available at which information space.

The information space is a virtual space where relevant information required to accomplish a task and/or mission is available to be processed, distributed, displayed and used. The identified information spaces in Figure 2-12 are categorized with respect to the echelon level (Platoon, STU/Team, and Individual Soldier).

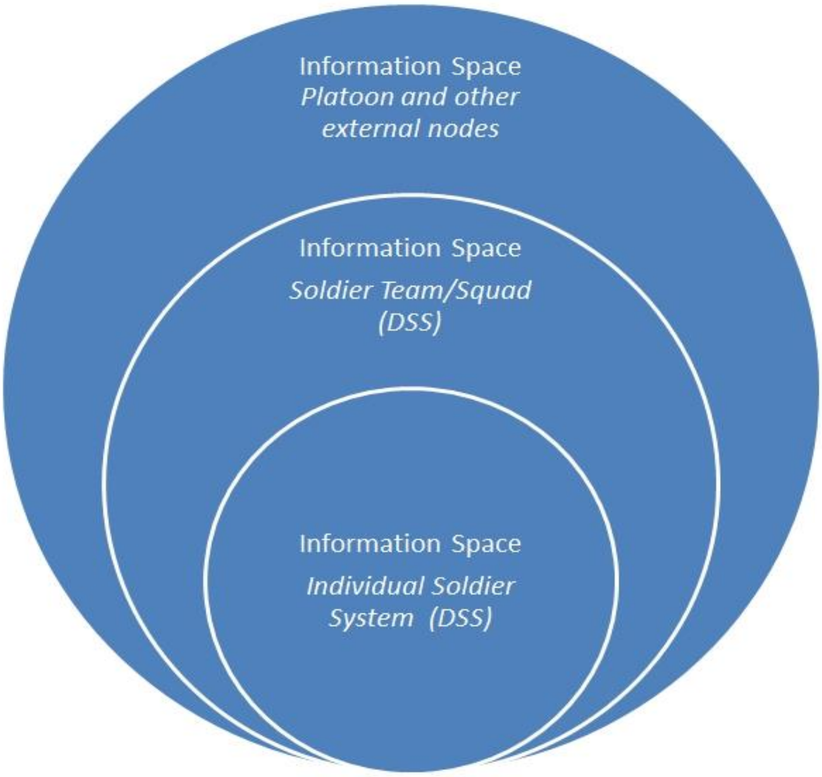
Information Space
Platoon and other external nodes
Information Space
Soldier Team/Squad (DSS)
Information Space
Individual Soldier System (DSS)

Figure 2-12 – Information Spaces

Most of the information types are used at all levels however, the level of detail is adapted by aggregated or disaggregation according to the needs at the specific level. At each level the relevant information is then displayed in the form of a CROP based on rules which determine what information is relevant for the specific level, branch and role. In a coalition operation, it can be useful to agree on such rules, coalition wide.

With modern C4I software/application it may be possible to implement and integrate these rules, via algorithms, in order to decrease the operational burden for each soldier.

The matrix below would become three–dimensional if the role dependency is also considered. As an example, the plan of manoeuvre shall be available for each individual soldier system but not, if the role is below STU leader, as they all belong to the column STU/team.

	Information shall be…		
Information type Enemy related:	**…available at each Individual Soldier System (DSS)**	**…exchanged within Soldier Team/STU (DSS)**	**…exchanged with Platoon and other external nodes**
Enemy position, direction, distance	●	●	●
Enemy type, strength	●	●	●
Enemy behaviour, mode	●	●	●
Timestamp	●	●	●

Table 2-4 – Mapping of Information spaces to information types – Enemy Related

	Information shall be…		
Information type Situation related:	**…available at each Individual Soldier System (DSS)**	**…exchanged within Soldier Team/STU (DSS)**	**…exchanged with Platoon and other external nodes**
Area organization, borders, reference positions and other control and coordination lines	●	●	●
Command posts, areas, battle positions	●	●	●
Facilities of combat support, mission support and C2-support	●	●	●
Organization for combat	●	●	●
Area of medical point	●	●	●
Important details for the conduction of operations	●	●	●
Forces and units of higher echelons, and if needed subordinate echelons	●	●	●
Neighbour/coalition forces and other units in the area of interest	●	●	●
Key terrain, geographical constraints, contaminated, blocked or unblocked areas and barriers	●	●	●
Own position	●	●	●
Team member position	●	●	●
Routes	●	●	●
Radio range	●	●	
Weather forecast	●	●	
NBC-alert / Warnings	●	●	●

Table 2-5 – Mapping of Information Spaces to Information Types - Situation Related

	Information shall be…		
Information type Operation related:	**…available at each Individual Soldier System (DSS)**	**…exchanged within Soldier Team/STU (DSS)**	**…exchanged with Platoon and other external nodes**
Plan of manoeuvre	●	●	●
Order	●	●	
Order status	●	●	●
scouting and observation results	●	●	●
Operational Support	●	●	●
Radio frequencies	●	●	●

Table 2-6 – Mapping of Information Spaces to Information Types - Operation Related

	Information shall be…		
Information type Effect related:	**…available at each Individual Soldier System (DSS)**	**…exchanged within Soldier Team/STU (DSS)**	**…exchanged with Platoon and other external nodes**
Target position	●	●	●
Target description	●	●	●
Required striking effect	●	●	●
Target priority	●	●	●
Date/time	●	●	●

Table 2-7 – Mapping of Information Spaces to Information Types - Effect Related

	Information shall be…		
Information type DSS equipment related:	**…available at each Individual Soldier System (DSS)**	**…exchanged within Soldier Team/STU (DSS)**	**…exchanged with Platoon and other external nodes**
Status of consumables (incl. power, ammunition)	●	●	●
Firmware version	●		
Configuration	●		
Status, failures	●		
Settings	●		
Components ID	●		
Maps/ -required	●		●
User information	●		
User role	●	●	
User authentication	●		
Key/ -ring	●	●	
Available team members	●	●	
Sensor information	●	●	●
Health status	●	●	

Table 2-8 – Mapping of Information Spaces to Information Types - DSS Equipment Related

Figure 2-13 shows the operational information flows between the STU or team and other external nodes. Physically, the information may not be transmitted directly between the nodes (blocks) but may be routed via intermediary elements.

The challenge of a DSS design is to provide information to the soldier/STU/team in a way which generates a high situational awareness, in a most efficient way, and with minimum burden to the soldier. Information overload is a known and important stress factor, especially to soldiers under fighting conditions.

Each DSS can be configured and used as a sensor to complement the CROP.

The trade-off between increased weight/volume/power consumption of additional equipment and mobility needs to be balanced out thoroughly.

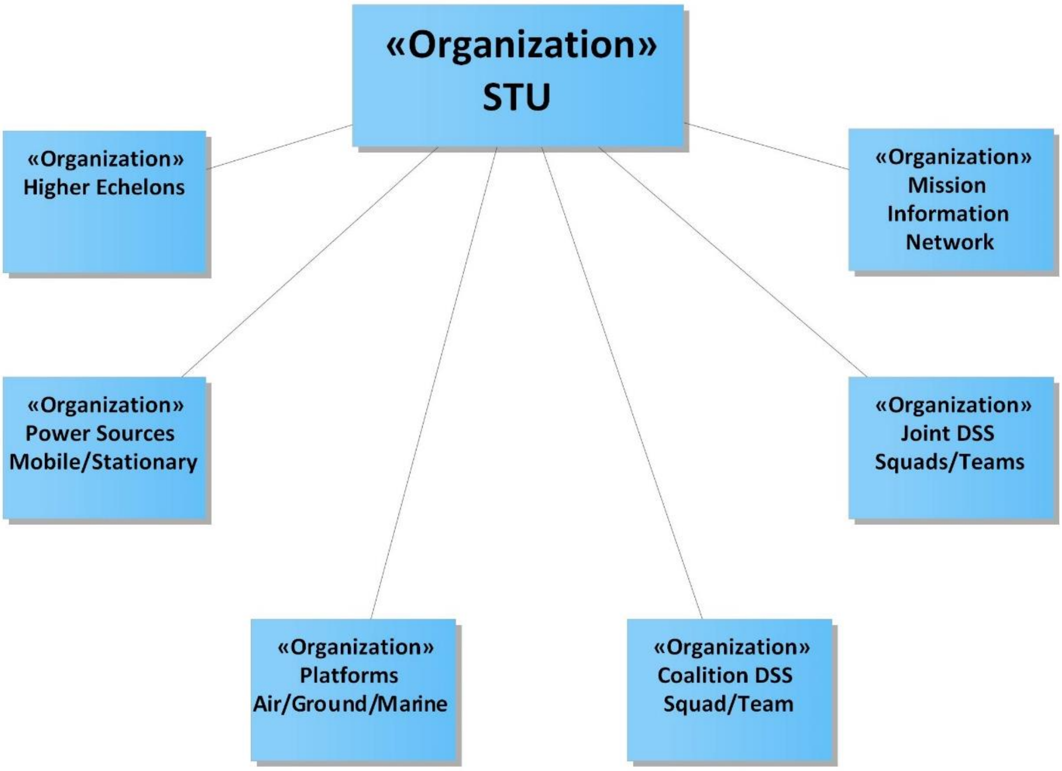
«Organization» STU
«Organization» Higher Echelons
«Organization» Mission Information Network
«Organization» Power Sources Mobile/Stationary
«Organization» Joint DSS Squads/Teams
«Organization» Platforms Air/Ground/Marine
«Organization» Coalition DSS Squad/Team

Figure 2-13 – Information Relations of a DSS Soldier-STU

2.3.1 DSS STU/Team

The **Soldier-STU** here is seen as a unit of soldiers with a specific number and a specific organisation in accordance to the branch, mission and task. They are using DSS which may be configured differently to provide role-specific capabilities and to provide added value when cooperating as a STU/team.

The synchronised information space provided by the DSS equipment, in a STU, is capable of being tailored according to the demands as a platoon, a STU or a team, independently from the voice network organization. It processes information according to CROP principles and provides user-friendly information to soldiers. Common Relevant Operational Picture (CROP) principles work as the name suggests on the following:

- **Commonality:** the same picture is available to all participating members in an operation; This also means that CROP fuses information from multiple sensors to present one coherent picture;
- **Relevance:** the geographical extent and contents of the operational picture is tailored based on relevance (e.g. the infantry STU will only be given the tactical picture, whereas the Brigade or Division Command Post would have the operational level picture). This principle is also referred to as *No information Overload*;
- **Operational:** CROP ensures that all aspects which impact operational planning and conduct are available to the soldier e.g. Enemy ORBAT and disposition, FLOT, Target Data, Fire Support available in range, ammunition state, decision support (e.g. reaction times for enemy reinforcements,, possible areas of influence of the enemy during the period of own planned operations, etc.), target designation, dynamic terrain analysis, geofencing guard zones to alert users when tracks violate guard zone settings, etc.;
- **Timeliness:** Timely access to all *relevant* geo-information is critical. Information gathered and relevant for own, joint or combined forces as well as for supportive participants is to be made available to the DSS-Soldier-STU in or as near to real time, as possible**.**

2.3.2 Higher Echelons

Higher Echelons is the main node from the perspective of DSS STU/Team. The closest **Higher Echelon** is the Platoon Commander. Between these nodes, the flow of information is crucial for achieving the required coordination in a mission.

2.3.3 Mission Information Network

The Mission Information Network is a tactical communications system from the command posts at the front to the rear boundary. It consists of a communication infrastructure and network components. The communications structure can use terrestrial and airborne assets as well as space-based resources.

It is capable of supporting multimedia tactical information systems within the mission area. It enables forces to plan, prepare, and execute multiple missions and tasks simultaneously.

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

The Mission Information Network provides

- Infrastructure for secure high-speed, interoperable voice and data communications network down to the battalion level;

- On-the-move networking -- a mobile infrastructure maintains connectivity to the network, without the need to stop and set up communications;
- Command from division, to brigade, to company, through a completely ad-hoc, self-forming network with access to timely, relevant and actionable information.

Sample services are:

- Email Delivery;
- Web Services;
- Centralized software distribution;
- Assured computing services.

Sample applications are:

- Battle management systems;
- Medical information systems;
- Combat support systems;
- Business applications.

Sample programmes are:

- LandWarNet: https://en.wikipedia.org/wiki/LandWarNet
- Joint Network Node Network: http://www.globalsecurity.org/space/systems/jnn.htm
- Warfighter Information Network-Tactical: https://gdmissionsystems.com/c4isr/warfighter-information-network-tactical-win-t

2.3.4 Joint DSS STUs/Teams

Joint DSS STUs/Teams are forces from other branches including Airforce, Navy and, if applicable, Marines cooperating in a common mission area. To exchange tactical information, besides voice communication, the DSS's of joint forces shall be enabled to communicate without extra equipment.

The DSS's shall be capable to exchange tactical information via predefined rules and, if necessary, using cross domain gateways in order to avoid IT-security gaps.

2.3.5 Coalition DSS STUs/Teams

Combined DSS STUs/Teams are cooperating in a common mission area within their area of responsibility. While joint forces are of the same nation, combined forces are built up from allied nations with their own national DSS.

To exchange tactical information, besides voice communication, the DSSs of combined forces may be enabled to communicate with minimum extra effort. It is a common practice that most nations have their own nation-made communication equipment with proprietary radio wave forms. This prevents direct communication.

The concept of STANAG 4677 is to use a common "Interoperability Radio", provided by a host nation, as additional equipment for each STU or team, which will enable combined multinational tactical data exchange, before Software Defined Radios, with a common waveform, become available or other communication means (civil mobile networks) are used by Soldier Systems.

The DSS's shall be capable to exchange tactical information via predefined rules and, if necessary, using cross domain gateways in order to avoid IT-security gaps.

2.3.6 Platforms Ground/Air/Marine

Platforms of any type are usually equipped with some sort of C4I equipment and interfaces to connect **DSS STU/Team** seamlessly. The connection can be wired or wireless, depending on mounted or dismounted fighting method.

Platforms can provide long range radio communication capabilities to access the Mission Information Network. Also, information, prepared in advance of the mission and stored in the platforms C4I-equipment (e.g. map sets and data bases of important facts of the mission area) shall be made available to the **DSS STU/Team**.

2.3.7 Power Sources Mobile/Stationary

Information to be exchanged between **Mobile/Stationary Power Sources** and the **DSS STU/Team**, relates to power status information, e.g. power demand of the DSS, power capabilities of the source and how to transport and condition the power for recharging or supplying the DSS.

2.4 NOV-4 Organisational Relationship Chart

2.4.1 Organisation of Small Tactical Units (STUs)[4]

Historically, a "STU" in the US and some other Army was a sub-unit of a Section, consisting of a few as two soldiers to as many as 12 and was originally used primarily for drill and administrative purposes (e.g., billeting, messing, working parties, etc.). A WWI British Infantry Company consisted of four platoons, each of about 50 men, under a Lieutenant or Second-Lieutenant, assisted by a Sergeant. Within a platoon were four sections of 12 men. The cavalry used different terms but had similar organisation. In March 1917, the German army also restructured their standard German infantry STUs based on a seven-man team as a manoeuvre element, and a fire element based on a four-man team armed with the M-1908/15 light machine gun. The German Wehrmacht of World War II retained that basic infantry STU structure.

The US Army employed the eight-man rifle STU through WWI and until the late 1930s. In 1939 rifle STUs were no longer organized into sections. Instead, the STUs were reorganized into a 12-man unit of three elements, or teams reporting directly to the platoon commander (an officer, usually a second lieutenant), assisted by a sergeant.

Currently (May 2018), US Army rifle STUs consist of nine soldiers, organized under a STU leader into two four-man fire teams; The STU leader is a staff sergeant and the two fire team leaders are sergeants. Mechanized infantry and Stryker infantry units are equipped with M2A3 Bradley - infantry fighting vehicles and M1126 Stryker - infantry carrier vehicles, respectively. Unlike the ROAD era mechanized infantry units, none of the vehicle crewman (M2A3 - three, M1126 - two) are counted as part of the nine-man rifle STU transported by the vehicles. The term STU is also used in infantry crew-served weapons sections (number of members varies by weapon), military police (twelve soldiers including a STU leader divided into four three-man teams, with three team leaders), and combat engineer units. US Marine Corps STU comprises 12 Marines, with three fire teams of three Marines each with an assistant STU leader and a STU systems operator[5].

The French Army infantry STU is composed of two fire teams based on the effective range of their weapon systems—a three hundred-meter team and a six hundred-meter team—and a vehicle crew. The French army organizes its infantry STUs around three-man cells, with the option of attaching specialists to them. Depending on the source, the composition of dismounted teams varies from two three-man teams to a three-man team and a four-man team. A STU leader is in charge of the two dismounted teams and the vehicle crew. The French army considers the STU a BIU (Basic Infantry Unit), as the cells are specialized based on their role in the fight and therefore incapable of independent action.

In most armies, STUs or Sections are organised under Rifle Platoons. A Rifle Platoon normally consists of a small platoon with three or four sections (Commonwealth) or STUs (US). In some armies, platoon is used throughout the branches of the army. In a few armies, such as the French Army, a platoon is specifically a cavalry unit, and the infantry use "section" as the equivalent unit. A platoon of the German Bundeswehr is called "Zug" in German. A unit consisting of several platoons is called a company/battery/troop.

[4] https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2018/Kamara-Infantry-Rifle-Squad/;https://en.wikipedia.org/wiki/Squad

[5] https://www.marines.mil/News/Press-Releases/Press-Release-Display/Article/1516580/marines-announce-changes-to-ground-combat-element-aimed-at-improving-lethality/

2.4.2 Organisational Chart

The Organizational Relationship Chart identifies the key players in the operational domain and illustrates the organizational relationships among them. Key players are best described using role-based descriptions, independent of the fact whether a role actually involves an entire operational node or just a single human role.

Organizational relationships are important to depict in a NATO Operational View, because they can illustrate fundamental human roles (e.g. who or what type of skill is needed to conduct operational activities) as well as management relationships (e.g., command structure or relationship to other key players).

The major challenge to define such a chart for the DSS at a European level is due to the different approach each European nation uses. A Generic Organizational Relationship Chart was therefore developed, as is shown in Figure 2-14, which has been taken from the previous STASS study and expanded at the STU level.

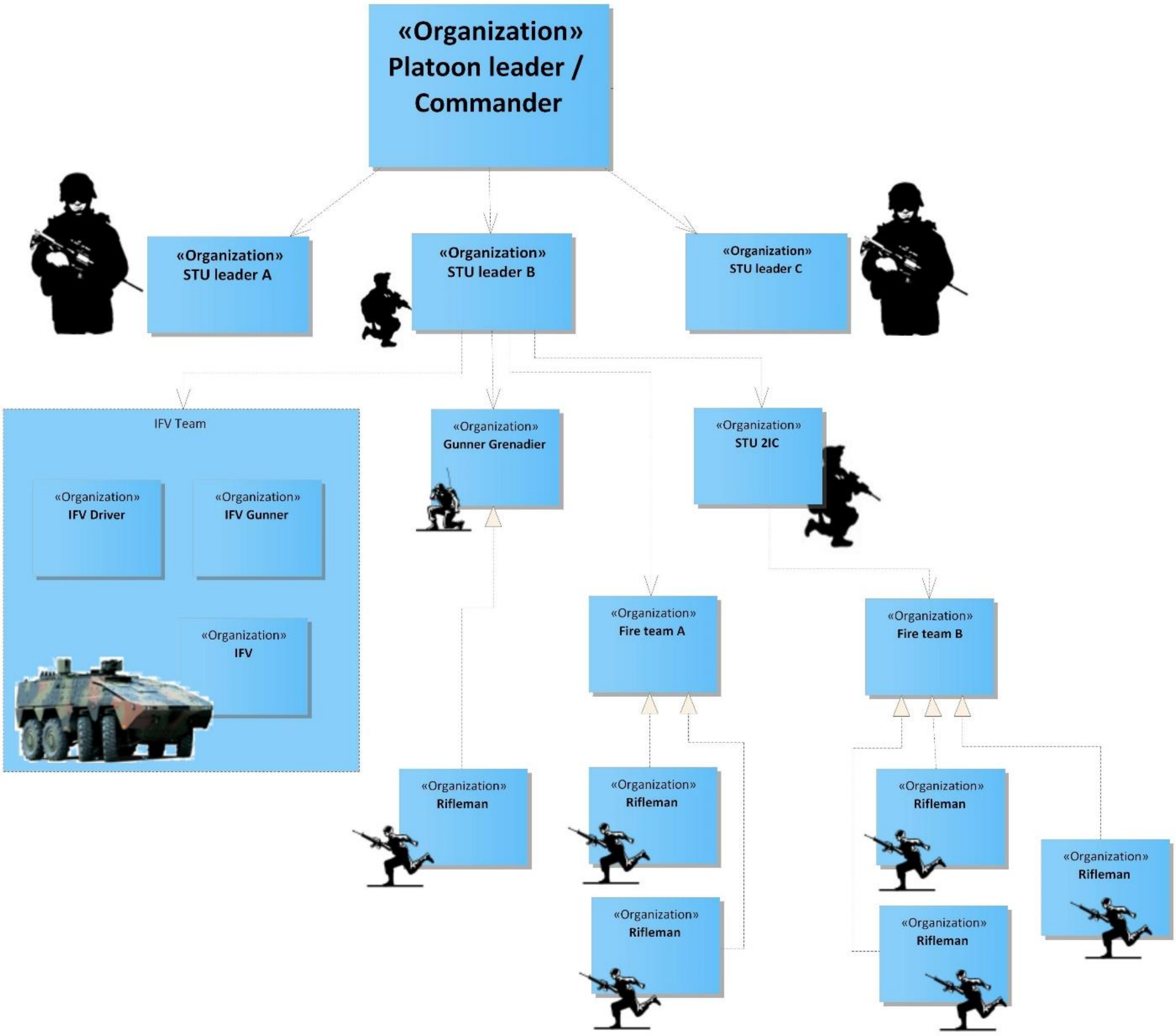
«Organization» Platoon leader / Commander
«Organization» STU leader A
«Organization» STU leader B
«Organization» STU leader C
IFV Team
«Organization» IFV Driver
«Organization» IFV Gunner
«Organization» IFV
«Organization» Gunner Grenadier
«Organization» STU 2IC
«Organization» Fire team A
«Organization» Fire team B
«Organization» Rifleman
«Organization» Rifleman
«Organization» Rifleman
«Organization» Rifleman
«Organization» Rifleman
«Organization» Rifleman

Figure 2-14 – Generic STU Organisational Relationship Chart

A soldier (with his/her specific role) is organized in fire teams as the smallest unit. A fire team is designed to optimize their situational awareness and movements and to coordinate their effects (fire) within a hostile environment. They are grouped by two or three fire teams into an STU (a section (Europe) or squad (US))) in coordinated operations, which is usually led by a STU Leader. If a STU operates in two fire teams, the 2nd in command becomes the leader of the 2nd fire team.

Two to four STUs are grouped as a platoon, led by the Platoon Leader who is assisted by a Platoon Sergeant and a Warrant Officer. In total, a platoon can consist of 16 to 40 soldiers.

The Mechanized Infantry uses its armoured vehicle for transport and, during battle, for fast movement and fire support. A typical mission domain of the Mechanized Infantry is urban warfare. The vehicle crew usually consists of a Vehicle Driver, a Gunner and the Vehicle Commander. Depending on the nation, the Vehicle Commander and the STU Leader are two soldiers or it could be just one soldier under command of the Platoon Leader. Then, the Vehicle Commander leads the dismounted soldiers from the vehicle.

The Light Infantry Platoon usually uses land and airborne vehicles for transport to the mission area. They operate in STUs or self-sustained teams and accomplish their special missions often without logistic or fire support.

Command relationships can alter depending on the fighting conditions.

2.4.3 Generic Roles

Three major roles are identified with respect to the DSS. The simplest one is the basic rifleman. By adding functionality or equipment to his DSS, the DSS is used with enhanced functions for specific roles (Gunner, Grenadier) and / or missions. The different roles are depicted in the Figure 2-15. A description of those roles will follow below.

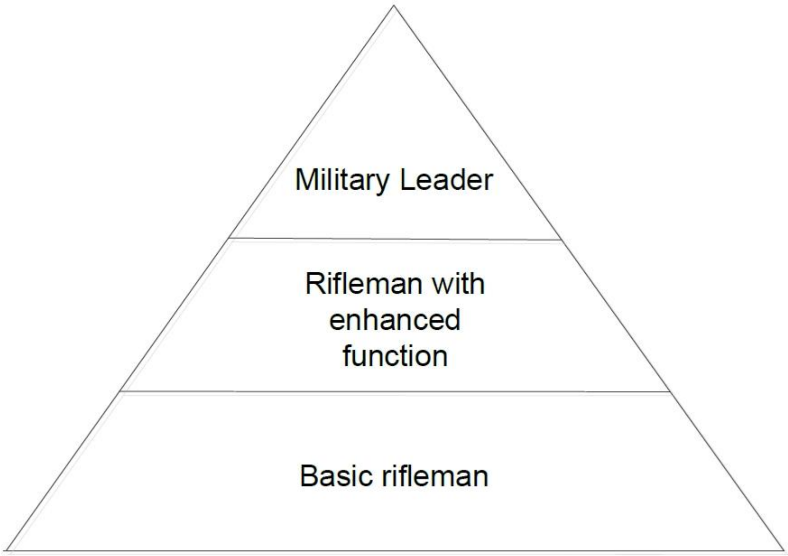

Figure 2-15 – Generic Roles of Infantrymen

2.4.3.1 Basic Rifleman

The DSS of the Basic Rifleman shall provide the suitable functionalities to enable and support a soldier’s basic capabilities.

This system may be used as a core system which is then extended to tailor for special roles with enhanced functions or for the Leader.

2.4.3.2 Rifleman with Enhanced Function

The DSS for a Rifleman with Enhanced Function provides additional specific capabilities depending on the specialisation of the rifleman to play specific roles. Examples for a Rifleman with Enhanced Function are:

- Gunners (Machine Gun, Grenade Launcher, Etc.);
- Snipers;
- Combat Medics;
- Communication Specialist;
- JTACs (Joint Terminal Attack Controllers);
- Signals, etc.

Such a DSS might be built upon the core system of a Basic Rifleman and use additional specialized equipment.

2.4.3.3 Military Leader

This role includes all designated leaders and commanders from STU up to company level:

- STU leader and Second in Command (2IC);
- Platoon leader and 2IC;
- Company commander and 2IC.

The DSS for a military leader needs to include enhanced C4I and communication capabilities to higher echelons or other similar units.

2.4.3.4 DSS-Services to Soldier Role Mapping

For the specification and design of a DSS, it is important to know about the services the system needs to provide for each role. This view is an addition to Chapter 2.3 which defines the information spaces. This view shows which role needs access to a certain service, thus not defining the needed information but the equipment to fulfil the role.

Table 2-9 shows a typical mapping of services to the Generic Roles. It does not represent all roles and services possible.

Soldier Role Information Exchange Requirements	Basic Rifleman	"Enhanced" Rifleman	STU-leader
Voice com to STU	●	●	●
Voice com to platoon			●
Data distribution	●	●	●
Blue-force tracking	●	●	●
Ear, passive and active protection	●	●	●
Direction finding		●	●
Situation awareness and maps		●	●
Route navigation		●	●
Night vision with overlay		●	●
Video grabbing and video distribution			●
Wireless PTT-control	●	●	●
Exchange of tactical objects to other BMS			●
Geographical position with higher accuracy and integrity (MIL-GPS)			●
Ergonomic GUI (Large display with multi-touch)			●
Power management		●	●
Radio management		●	●
Zeroizing and isolation of specific DSS		●	●
Zeroizing and isolation of specific DSS remotely			●
Displaying images at the GUI		●	●
Distributing images			●
Permitting STU-access for new members			●
Creating and distributing reports and text messages		●	●
Energy system configuration tools	●	●	●

Table 2-9 – DSS-services to Role Mapping

2.4.4 Other Branches for Joint Operations

2.4.4.1 Principles of Operational Support

During battle, the infantry company (with its DSS STUs) is normally supported by other arms and services. The principles of operational support warrant that the supporting arm or service be provided with clear instructions (normally as a part of the Battalion Operational Order) with respect to the following:

- The location or area, or exact extent of area, where support is required. This would also entail specifying boundary demarcations like Fire Support Coordinating Line (FSCL), Forward Line of Own Troops (FLOT), Forward Line of Enemy Troops (FLET), etc.;
- The tactical purpose or intention (this normally includes the immediate operational aim as well as the higher commander's intent);
- Date and time (including start and end timings);
- The sequence of the required support, and;
- The kind of safeguard measures, given by the company/STU during preparation and execution of the required support.

During OOTW (Operations Other Than War), which cover a large spectrum of operational scenarios ranging from *Support to Civil Authorities, Peace Support Operations, Disaster Relief, Search and Rescue, Consequence Management (Maintain/Restore Essential Services), Anti-Terrorism*, *Counter Insurgency*, etc., the STU/Force HQ may need to seek assistance in support of military operations from civilian organisations. In all such operations, it is imperative that the soldier understands the tenets of CIMIC (Civil Military Cooperation) and the actions of civilian actors on the ground, such as local governments, media, NGOs, humanitarian actors, and private companies, all of whom shape the increasingly complex environment.

At the same time, the growing reliance on certain supporting functions like logistics, will require increasing cooperation on securing civilian networks and operations against physical or cyberattack, in order to counter vulnerabilities of the civilian sector supporting frontline military operations.

Figure 2-16 shows the relations of the DSS STU to other branches as a consequence of their support to the Company.

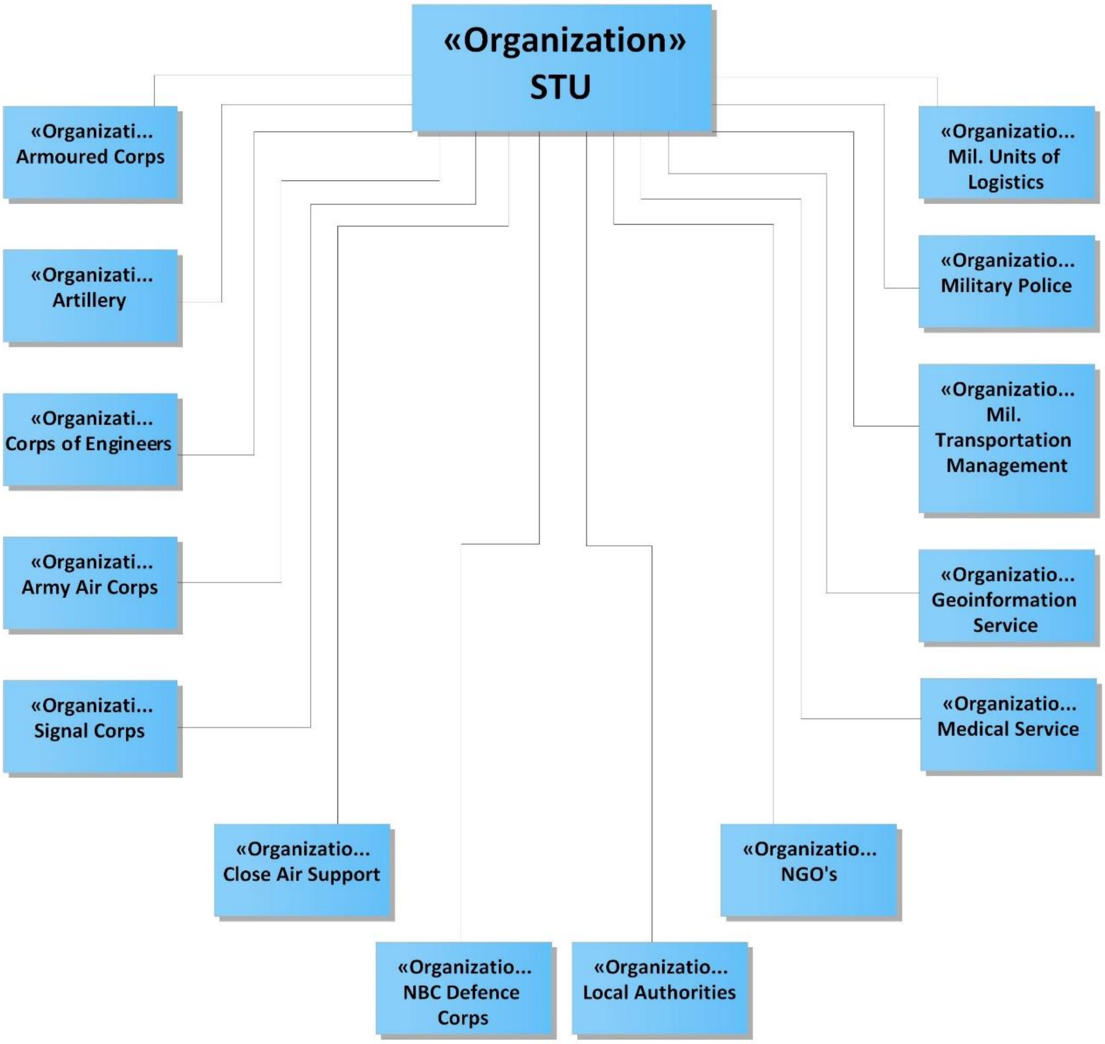

Figure 2-16 – System Context Action with Other Branches

2.4.4.2 Armoured Corps

An armoured troop or platoon, subordinated to the company, is often the main weapon of the company commander. The armoured platoon operates mounted as a closed unit.

The armoured platoon can be the focal point of the operation in terms of protected mobility and fire power.

The associated requirements are:

- Coordination between the infantry and armoured sub-unit commanders;
- Independent and secure communication link during battle;
- Quick exchange of current observation and reconnaissance results;
- Exchange of target data and allocation of targets.

2.4.4.3 Artillery

The artillery supports the company by fire support. The company commander and/or platoon leaders request fire support during battle.

Within the company, the battalion commander orders a Joint Fire Support Team (JFST) to operate together with the company. The JFST is part of the company network.

During battle the JFST:

- Maintains communication with the company commander for consulting;
- Receives and forwards request for fire support;
- Reports observation results;
- Orientates the company via its own fire.

The fire support request to the JFST contains:

- Target position;
- Target description;
- Required striking effect;
- Date/time.

2.4.4.4 Corps of Engineers

The Corps of Engineers is ordered to work together with the company, supporting the movement of the Company by providing and denying mobility. The tasks given to the Corps of Engineers include:

- Laying of minefields and obstacles as well as breaching obstacles and minefields;
- Crossing of water and other obstacles;
- Clearance of unexploded ordnance blinds.

2.4.4.5 Army Air Corps

The army air corps with its antitank helicopters supports a company temporarily. Additionally, they are able to provide medical evacuation, observation and reconnaissance in their entire operational area.

Location and time to establish the communication between the Company and the pilot will be intimated to the company by the Battalion HQ.

Operations of antitank helicopters are led by the Brigade. The battalion informs the company in advance if the operation is within its area of responsibility. In case of support of antitank helicopters for the Company, the commander of this operation establishes communication with the Company Commander via the battalion network.

The Company Commander makes available the following information:

- Forward Line of Enemy Troops (FLET);
- Forward Line of Own Troops (FLOT);
- Targets with priority;
- Enemy’s and own minefields.

2.4.4.6 Signal Corps

The Signal Corps sets up an automated communication network in the tactical control area. It provides communications connection points for the command post for a brigade size or higher unit. If required for the operation, the company can use the communications connection points. Gateways and network accesses provide the interface between networks.

2.4.4.7 Close Air Support

CAS is defined as air action against targets that are in close proximity to friendly forces and require detailed integration of each air mission with the fire and movement of these forces. In case operations are executed by the air forces for close air support, it can be necessary to limit the movement and/or the fire fight of the company, in space and time.

Details for coordination are:

- Planning of manoeuvre of the ground forces;
- Beginning of the attack;
- Determining time and duration of the close air support;
- Assigning and combating targets;
- Defining borders for the safety of the company;
- Apply special marking of own forces identifiable from the air;
- Tactical situation briefing of the air control team (ACT) or the Forward Air Controller (FAC).

Usually close air support is ordered at the battalion network level and coordinated by an ACT/FAC/ US AF Combat Control Teams. Co-operation between different NATO agencies such as the NATO Standardization Agency and the JAPCC has resulted in the development of common standards for *Forward Air Controllers* and these are now set out in STANAG 3797 (Minimum Qualifications for Forward Air Controllers). NATO FACs are trained to request, plan, brief and execute CAS operations both for Low Level and Medium/High Level operations and their training includes electronic warfare, suppression of enemy air defences, enemy air defence, air command and control, attack methods and tactics and weapons[6].

2.4.4.8 NBC Defence Corps

The tasks of the NBC Defence Corps are to monitor and assess CBRN threat /contamination and issue warning as well as assist in evacuation and decontamination procedures.

In case of defence or delaying operation, the NBC defence corps is located in the rear of the operation area to observe the NBC-status and to be protected against enemies' fire. During attack operations the NBC defence corps is in close distance to the company commander.

2.4.4.9 Military Units of Logistics

The maintenance service supports the company with maintenance by checking and repairing the equipment at the maintenance collection points. Maintenance can be provided by:

- Exchanging Line Replaceable Units (LRU);
- Supplying consumables;
- Providing recovery support.

The company ensures the transport of defective equipment to the collection points with own resources. Maintenance troops ordered to provide close support to the company are supplied by the company.

[6] Joint Publication 3-09.3 Joint Tactics, Techniques, and Procedures for Close Air Support (CAS)

2.4.4.10 Military Police

The military police support the company by carrying out:

- Military security tasks;
- Military traffic control tasks.

The military police undertake its duties without special order. It supports:

- Investigations;
- Monitoring of environmental pollution;
- Regrouping and redeploying stragglers;
- Regrouping and transporting prisoners of war;
- Securing areas and facilities;
- Securing of convoys;
- Preparing and conducting marches and relocation movements.

2.4.4.11 Military Transportation Service

The Military Transportation Service provides management and resources for the transport of military units to their mission area. In general, military units are transported by road, rail, air and sea.

Rail-transport:

By rail a company can be transported via large distances without stress for personnel and material. The company has to find a suitable location for loading and to prepare for it.

Sea-transport:

For large-scale transport the company can be moved by sea-transport, especially if the transport is not time critical or the material is not suitable for air-transport. Transport to and from the ports is to be done by marsh or by rail. The company has to take care for suitable measures to protect the material against moisture.

Air-transport:

Generally, only part of an Infantry Company will be air-transported by aircraft or helicopters over large distances over a short period of time. Air-transportation may be by landing at a forward airbase, while air – assault may be parachute landing, gliders, or even rappelling for vertical envelopment over obstacles like rivers, canals or heavy defences.

2.4.4.12 Geographic Information System (GIS) Service

A geographic information system (GIS) is a system designed to capture, store, manipulate, analyse, manage, and present spatial or geographic data. GIS applications are tools that allow users to create interactive queries (user-created searches), analyse spatial information, edit data in maps, and present the results of all these operations[7].

[7] https://en.wikipedia.org/wiki/Geographic_information_system

2.4.4.13 Medical Service

Usually two troops of armoured medical service are subordinated to the company. After rescue and first aid measures, the wounded will be transported to the medical service station.

2.4.4.14 NGO’s

A Non-Governmental Organization is an association of interests initiated by the civil society. NGO’s are independent from states and governmental representation and organizations. They are working on environmental, political and social issues. In a conflict area, the groups are most often represented by volunteers with a variety of capabilities to accomplish their engagement.

2.4.4.15 Local / International Authorities

The local authorities are represented by the country, district, and borough or community administration, depending on form of government and/or culture. In tribal cultures, the local authority is the chief of a clan or tribe. International authorities may be organisations like OCHA (Office for the Coordination of Humanitarian Affairs) and DPKO (Department of Peacekeeping Operations) /UN Force HQ.

2.5 NOV-5 Operational Activity Model

Operational Activity Model shall provide a clear picture of how operations are performed and thereby support analysis and design of services and systems.

Following sections describe Command and Control, Tasks and Activities from a company level point of view which is or may easily be broken down to STU level which is the focus of this study.

2.5.1 C4I Activities with Respect to DSS

Another decision cycle is Observe, Orient, Decide, Act (OODA) which is well known and was developed by military strategists and the US Air Force Colonel John Boyd, see Figure 2-17.

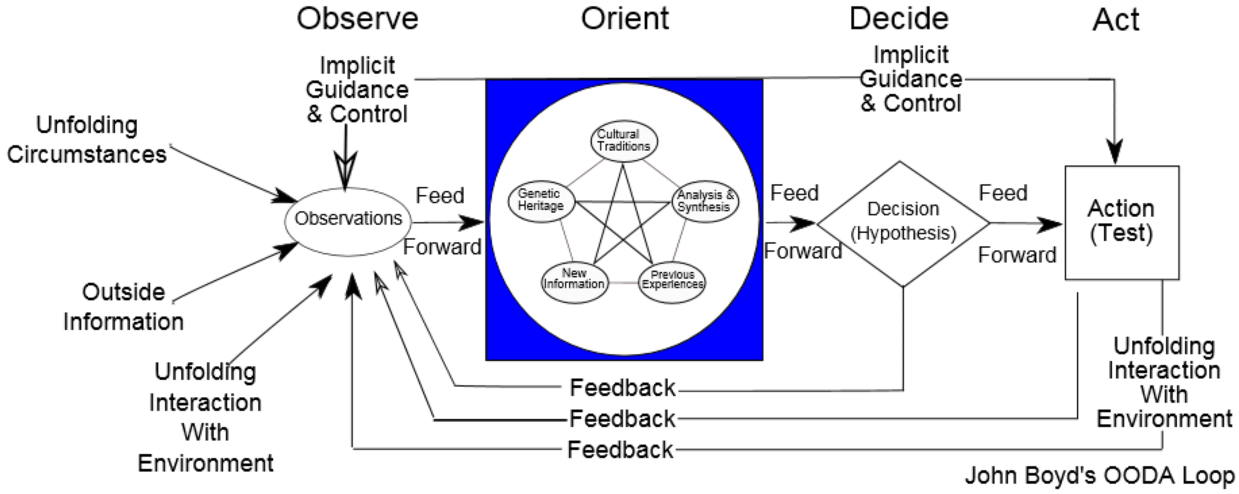

Figure 2-17 – Decision Cycle "Observe, Orient, Decide, Act (OODA)"

The US Army uses the seven-step process "Military Decision-Making Process (MDMP)" with the basic steps:

- Receipt of Mission
- Mission Analysis
- Course of action (COA) Development
- COA Analysis (aka Wargaming)
- COA Comparison
- COA Approval
- Orders Production, Dissemination, and Transition

2.5.1.1 Observation and Acquisition of Situation

The enabler for the mission is the order which the company commander receives from the battalion commander. The platoon leader receives his order from the company commander and the section leader his order from the platoon leader.

The acquiring of the situation provides the prerequisites for appropriate planning and consequent acting. A battle is characterized by often changing and unclear situations. Thus, each commander/leader complements the situation awareness by continuously acquiring and processing relevant information. The company command post supports the company commander by acquiring, processing and providing information as well as coordination the mission support.

Information can be gathered from:

- Orders;
- Own observation and assessment;
- Subordinate units;
- Neighbouring forces;
- Other echelons (ISR services, e.g. Air Force, intelligence services);
- News, newspaper;
- Analysis of documents, maps or satellite images provided by services;
- Statements of local population.

Fast and comprehensive messaging is the groundwork for a current and correct assessment of the situation. Exchanging graphics and sketches with exact values of position, time and numbers are optimal to achieve a good common situational awareness.

The content of messages is:

- Where (is the enemy, position, direction, distance););
- Who (Type, strength););
- When;
- How (behaviour, mode););
- What (do I do).).

Speculations and assumptions should be marked accordingly.

Important information should be stated on maps, whereby the situation map should display clear and up-to-date information, on the basis of which of the military leaders are able to plan, to issue orders and to control.

Situation maps shall display:

- Area organization, borders, reference positions and other control and coordination lines;
- Command posts, areas, battle positions;
- Facilities of combat support, mission support and C2-support;
- Organization for combat;
- Area of medical point;
- Important details for the conduct of operations;
- Forces and units of higher echelons, and if needed subordinate echelons;
- Information about neighbour forces and other units in the area of interest;
- Key terrain, geographical constraints, contaminated, blocked or unblocked areas and barriers;
- Enemy-related information.

2.5.1.2 Assessment and Decision Making

While assessing the situation, it is important to consider:

- What is the intention of the higher commander;
- What effect is required;
- What are the constraints to my actions;
- Is there a fundamental change in the situation and what are the conclusions of it;
- What additional information is required;
- What has to be decided and when.

During the operation the assessment of the situation is often limited to whether and when there is a new decision to be made. Following the intention of the higher echelon, the leader is evaluating the capability of its own unit and that of the enemy, as well as the positive or negative influence of environmental factors.

After evaluation of the order and the assessment of the situation, the leader comes to the decision:

- Who;
- What;
- How;
- When;
- Where;
- For what purpose.

The decision is the foundation for all following steps.

2.5.1.3 Operation Planning

After receiving the order from the battalion commander, the company commander first places arrangements with the leaders of cooperating and subordinated units. If the present situation allows, the company commander will perform the following actions:

- Firstly, he develops a preliminary course of action according to his first impression of the situation;
- Secondly, he develops a plan for scouting and information gathering and places orders to the respective team;
- Thirdly, the company commander, the platoon leaders and cooperation units perform the scouting and information collection tasks.

Then, all surveillance and reconnaissance results are to be presented graphically and explained. With this, the company commander develops the course of actions.

2.5.1.4 Order Production and Dissemination

All company leaders issue orders mostly orally supported by graphical representations. If possible, they brief in the relevant terrain so the intent can be easily reproduced. During the operation, short orders are placed by voice and/or radio.

Leaders lead by examples, signs or keywords to initiate prepared actions and to relieve radio communication.

Platoon leaders issue orders to all soldiers of the platoon, if possible. Orders shall be complemented, if required, during operation interval.

While briefing, the leaders can proceed as follows:

- Check completeness;
- Receive messages from subordinates;
- Brief the terrain;
- Place complete order;
- Place single order;
- Order radio frequencies;
- Clarify questions, and;
- Synchronize watches.

2.5.1.5 Execution Control

The leaders need to evaluate the state of the implementation of the orders given, as well as the status of the units. Controlling the action shall improve the performance of the operation.

Execution control is performed by:

- Letting soldiers confirm orders;
- Controlling own execution, and;
- Requiring confirmatory message when an order/mission has been completed.

2.5.2 Generic Tasks for DSS STU during a Mission

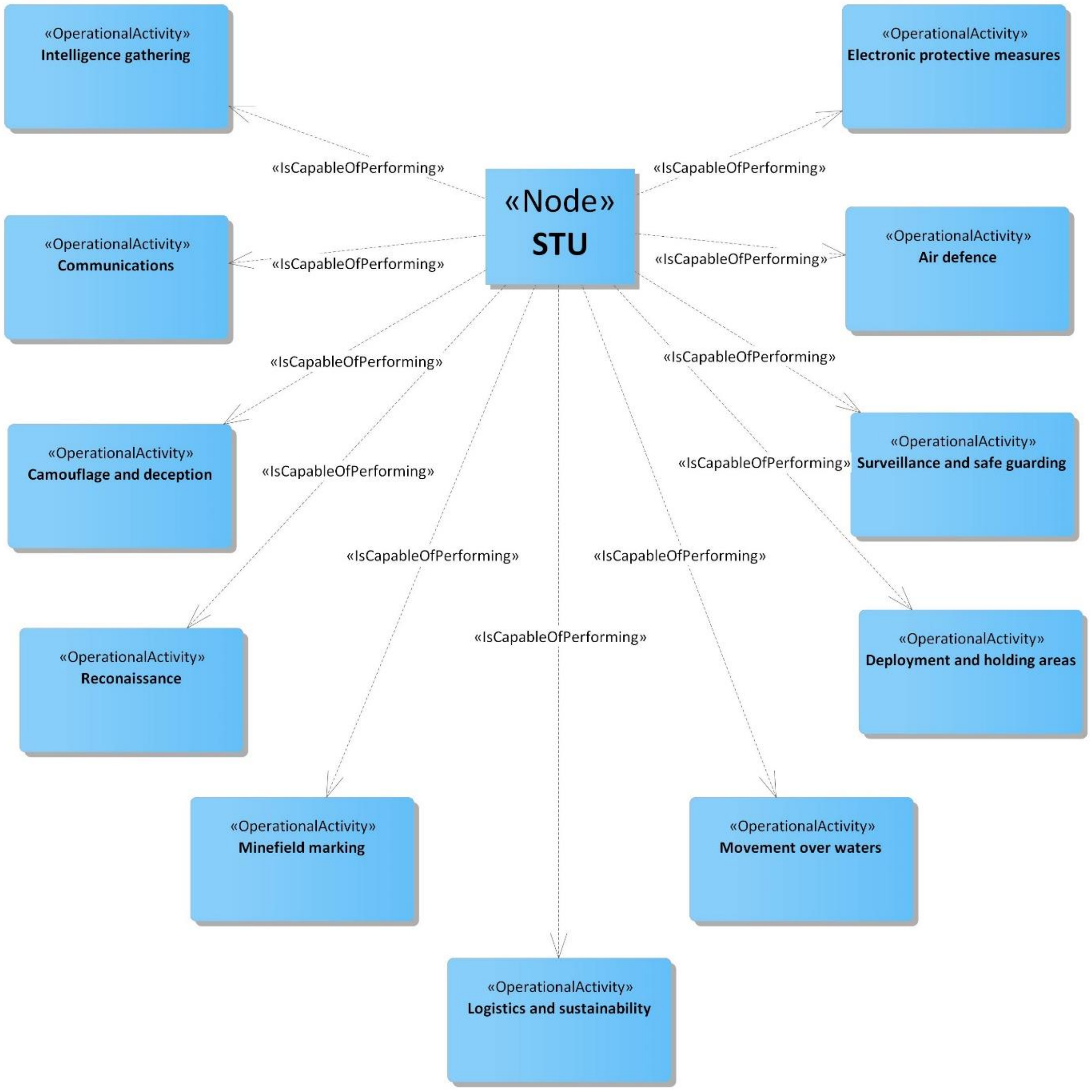

Figure 2-18 – Generic tasks of a STU in a mission

2.5.2.1 Intelligence Gathering

The purpose of intelligence gathering is to gain timely, reliable and complete information for the mission.

The purpose of combat intelligence, including scouting, is to guard own forces from surprises and provide the foundation for a targeted approach.

A reconnaissance patrol, also armoured, may consist of two sections, two armoured vehicles or a platoon, depending on situation and order.

Reconnaissance patrols are responsible for:

- Making exploratory contacts with the enemy;
- Finding the type, strength, expansion, status, behaviour as well as intention of the enemy;
- Finding any barriers and accessibility issues in the terrain blocking the progress of own forces;
- Finding the enemy's flanks as well as terrain unoccupied by the enemy;
- Observing unoccupied areas and gaps between own military elements;
- Establishing and maintaining contact to military elements at the front as well as to neighbours, and;
- Securing the march upfront the advanced guard.

2.5.2.2 Reconnaissance

The purpose of reconnaissance is gathering information about the terrain as well as potential enemies and their activities or resources. This includes, but not limited to:

- Quality of the network of roads and streets;
- Accessibility of ways away from paved roads;
- Possibility to install battle positions, observation posts also in limited visibility conditions;
- Possibility for camouflaged positions;
- Positions to establish and maintain contact to neighbour forces;
- Enemies' positions and deployed units, and;
- Enemies' capabilities.

2.5.2.3 Communications

Communication shall be established and maintained:

- From subordinated to superior unit;
- Between neighbours from left to right;
- From supporting to supported unit, and;
- From guest to hosting unit.

2.5.2.4 Surveillance & Safe Guarding

Surveillance is one of the key aspects in a mission. It is the continuous systematic observation of the surrounding environment with the purpose of detecting possible threats. A soldier first tool for surveillance are his or her senses. Due to the technological progress surveillance is not limited to the human senses, but can be aided by technology e.g. thermal imaging thermal imaging or sound detection.

Surveillance is also a key part of safeguarding. The company safeguards itself during mission at every location, at every time and in every situation. This must be performed without a special order within its allocated area.

The purpose is:

- To safeguard own forces against enemy attacks on the ground and via air;
- To achieve time and space for countermeasures in case of enemy attacks;
- To protect objects and areas from the enemy, and;
- To deny or hinder reconnaissance by the enemy.

Continuous measures are:

- Concealment, coverage, dispersal;
- Avoiding detectable lights and noise;
- Inspection of persons and vehicles;
- Scouting and preparation of alarm positions;
- Barriers and intruder detectors;
- All-arms air defence and NBC protective measures, and;
- Securing communications.

2.5.2.5 Camouflage and Deception

Camouflage is extremely important, without sufficient camouflage the enemy can easily find and identify units and engage them, thus camouflage is important for the survivability and accomplishment of the mission. Due to technological developments, camouflage has evolved from colour of the clothing, to other techniques, as handheld thermal imaging devices can easily discover humans and electronic devices at night.

Hence camouflage may also be achieved by:

- Using coverage of the natural terrain;
- Shielding sources of heat;
- Avoiding noise, and;
- No coverage areas, against RADAR.

Deception, as defined by NATO, means: “Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests”. This not only means to lay wrong trails or trap the enemy by faking wrong or insufficient camouflage, but also to disguise its own strength from the enemy. Hence it is used as a tactical instrument to mislead the enemy and force him to predictable movements or actions.

2.5.2.6 Electronic Protective Measures

Forces always have to consider the possibility of being detected due to their own electro-magnetic emission. Electronic protective countermeasures are intended to hinder the enemy from doing that.

Tactical countermeasures are:

- Suitable battle position;
- Use of alternative command and control means;
- Change of position, and;
- Silence for radio, RADAR and LASER.

Technical countermeasures are:

- Use of encryption and disguise;
- Radio discipline (more difficult with data radios);
- Observation with laser-protected optics;
- Use of minimum transmitting power;
- Decreasing the antennas height, and;
- Changing the antennas beam characteristics.

2.5.2.7 Deployment and Holding Areas

It is important that the company arrives on time and is ready for fighting at the place of deployment. Depending on the area of operation and the available resource the type of transportation can differ. Soldiers may arrive at the place of deployment by foot, vehicle (land/air/sea) or air/parachuting. The way soldiers arrive at the scene greatly influences their fighting capabilities e. g. a platoon that has marched 30 km without pause and under pressure may be exhausted and lack concentration.

2.5.2.8 Movement over Water

For movement over water the STU adheres to time schedules and orders indicating where to transit over water. The company often waits in areas close to the transition point prior:

- To using ferries or bridges provided by engineer units or;
- To use crossing areas.

The company uses its own soldiers to safeguard the movement. The liaison officer of the company is in close contact with the head of the transition point.

If the company must cross over water bodies on its own, the company leader has to decide, where and how to cross and after scouting, if support has to be requested.

2.5.2.9 Air Defence

The company is constantly threatened by the enemies' aerial reconnaissance and air to ground attacks. The company protects itself by using passive and active air defence measures.

Passive Air Defence Measures include:

- Dispersal, concealment and camouflage;
- Avoiding making tracks;
- Observation of the airspace, and;
- Engagement of enemy low flying aircrafts and other airborne vehicles.

2.5.2.10 Minefield marking

The company is threatened by systematically or erratically laid mines as well as the risk of unexploded ordnance. To avoid this threat, forces are to be provided with reconnaissance information in order to overcome the minefield as well as for clearing the explosive ordnances. If available, the company uses subordinated engineering corps.

Laying barriers to hinder the enemies' movement takes place according to the order of the major unit on demand.

2.5.2.11 Logistic sustainment

Mission support provides services to mainly maintain the personnel, medical and logistic capabilities of a company. The efficiency of mission support influences the plan of manoeuvre of the company.

The timely initiation of medical services by the company leader takes priority in all situations. Personnel replacement is for battle casualties and logistic service is for the replacement of consumables, maintenance and repair.

2.5.3 Specific Tasks for DSS STU during a Mission

2.5.3.1 During Battle/Engagement

STUs are engaged with missions and operations within a spectrum of intensities and complexities. Combat operations are characterized by fast and frequent changes in the method of fighting, fire and movement, as well as de-concentration and concentration of forces.

The company/platoon/section leader coordinates fire and movement between his platoons and monitors every movement.

In open terrain the fight is often intensive, of short duration and medium to long distances, while in overcast, urban and wooded terrain, the engagement usually lasts longer as the movement of vehicles is limited thus, the mechanized infantry has to change often from mounted to dismounted fighting method and vice versa. Fighting in this environment is at short to medium distances.

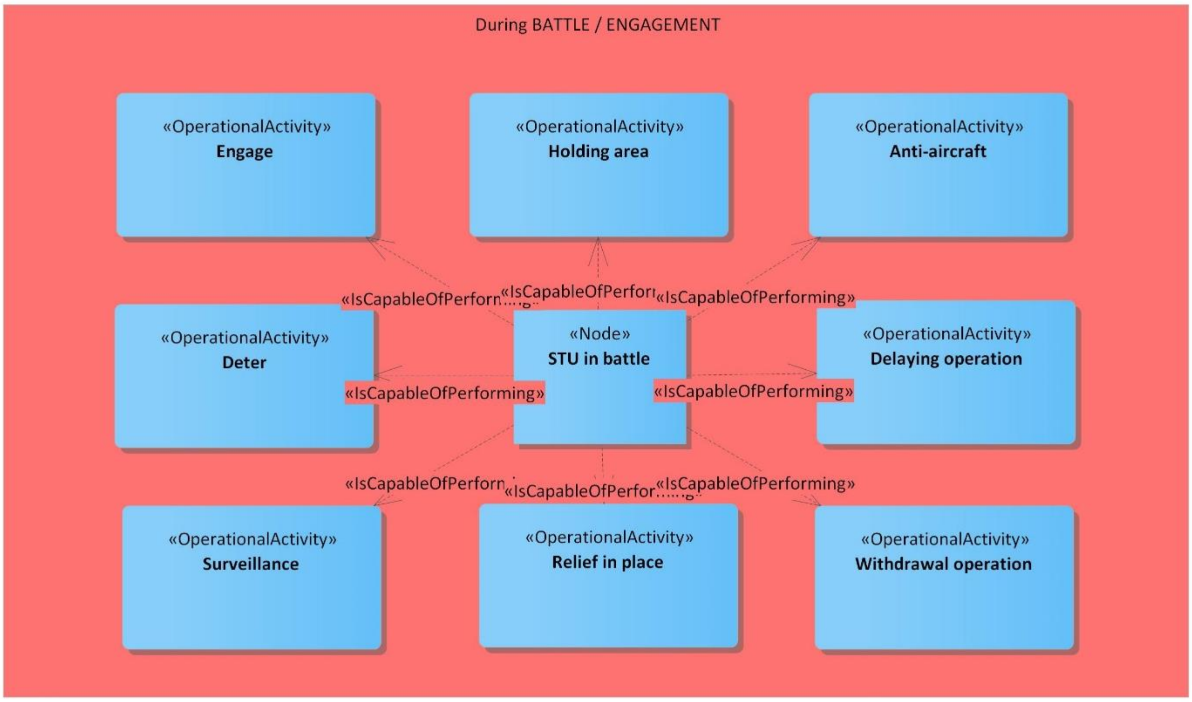
During BATTLE / ENGAGEMENT
«OperationalActivity» Engage
«OperationalActivity» Holding area
«OperationalActivity» Anti-aircraft
«OperationalActivity» Deter
«Node» STU in battle
«OperationalActivity» Delaying operation
«OperationalActivity» Surveillance
«OperationalActivity» Relief in place
«OperationalActivity» Withdrawal operation
«IsCapableOfPerforming»

Figure 2-19 – General elements of battle/engagement

From NATO perspective **Engage or Engagement** is “In the context of rules of engagement, action taken against a hostile force with intent to deter, damage or neutralize it.” (See Figure 2-19) In the context of a dismounted soldier this means not only to attack a knowingly hostile force, but also to react to hostile actions by civil or non-conventional combatants.

Deter or Deterrence is “The convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act.” (See Figure 2-19).

Deterrence, from a dismounted soldiers view, can be achieved by different means. The basic show of force brought by a variety of capabilities, e.g. Close Air Support, can be enough to deter an enemy, but these capabilities need to be available. Deterrence can also be achieved by smart coordination and deployment of personnel in the terrain, thereby even an inferior defender can maintain dominance over an area.

Holding an area or holding attack is from a NATO perspective "An attack designed to hold the enemy in position, to deceive him as to where the main attack is being made, to prevent him from reinforcing the elements opposing the main attack and/or to cause him to commit his reserves prematurely at an indecisive location." (See Figure 2-19).

Surveillance is defined as "The systematic observation of aerospace, surface or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means." (See Figure 2-19)

Anti-Aircraft actions in a context of a dismounted soldier or a dismounted soldier STU are greatly limited, since the equipment is usually not capable to engage highflying fixed wings or helicopters. Hence the only application is to engage low flying or landing rotary wings, which typically possible with weapons deployed with standard soldiers.

A **delaying operation** is defined as "An operation in which a force under pressure trades space for time by slowing down the enemy's momentum and inflicting maximum damage on the enemy without, in principle, becoming decisively engaged." (See Figure 2-19)

Withdrawal operations are "planned operation in which a force in contact disengages from an enemy" (see Figure 2-19). This especially means tight coordination since a military unit (unwillingly) left-behind will be captured or destroyed by the enemy. Normally the withdrawal operations are used to reorganize the forces at another position or line on which the enemy will be annihilated.

Relief in place is "An operation in which, by direction of higher authority, all or part of a unit is replaced in an area by the incoming unit. The responsibilities of the replaced elements for the mission and the assigned zone of operations are transferred to the incoming unit. The incoming unit continues the operation as ordered. This means the soldier must transfer his knowledge about the area, the mission itself etc. to new personnel.

2.5.3.2 During Peace Operations

A company, as a part of a battalion, can belong to task force or a mission contingent in the context of a peace mission or a humanitarian intervention.

Peace missions are measures undertaken as crisis response (e.g. by United Nations (UN) mandated multi-national forces, with affiliated international and local staff) which often take place in irrational and violent surroundings, where regulatory functions of an orderly state mechanism are absent.

The leaders of a STU have to be prepared for interoperability and cooperation with other nation's military forces, local government and NGOs. The cooperation can be complicated due to:

- Language barriers;
- Different interpretation (of cultural influenced) behaviour;
- National interests;
- Different legal interpretation, and;
- Differences in leading and operation principles, equipment and training.

The rules of operation, defined prior to the peace mission, differ:

- From a mission without military force (self-defence excluded););
- To missions where military force is a legitimate means to enforce peace.

"Leading from the front" is essential also in peace missions. Personal presence of the units' leader, in difficult situations or dangerous tasks, creates trust in uncomfortable surroundings. The presence of the leader has also an effect on the representatives of the conflicting parties, other military contingents or civil organisations.

In order of priority, a company may have to consider the following operations in a peace mission:

- peace keeping;
- peace enforcement;
- peace building, and;
- humanitarian operations;

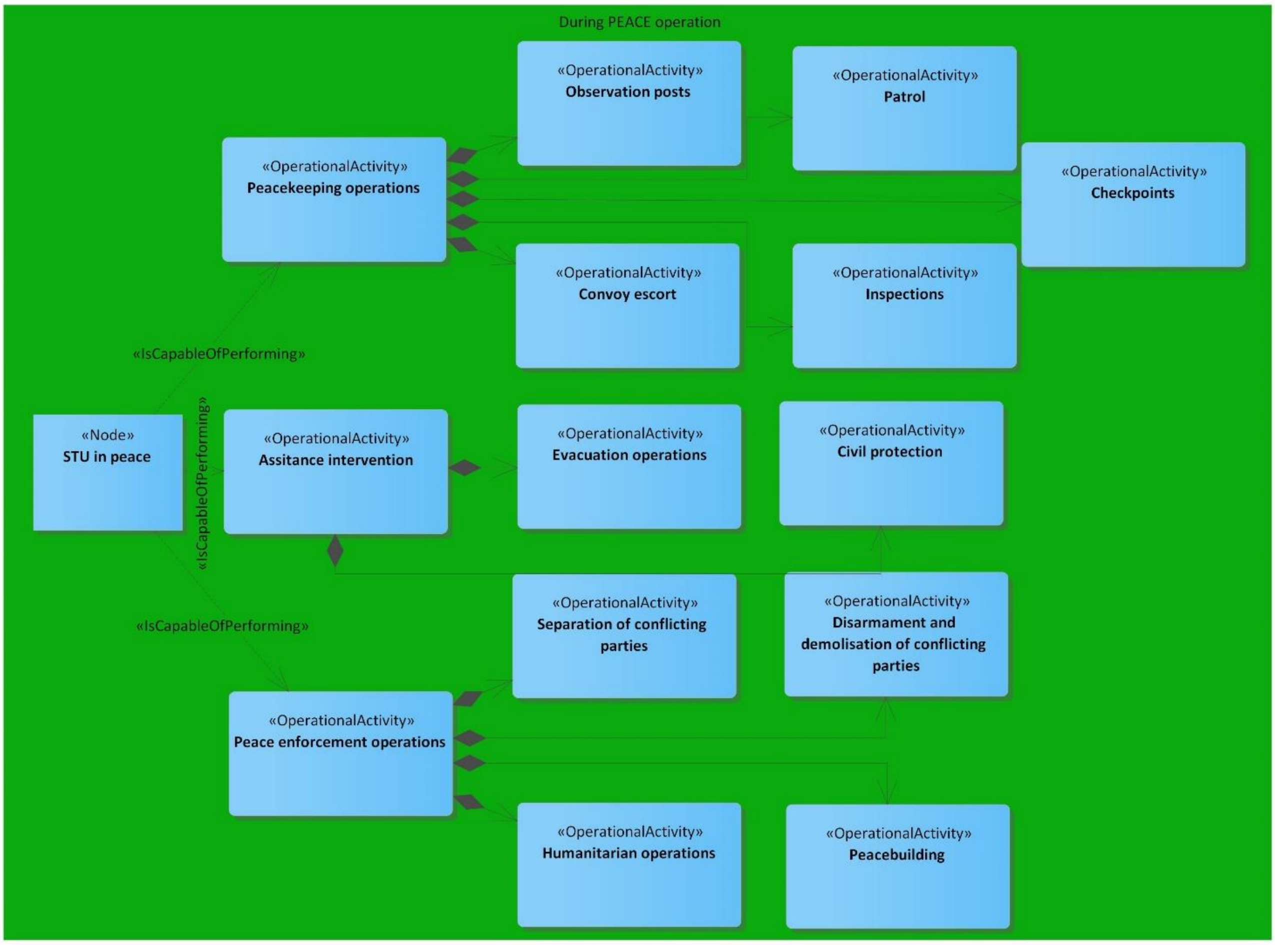
During PEACE operation
«OperationalActivity» Observation posts
«OperationalActivity» Patrol
«OperationalActivity» Peacekeeping operations
«OperationalActivity» Checkpoints
«OperationalActivity» Convoy escort
«OperationalActivity» Inspections
«IsCapableOfPerforming»
«Node» STU in peace
«IsCapableOfPerforming»
«OperationalActivity» Assitance intervention
«OperationalActivity» Evacuation operations
«OperationalActivity» Civil protection
«IsCapableOfPerforming»
«OperationalActivity» Separation of conflicting parties
«OperationalActivity» Disarmament and demolisation of conflicting parties
«OperationalActivity» Peace enforcement operations
«OperationalActivity» Humanitarian operations
«OperationalActivity» Peacebuilding

Figure 2-20 – General elements of a peace mission

2.5.3.2.1 Peacekeeping

Tasks for a company may be:

- Monitoring and controlling the peacekeeping measures;
- Monitoring of the area of separation;
- Establishing areas to protect the inhabitants;
- Evaluation of compliance of agreements, and;
- Enforcement of sanctions.

2.5.3.2.2 Peace Enforcement

Peace enforcement is characterized by agreed measures against the will of the affected state or conflicting parties.

Tasks for a company may be:

- Keeping the conflicting parties apart and;
- Disarmament and demobilisation of the conflicting parties.

2.5.3.2.3 Peacebuilding

Peace building supports the creation of structures to consolidate peace and prevent the outbreak of new conflicts.

Tasks for a company may be:

- Collecting and destroying weapons;
- Safeguarding and supporting the return of refugees to their homeland;
- Restoring and establishing the public order;
- Training of the local security forces, development of democratic structures, and;
- Assisting to repair damages caused by the conflict.

2.5.3.2.4 Humanitarian operations

The purpose of humanitarian operations is:

- To deliver aid supplies to save lives;
- To secure the survival of affected people;
- To support self-initiatives and to restore the essential infrastructure.

Required for these operations are mainly logistic, medical and engineer forces. However, the company can be required to safeguard and secure these operations.

2.6 NOV-6 Operational Activity Sequence & Timing Description

Figure 2-21, Figure 2-22 and Figure 3-23 show typical mission profiles with respect to the sequence and timing of the operational activities of a High Intensity 24 Hour Mechanised Infantry STU Operation, a 36 Hour Regular Infantry STU Cordon and Search Operation (Counter Insurgency/Counter Terrorism Environment), and a 72 Hour Special Forces Evacuation Operation, respectively. From these sequence and timings, the usage profiles for the DSS and its sub-systems can be derived.

The different activities are separated into columns with the combat intensity indicated using colours, starting with green (low intensity – 30 % usage), yellow (middle intensity – 50% usage) to red (high intensity 100% usage).

The horizontal timeline labelled with expired time, in hours, shows the duration of the mission activities.

The status of mounted/dismounted soldiers and DSS-equipment, such as radios and optics/optronic is depicted and can be used for estimating:

- The time duration of electrical energy being available from platforms for powering a DSS;
- The time duration of electrical energy being available from platforms for charging/refuelling its power sources;
- The time duration of charged power sources (e.g. batteries, fuel tanks) being available to be exchanged;
- The time duration and number of soldiers with special tasks;
- The time duration the DSS is either fully or partly used.

	High-Intensitiy Attack, Mechanized Infantry, 24 hrs																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Activity	technical service/ safeguarding						advance/ approach				incursion/ combat						safeguarding captured area/ logistics							
Vehicle																								
Weapon	only for special cases						in standby				in operation (stabilized)						in standby for safeguarding							
Optics/Optronics	in operation for safeguarding						in operation				in operation						in operation for safeguarding							
Voice Radio	standby						standby				in operation						standby							
BMS	in operation						in operation				in operation						in operation							
Vehicle	move for supply and safeguarding						cruising speed (10-30km/h in light terrain)				maximum speed (10-30km/h in rough terrain)						move for supply and safeguarding (e.g. 15km radius)							
Engine	for electrical power supply						mainly for driving				only for driving						for electrical power supply							
DSS																								
Mount Status	partly mounted (30% dismounted for safeguarding)						all mounted				alternating between mounted / dismounted						partly mounted (60% dismounted for safeguarding)							
Connected to Vehicle	partly						yes				no						partly							
Soldier Equipment	soldiers are partly equipped						all soldiers are fully equipped				all soldiers are fully equipped						soldiers are partly equipped							
Soldier C4I	in operation (for 30%)						in operation				in operation						in operation (for 60%)							
Radio	in operation (for 30%)						no radio				radio only when dismounted						in operation (for 60%)							
Squad Leader C4I	in operation						in operation				in operation						in operation							

Figure 2-21 – High Intensity Attack, Mechanized Infantry, 24 hrs

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

	Military Evacuation Operation, Special Forces, 72 hrs																																	
	1	2	3	4	5	6	7	8	…	23	24	1	2	3	4	5	6	7	…	20	21	22	23	24	1	2	3	4	…	19	20	21	22	23	24
	🟩	🟩	🟩	🟩	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟨	🟥	🟥	🟥	🟥	🟥	🟨	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩
Activity	Transport				Assemble		Combat					Safeguarding/ Resting				Pre-pa-re	Combat					Log-is-tics	Safeguarding/ Resting				Combat					Resting/ Logistics/ Safeguarding			
Soldier Equipment (incl Backpack)	fully carried				fully carried		fully/partly carried					fully carried (for 30%)				fully (no backpack)						fully carried (for 30%)					fully carried					fully carried (for 30%)			
Soldier C4I	in operation (low usage)				in operation (high usage)		in operation (medium usage)					in operation (low usage, for 50%)				in operation (medium usage)						in operation (low usage for 50%)					in operation (medium usage)					in operation (low usage, for 50%)			
Voice Radio	5% of the time				10% of the time		10% of the time					10% of the time (for 30%)				10% of the time						10% of the time (for 30%)					10% of the time					10% of the time (for 30%)			
Optics/Optronics	50% in operation				50% in operation		100% in operation					50% in operation (for 30%)				50% in operation						50% in operation (for 30%)					50% in operation					50% in operation (for 30%)			
Weapon	only for special cases				only for special cases		in operation					in standby (for 30%)				in operation						in standby (for 30%)					in operation					standby (for 30%)			
external power supply / spare batteries	no				no		no					recharge/ replacement				no						recharge/ replacement					no					recharge/ replacement			
Squad Leader C4I	in operation				in operation		in operation					in operation				in operation						in operation					in operation					in operation			

Figure 2-22 – Military Evacuation Operation, Special Forces, 72 hrs

	Cordon and Search Operation, Regular Infantry, 36 Hours							
	1 2 3 4 5 6	7 8 9 10	11 12 13 14	15 16 17 18 19 22 23 24	25 26 26 27	28 29	30 31	32…36
	🟩🟩🟩🟩🟩🟩	🟨🟨🟨🟨	🟥🟥🟥🟥	🟥🟥🟥🟥🟥🟥🟥🟥	🟨🟨🟨🟨	🟥🟥	🟨🟨	🟩
Activity	Receive Intelligence, Plan, Assemble, Briefing	Reconnaissance and Surveillance of Target Area	Move and Deploy Cordon (Outer/Inner Perimeter & Stops)	**Search Operations and Combat**	**Combing Operations** (Possible Encounters)	**Sanitising Area** (Likely Encounters)	**Link Up & Reporting**	**De-induction**
Soldier Equipment (incl. back pack)	Not Carried	Partly Carried	Fully Carried	Fully Carried	Fully Carried	Fully Carried	Fully Carried	Partly Carried
Soldier C4I	In Operation (Low Usage)	In Operation (Low Usage)	In Operation (Medium Usage)	In Operation (High Usage)	In Operation (Medium Usage)	In Operation (High Usage)	In Operation (Medium Usage)	In Op. (Low Usage 60%)
Voice/ Radio	In Operation (but maintaining radio silence)	In Operation (but maintaining radio silence)	In Operation (but maintaining radio silence)	In Operation (High Usage)	In Operation (Medium Usage)	In Operation (High Usage)	In Operation (High Usage)	In Operation (Low Usage)
Optics/ Optronics	Not in operation	In Operation (High Usage)	In Operation (High Usage)	In Operation (High Usage)	In Operation (High Usage)	In Operation (High Usage)		In Operation (Low Usage)
Weapon	Not in operation	Usage only in Emergency Encounters	Usage only in Emergency Encounter	In Operation (High Usage)		In Operation (High Usage)		Usage Only in Emergencies
External PS /Spare Batteries	Recharge / Replacement	No	No	No	No	No	No	Recharge / Replacement
LEGEND:	🟩 Low Intensity	🟨 Middle Intensity	🟥 High Intensity					

Figure 2-23 – Regular Infantry Cordon & Search Operations 36 Hours

2.7 Non-Functional Requirements

A DSS needs to work in differing environmental conditions. For the harmonization of non-functional requirements, the taxonomy in Figure 2-24 presents six different top-level categories of requirements for a generic DSS. Each category class includes a collection of requirements which is described in detail in the following sections.

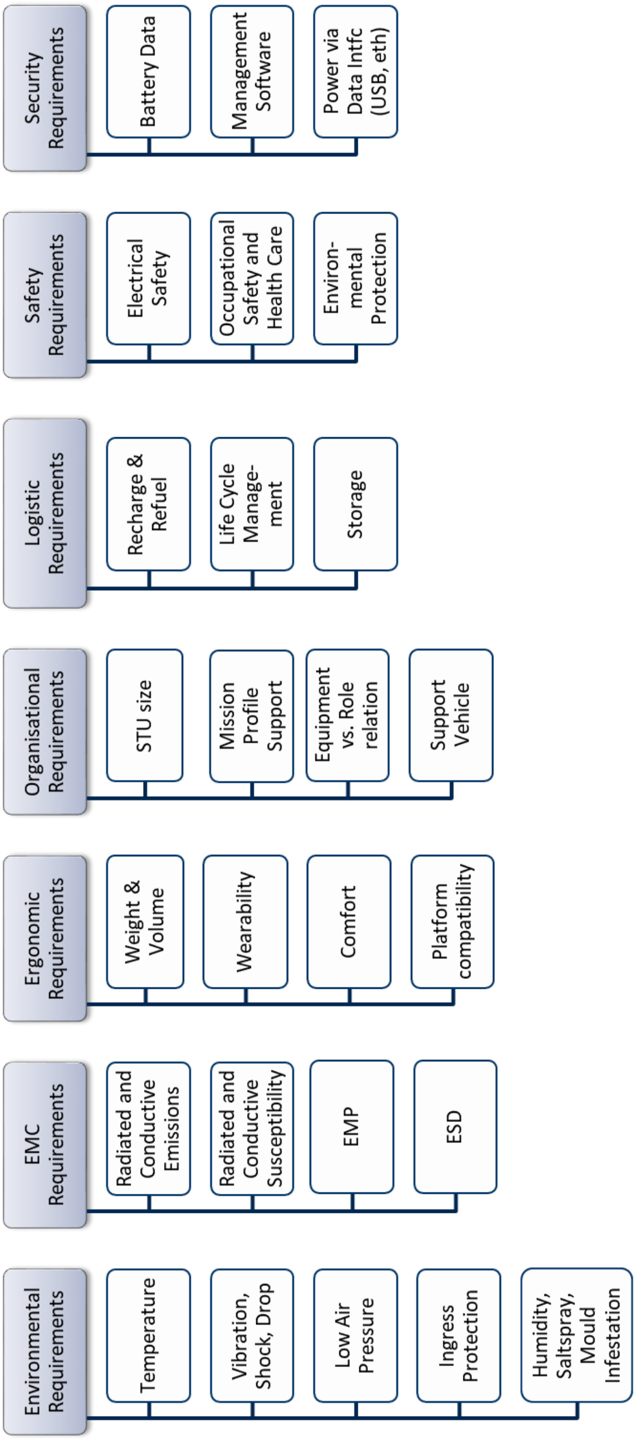

Figure 2-24 – Non-functional requirements taxonomy

2.7.1 Environmental Requirements

Overstated requirement might result in oversized weight and volume, reduced performance or significantly increased cost, therefore requirements need to be carefully defined. Nations and NATO provide guidelines for environmental requirements and testing.

2.7.1.1 Temperature

Soldier System needs to be designed to operate in certain defined temperature ranges. For storage, temperature limits may be different. In order to define the temperature range requirements, temperatures to which the Soldier Systems will be exposed, which are dependent on the geographic area and the tactical scenario, need to be considered.

Electrical and electronic equipment, cables and plugs are affected by extreme temperatures which can cause degradation of performance, break down or mechanical damage.

2.7.1.2 Vibration, Shock, Drop

The system or sub-system must withstand vibration e.g. induced by the vehicles. It also has to consider that person-carried equipment is indirectly subjected to externally induced vibrations. In every case, the damping effect of the body has also to be considered.

The system or sub-system has to withstand shocks according to Crash Hazard Shock Test for Ground Equipment in operational mode.

2.7.1.3 Low Air Pressure

The system or sub-system must withstand low pressure without damage, e.g. for air transport and rapid decompression without impairment.

The system also needs to function at higher altitudes which are accessible for infantrymen. If required, due to technical limitations, the performance can be degraded if a threshold altitude (e.g. 2000 m above sea level) is exceeded as long as reliable operation remains secured.

2.7.1.4 Ingress Protection

The system or sub-system has to withstand sand and dust environment as well as water immersion without impairment.

2.7.1.5 Humidity, Salt Spray, Mould Infestation

The system or sub-system has to withstand the salt fog environment without impairment.

2.7.2 EMC Requirements

Electromagnetic compatibility besides the general regulations is key radio communication performance. Radios are limited in power because of soldier's health such that range is achieved by high sensitivity of the receiver. EMC can severely disturb such a receiver and drastically reduce the radio's communication range.

EMC is also important in man-pack applications, where devices are positioned near each other. In practice, this means that the electromagnetic disturbances from each item of equipment must be limited and that each item must have an adequate level of immunity to the disturbances in its environment.

Any EM emission, natural or 'man-made', is potentially a disturbance to any other susceptible device in the environment. It may either put it out of action or, in many causes it to malfunction. So there are two sides to the EMC equation:

- Source equipment whose controllable emissions must be limited;
- Equipment that needs to have adequate immunity to those disturbances in its environment to which it is exposed.

EM disturbances may work in more than one direction, disrupting more than one device, or multiple sources may have a cumulative effect on a single piece of equipment. On the emissions side of the equation, therefore, the aim of EMC is to ensure that equipment does not disturb other equipment, radio services, power, electronics or networks. On the immunity side, the aim is to ensure that equipment is not affected by, e.g., radio transmissions, mains-borne disturbances, electrostatic fields and other phenomena.

2.7.2.1 Radiated and Conductive Emission

Radiated and Conductive Emission is the phenomenon by which electromagnetic energy emanates from a source.

Data transmission inside a device or from one device to the other, is mostly implemented digitally, which causes severe switching noise caused by the abrupt zero to one voltage transition especially at high speed. The used technology shall natively generate low electrical noise transmission speeds may need to be reduced and adequate shielding is necessary.

For power conditioning in devices, power converters are often used. They naturally emit transients and/or harmonic waves with high energy. Step down DC-DC converters usually have lower noise levels than step up DC-DC converters. Power source should therefore have rather higher voltages than needed. Therefore, power sources with a native low electrical noise profile (e.g. batteries) are preferable rather than technologies that need dedicated electronic devices for conversion.

Unmated connections shall be protected to avoid electromagnetic emissions and interferences (EMI) and to avoid disturbing other equipment or being detected by hostile forces.

2.7.2.2 Radiated and Conductive Susceptibility

Electromagnetic susceptibility is the inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance.

An EM-shielded system is state of the art but its interfaces, usually connectors, are often a weak point when unmated. Unmated connections shall be protected to avoid the "antenna effect" and receiving emissions from other equipment.

In a military environment high power radio transmitter are usual, e.g. at a STU vehicle or transporter. They might interfere with the DSS-equipment and limit or impede a system function, and are to be considered in an EMC-analysis.

2.7.2.3 Electrostatic Discharge (ESD)

Electrostatic discharge is the transfer of electric charge between bodies of different electric potential in proximity or through direct contact.

ESD can create spectacular electric sparks. Lightning, with the accompanying sound of thunder, is a large-scale ESD event. Nevertheless even less dramatic forms which may be neither seen nor heard, can still cause damage to sensitive electronic devices. Grounding is especially important for effective ESD control.

A DSS in ES-environment (e.g. lightning) cannot be efficiently protected. In an operation, the soldier needs to cover himself, e.g. by mounting the vehicle.

2.7.2.4 Electromagnetic Pulses (EMP)

There are different types of EMP: natural, man-made and military. They all have a short-duration pulse of energy in common. The energy is usually broadband by nature, although it often excites a relatively narrow-band damped sine wave response in the affected device. Some types are generated as repetitive and regular pulse signals.

EMP with high energy does not have an effect to the equipment only. It also impairs the person who is carrying it. The high effort to fail-safe the equipment needs to consider an EMP level which does not disable the soldier.

2.7.2.5 EMC Control Plan

The EMC Control Plan describes measures to be taken as a result of an EMC-analysis.

An EMC-analysis matches the functional and non-functional requirements of a DSS with its surrounding elements, existing systems and environment with respect to electromagnetic compatibility.

The EMC Control Plan includes organizational and technical methods and measures to ensure the electromagnetic compatibility and electrical safety of the DSS within its surrounding elements and environment. With respect to EMC also the cooperation between customer, supplier and sub-supplier shall be described here. Usually on each side of contract partners are people in charge to supervise, coordinate and monitor measures related to EMC.

2.7.3 Ergonomic Requirements

2.7.3.1 Weight & Volume

Dismounted Soldiers usually need to carry everything they take with them. There are research efforts on “E-Donkeys” which could carry some equipment but they are still in a research stage and do not yet have the necessary TRL. The weight of a DSS must be such that it can be carried by the soldier together with the necessary supply of ammunition, water, etc.

The volume needs to be such that it still fits onto a soldier with all the supply listed before.

2.7.3.2 Wearability (Ergonomics/Unhindered Mobility)

The DSS must not prevent dismounted mobility. Each body joint have to remain free to move.

The shape of the electrical and electronics should, where possible, be designed such that it does not exceed the dimension of the body’s part chosen to carry it on.

2.7.3.3 Comfort

Avoid hot spot points. A compact (high density) solution allows better perspiring than solution requiring a large surface. However, heat produced from devices need to be transferred to the environment which may require larger surfaces.

2.7.3.4 Platform compatibility

Do not prevent mounted operations (e.g. seated, fasted belt, egress and ingress).

2.7.4 Organizational Requirements

2.7.4.1 STU Size

STU radio communication capacity shall be large enough to cope with the load generated by the number of soldiers in a STU. Position reporting frequency shall be set accordingly.

Enough shared equipment needs to be provided such that enough soldiers will be able to use it.

The recharge/refuel and consumable supply capability available during the mission shall fit the STU‘s number of soldiers.

2.7.4.2 Mission Profile Support

Data Management and Infrastructure needs to support the possible mission profiles. It should need to be configurable the specific mission profile by configuring the software or by adding or leaving behind devices.

The recharge/refuel and consumable supply capability shall fit the mission profile (e.g. batteries number, fuel quantity).

2.7.4.3 Equipment vs. Roles Relation

The Data Management and Infrastructure equipment needs to enable and support the soldier’s role or a potential role which he might take over, e.g. for the Second in Command, which will have similar equipment as the STU Leader.

Considering weight, size and power, the soldier shall not be provided with equipment which he does not need in his role.

The recharge/refuel and consumable supply capability shall consider the role-depending equipment of the Soldier System.

2.7.4.4 Support Vehicle

The Soldier System should be connectable to the support vehicle in order to exchange data or to receive power.

At least two modes shall be supported: mounted and dismounted. A nearfield mode, specific to “dismounted”, may also be considered, if e.g. the operation requires a tight interaction between the STU and the vehicle or a high Data Throughput Capacity for the radio is needed.

If mounted, the Soldier System should:

- Be able to communicate to the vehicle crew via voice;
- Be provided with the current own position;
- Keep C4I data current;
- Exchange data which, due to its size, may not have been transmitted via the tactical radio (map data, etc.);
- Be provided with power to save or recharge / refuel its power supply.

The mounted soldier may even take over crew tasks of the support vehicle, either by using his own equipment or by using devices of the vehicle.

If dismounted, the Soldier System should:

- Be able to communicate to a vehicle crew member via voice;
- Exchange C4I data in a timely manner.

Tight operation with the support vehicle may be necessary, e.g. the dismounted soldier may benefit from the higher performance devices (sensors, weapons, radios) of the vehicle or the vehicle benefits from the better flexibility in movement of the soldiers or their better nearfield situation awareness.

The recharge/refuel feature may be applied to the entire Soldier System or each single power source of the Soldier System or both.

The Soldier System shall be able to interoperate, specifically with support vehicles using STANAG 4754 NGVA.

The support vehicles shall also be able to supply all necessary consumables.

2.7.5 Logistic Requirements

2.7.5.1 Recharge & Refuel

For recharging, the number of battery types shall be as low as possible, ideally just one, in order to avoid the management of a large number of different voltages and technologies.

For refuelling, the power source technology should consider the fuel type as already included in the logistic supply chain.

2.7.5.2 Life Cycle Management

An important part of the Life Cycle Management is the obsolescence and innovation management process. During the operational life of the DSS, it's expected that there will be significant changes to the operational profile of the user as well as availability of new technologies on the market. In addition to standard obsolescence issues of information systems, these changes need to be managed during the life of a DSS.

It is recommended that there shall be established a joint team of key stakeholders taking necessary decisions on how the DSS shall be managed with obsolescence and innovation.

Preferable DSS technologies:

- Have a long life;
- Do require minimum maintenance;
- Do use as little consumables as possible;
- Support easy updating;
- Can easily be upgraded with new devices;
- Can be disposed easily with little impact on the environment.

2.7.5.3 Maintainability

The DSS shall be maintained by both dedicated maintenance staff as well as the user. Maintenance are divided into corrective and preventive maintenance. The existing maintenance organisation shall preferably be used, and the number of specific maintenance equipment and procedures shall be minimized.

Fault location and identification shall be supported by built-in functions in the DSS as described in the System and Technical views. The purpose of these functions is to support the concept of integrated and user-friendly maintenance of the DSS.

2.7.5.4 Reliability

The DSS shall be capable of operation without loss of core functions throughout its expected service life, across the full spectrum of environments and operating conditions.

Core functions are defined in the performance requirements. Some minor temporary degradation of performance, clarity of message, or response time is acceptable, as long as the image, symbol or message is legible, understandable and timely enough as to not affect the overall function.

Failure is defined as an event, or inoperable state, in which an item is unable to perform within specified performance requirements or intended function. Typically, it is any event that requires corrective maintenance to restore the system to its normal performance standard, which excludes preventive maintenance, but includes any corrective maintenance activities found necessary during preventive maintenance.

2.7.5.5 Storage

Preferable technologies should not have specific requirements of storage.

2.7.6 Safety Requirements

Products placed on the market in the EU are subject to general safety requirements. These requirements are included in /12/ which aims at ensuring that only safe consumer products are sold inside the EU.

Although military products might be excluded in national safety laws, e.g. as stated in the Equipment and Product Safety Act in Germany, the army as an employer has the obligation to arrange all measures and to provide safe work equipment to ensure occupational safety and health.

Thus, products which are explicitly determined for military use shall be subject to safety requirements as mentioned above. Risk assessment has to be performed and exemptions should be limited to exceptional, clearly defined and individually justified cases.

General Product Safety Directive (GPSD) of the European Commission, Product Safety Legislation:

A product is deemed safe once it conforms to the safety provisions provided in European legislation or national legislation of Member States adopted in accordance with EU law. In the absence of such regulations or EU standards, the references of which were published in the Official Journal of the EU, the product's compliance is determined according to other reference documents such as national standards, Commission recommendations and codes of practices.

In addition to the basic requirement to place only safe products on the market, manufacturers must inform consumers of the risks associated with the products they supply. They must take appropriate measures to prevent such risks and be able to trace dangerous products.

2.7.6.1 Electrical Safety

Particularly the DSS Power System has to be designed and assessed with regard to electrical safety. The system shall work on safe extra-low voltage and shall not be connected to systems with higher voltage without protective measures.

2.7.6.2 Occupational Safety and Health Care

In practice, experience has shown that devices and their cabling shall be easily removed without much strain (e.g. helmet equipment), in order to avoid the risk of injury, e.g. due to getting caught or to be pulled in.

2.7.6.3 Environmental Protection

Environmental protection is a practice of protecting the natural environment from individuals, organizations or governments for the benefit of both the natural environment and humans.

The DSS shall contain as little hazardous material as possible, but definitely no material which is against regulatory compliances. Additionally, in times of ever decreasing resources, it becomes even more important to reuse recyclable and/or potentially recyclable material.

Environmental standards do exist at the international and national level. They require an assessment of the environmental impact of a system and its components for their production, use and discard (life cycle). Hazardous and polluting substances have to be identified and either not used or their disposal has to be managed.

These requirements of maintaining environmental protection standards are given in the following NATO Standards Agreements (STANAGS): STANAG 7141 Joint NATO Doctrine for Environmental Protection During NATO-led Military Activities (AJEPP-4); STANAG 2510 Joint NATO Waste Management Requirements During NATO-led Military Activities (AJEPP-5); and; STANAG 2583 Environmental Management System in NATO Operations (AJEPP-3).

2.7.7 Security Requirements

The measures to accomplish confidentiality, integrity and reliability of information exchanged, processed and stored in a DSS depends on its protection needs, which is mainly dependent on the official confidentiality level of the information.

Sensitive information shared amongst NATO allies has four levels of security classification, which are given below in descending order of importance:

1) COSMIC TOP SECRET (CTS);
2) NATO SECRET (NS);
3) NATO CONFIDENTIAL (NC);
4) NATO RESTRICTED (NR);
5) NATO UNRESTRICTED (NU).

A special case exists with regard to NATO UNCLASSIFIED (NU) information. Information with this marking is NATO property (copyright) and must not be made public (outside NATO) without NATO's explicit permission.

2.7.7.1 Protection Requirements Analysis

In general, the following procedure is proven to derive suitable measures for protection:

- Threat Analysis based on the System Architecture;
- Development of Security Architecture and Definition of Counter Measures;
- Analysis of confidentiality and integrity;
- Analysis of crypto requirements;
- Analysis of risks, also to consider remaining risks after mandated measures are taken.

Examples of measures with subject to critical aspects are described in the sub-sections below.

2.7.7.1.1 Voice Communication

Depending on the result of the protection requirements analysis, wireless and/or wired voice transmission shall be encrypted. There may be national and/or NATO-wide requirement to consider what measures, technologies and algorithms are to be used.

2.7.7.1.2 Data

Depending on the result of the protection requirements analysis wireless and/or wired data transmission shall be encrypted. There may be national and/or NATO-wide requirements to consider which measures, technologies and algorithms are to be used.

2.7.7.1.3 Software

C4I and management software of a DSS may be subjected to security requirements. Complex management software, including battery management software, may have a huge impact to system reliability, so it shall be secured to avoid unauthorized manipulation.

Depending on the result of the protection requirements analysis software and the granted access, it may be allowed to authorize personnel only. Operating systems, application software and cached data may be stored encrypted on the systems' storage. There may be national and/or NATO-wide requirements to consider which measures, technologies and algorithms are to be used.

Software interfaces to external systems may be also exposed to threats and thus strictly reduced to necessary ports. Firewalls may control allowed traffic and unused IP-ports are to be disabled.

2.7.7.1.4 Hardware

Hardware interfaces, especially the interfaces which comply with industrial standards such as USB, Ethernet, etc. may be subject to threats and their number shall be minimal. Unused hardware interfaces shall be disabled. Traffic shall be limited to allowed data types and can be access controlled.

Especially gateways to external systems shall be protected and allowed data may be virus-checked before stored in the DSS.

3 Integrated Dictionary

3.1 Abbreviations and Acronyms

AC	Alternating Current
AF	Air Force
ACT	Allied Command Transformation
AI	Artificial Intelligence
BIU	Basic Infantry Unit
BMS	Battery Management System
CG	Capability Group
CRB	Central Rechargeable Battery
CBRN	Chemical, Biological, Radiological, and Nuclear
CIMIC	Civil Military Cooperation
CAS	Close Air Support
CSS	Combat Service Support
CAT	Combined Arms Teams
COP	Common Operational Picture
CROP	Common Reference Operational Picture
CTS	Cosmic Top Secret
COA	Course Of Action
DPKO	Department of Peacekeeping Operations
DNV GL	Det Norske Veritas Germanischer Lloyd (NLD)
DEU	Deutschland (Germany)
DC	Direct Current
DEW	Directed Energy Weapon
DSS	Dismounted Soldier System
DCI	Distribution, Control and Information (Power Distribution Network)
ET	Ejercito de Tierra
EM	Electro Magnetic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
ECM	Electronic Counter Measures
EW	Electronic Warfare
ESD	Electrostatic Discharge
EC	European Comission
EDA	European Defence Agency
EU	European Union
FMN	Federated Mission Networking
FSCL	Fire Support Coordinating Line
FHA	Foreign Humanitarian Assistance
FID	Foreign Internal Defence
FAC	Forward Air Controller
FLET	Forward Line of Enemy Troops

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

FLOT	Forward Line of Own Troops
FO	Forward Observer
FDD	Future Development Document
FST	Future Soldier Technology
GPSD	General Product Safety Directive
GOSSRA	Generic Open Soldier System Reference Architecture
GIS	Geographic Information System
GPS	Global Positioning System
GUI	Graphic User Interface
HMD	Head Mounted Display
HQ	Headquarters
HPM	High Power Microwave
ID	Identification
ICV	Infantry Carrier Vehicle
IO	Information Operations
IT	Information Technology
IR	Infrared
ISR	Intelligence Surveillance and Reconaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconaissance
IP	Internet Protocol
ITA	Italy
JFST	Joint Fire Support Team
JFC	Joint Forces Command
LCG-DSS	Land Capability Group – Dismounted Soldier Systems
LI	Light Infantry
LRU	Line replaceable unit
LPD	Low Power Devices
MMG	Medium Machine Gun
MIL	Militar
MDMP	Military Decision-Making Process
MOUT	Military Operation in Urban Terrain
MDE	Ministerio de Defensa de España
MNF	Multi National Force
MUMSIS	Multi-Modal Soldier Interface System
NAV	NATO All View
NCV	NATO Capability View
NC	NATO Confidential
NGVA	NATO Generic Vehicle Architecture (STANAG 4754)
NOV	NATO Operational View
NR	NATO Restricted
NS	NATO Secret
NSOV	NATO Service Oriented View
NSV	NATO System View
NTV	NATO Technical View
NU	NATO Unrestricted
NLD	Netherlands
NCO	Network Centric Operations

NEC	Network Enabled Capability
NCW	Network-Centric Warfare
NEO	Non-combatant Evacuation Operation
NATO	North Atlantic Treaty Organization
NBC	Nuclear Biological Chemical
OODA	Observe, Orient, Decide and Act
OCHA	Office for the Coordination of Humanitarian Affairs
OOTW	Operations Other Than War
ORBAT	Order of Battle
PO	Peace Operations
PR	Personnel Recovery
POL	Poland
PRT	Portugal
PADR	Preparatory Action on Defence Research
PU	Public
PRS	Public Regulated Service
PTT	Push-to-talk
RF	Radio frequency
RBCI	Radio-Based Combat Identification
SAR	Search and Rescue
STU	Small Tactical Unit
SDR	Software Defined Radio
ESP	Spain
SOF	Special Operations Forces
STANAG	Standardisation Agreement (NATO)
STASS	Standardized Architecture for Soldier System
SWE	Sweden
TRL	Technology Readiness Levels
UGS	Unattended Ground Sensors
UN	United Nations
US	United States
USA	United States of America
USB	Universal Serial Bus
UAGS	Unmaned Air / Ground Systems
UAS	Unmaned Aircraft Systems
UAV	Unmanned Aerial Vehicle
WAN	Wide Area Network
WWI	World War 1

3.1 Referenced Documents

3.1.1 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, 31-03-2020

/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, 31-03-2020

/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, 31-03-2020

/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, 31-03-2020

/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, 31-03-2020

/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, 31-03-2020

/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, 31-03-2020

/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

3.1.2 Document related references

/9/ AAP-6 (version 2015); NATO Glossary of Terms and Definitions

/10/ W. Ross Ashby "An Introduction to Cybernetics", Chapman & Hall, 1956.

/11/ ALBERTS D S, GARSTKA.J.J and STEIN F, "Network Centric Warfare; Developing and Leveraging Information Superiority". 1999, CCRP, DoD. Washington, DC, USA.

/12/ General Product Safety Directive 2001/95/EC (GPSD)

/13/ LCGDSS Overarching Definition, NATO AC/225(DSS)D(2017)0003