



Security And Interoperability in Next Generation PPDR  
Communication Infrastructures



Project Number: 313296

---

## Deliverable 3.1

### System requirements, Enterprise Architecture and methodology

---

|                              |                              |
|------------------------------|------------------------------|
| Scope                        | Scheduled deliverable        |
| Lead Beneficiary             | Alcatel-Lucent International |
| Dissemination level          | Public                       |
| Document creation date       | 08/Jan/2014                  |
| Document release date        | 12/Mar/2014                  |
| Contractual Date of Delivery | 28/Feb/2014                  |
| Version                      | 1.2                          |
| Status                       | Released                     |

**Abstract:** Deliverable 3.1 includes an analysis on the PPDR organisation strategy and information flows, provides system level requirements from the PPDR end users' requirements and specifies preliminary Enterprise Architecture methodology.

[illegible]

| Name                   | Organisation | Email                                                                        |
|------------------------|--------------|------------------------------------------------------------------------------|
| Hervé Mokrani          | CAS          | <a href="mailto:herve.mokrani@cassidian.com">herve.mokrani@cassidian.com</a> |
| Konstantia Barbatsalou | ONE          | <a href="mailto:konstantia@dei.uc.pt">konstantia@dei.uc.pt</a>               |
| Panagiotis Galiotos    | UPAT         | <a href="mailto:pgaliot@gmail.com">pgaliot@gmail.com</a>                     |

## EXECUTIVE SUMMARY

By leveraging emerging broadband wireless technologies (such as Long Term Evolution, LTE) in addition to existing legacy Private Mobile Radio (PMR) systems (TETRA/TETRAPOL), the future communication system for Public Protection and Disaster Relief (PPDR) proposed by the SALUS project will enhance present mode of operations by offering new services and capabilities to PPDR organisations. This will improve operational effectiveness of the PPDR users in their different missions (day-to-day, planned and unplanned events) while enhancing safety for everyone. However, the definition and design of an efficient next generation communication system for PPDR is a complex task. Many different aspects such as strategic aspects, organisational aspects, regulatory aspects, technical aspects and economical aspects have to be taken into accounts. The SALUS project has decided to follow the Enterprise Architecture methodology [9] to ease this task,

The scope of deliverable D3.1 “System requirements, Enterprise Architecture and methodology” is to provide the first elements that will help defining, specifying and designing the SALUS system. Its main objectives are:

- To consolidate the high level system requirements and the information flows of the SALUS system; these will be the basic initial elements driving the design of the SALUS solution,
- To propose a methodology (based on the Enterprise Architecture concept) that will be used in the subsequent deliverables of WP3 for supporting the actual definition and specification of the SALUS enterprise and system architecture.

The first objective is realized by analysing the three scenarios (City Security, Temporary Protection and Disaster Recovery) and their underlying use cases developed within SALUS WP2 activities. Key inputs for this deliverable are the storyboards for each use case. These storyboards are analysed so as to identify the following items in a systematic way:

- The operational and end-user needs during the flow of events,
- The actors engaged in the use case,
- The required applications and information flows during the mission.

From this systematic analysis, high level system requirements expressed in “needed capabilities” and information flows are derived for each use case. In the Enterprise Architecture nomenclature, a “capability” has to be interpreted as *“an ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology to achieve.”* [7] or *“a high level specification of the enterprise’s ability”* [14].

It is to be noted that this document focuses on capabilities and information flows that will enable to efficiently support advanced and secured applications over multiple PPDR networks including legacy systems (TETRA and TETRAPOL) and future systems (LTE private, LTE commercial, Wi-Fi private...). This document illustrates that there are some common capabilities and information flows among the three use cases but also that some of them are unique for each use case. It has been deliberately decided to have a systematic presentation of the needed capabilities and information flows for each use case. Although this creates some repetition within the document, an accurate and complete presentation of the capabilities and information flows will be useful for the next steps of the definition of the SALUS enterprise and architecture solution.

Since the task of specifying such a system and its characteristics is complex, the SALUS project will use the Enterprise Architecture concept to ensure that the solution specified and developed within the SALUS context will be consistent with all the aspects mentioned above. Initially, while

aiming at familiarizing the reader with the Enterprise Architecture methodology, a short overview of the Enterprise Architecture concepts and major existing Enterprise Architecture frameworks is provided. Then, the document describes the proposed the Enterprise Architecture framework that will be used by SALUS for the upcoming architecture and specifications tasks. This proposed framework is based on Open Safety and Security Architecture Framework (OSSAF) [8] (that has been designed for Public Safety and Security agencies), complemented with the NATO Architecture Framework (NAF) meta-model and views [14] to represent the different OSSAF views included in the different OSSAF perspectives.

The derived needed capabilities and information flows will serve as inputs to the next tasks and deliverables (D3.2 and D3.3) that will further elaborate on functional building blocks, interfaces between the building blocks and operational procedures and workflows using the proposed OSSAF Enterprise Architecture Framework.

## TABLE OF CONTENTS

|                                                                   |    |
|-------------------------------------------------------------------|----|
| EXECUTIVE SUMMARY .....                                           | 3  |
| TABLE OF CONTENTS .....                                           | 5  |
| TABLE OF FIGURES .....                                            | 7  |
| TABLE OF TABLES .....                                             | 7  |
| 1 INTRODUCTION.....                                               | 8  |
| 2 CITY SECURITY – SYSTEM REQUIREMENTS .....                       | 9  |
| 2.1 Inputs .....                                                  | 9  |
| 2.1.1 Key applications .....                                      | 11 |
| 2.1.2 Main actors .....                                           | 11 |
| 2.2 Needed Capabilities for City Security Use case.....           | 12 |
| 2.3 Information flows for City Security Use case .....            | 14 |
| 3 TEMPORARY PROTECTION – SYSTEM REQUIREMENTS.....                 | 19 |
| 3.1 Inputs .....                                                  | 19 |
| 3.1.1 Key applications .....                                      | 20 |
| 3.1.2 Main actors .....                                           | 21 |
| 3.2 Needed Capabilities for Temporary Protection Use case .....   | 21 |
| 3.3 Information flows for Temporary Protection Use case .....     | 23 |
| 4 DISASTER RECOVERY – SYSTEM REQUIREMENTS.....                    | 26 |
| 4.1 Inputs .....                                                  | 26 |
| 4.1.1 Key applications .....                                      | 27 |
| 4.1.2 Main actors .....                                           | 27 |
| 4.2 Needed Capabilities for Disaster Recovery Use case.....       | 27 |
| 4.3 Information flows for Disaster Recovery Use case .....        | 28 |
| 5 ADDITIONAL SYSTEM REQUIREMENTS ON SECURITY.....                 | 30 |
| 6 ENTERPRISE ARCHITECTURE METHODOLOGY .....                       | 31 |
| 6.1 Introduction .....                                            | 31 |
| 6.1.1 Core concepts and definitions .....                         | 31 |
| 6.1.2 Problem addressed by an EA.....                             | 32 |
| 6.1.3 Overview on EA frameworks .....                             | 33 |
| 6.1.4 Open Safety & Security Architecture Framework (OSSAF) ..... | 34 |
| 6.2 Methodology .....                                             | 35 |
| 6.2.1 EA derivation process .....                                 | 35 |
| 6.2.2 Definition of the Modelling Vocabulary .....                | 36 |
| 6.2.3 Proposed Model for SALUS .....                              | 41 |
| 7 Considerations and future steps.....                            | 66 |
| 8 ANNEX 1 – CITY SECURITY STORYBOARD .....                        | 67 |
| 8.1 Abstract.....                                                 | 67 |

|        |                                                |    |
|--------|------------------------------------------------|----|
| 8.2    | Use case description.....                      | 67 |
| 8.3    | Expected users (use case actors) .....         | 68 |
| 8.4    | Story board .....                              | 68 |
| 8.4.1  | Precondition .....                             | 68 |
| 8.4.2  | Flow of events .....                           | 68 |
| 9      | ANNEX 2 – TEMPORARY PROTECTION STORYBOARD..... | 72 |
| 9.1    | Abstract.....                                  | 72 |
| 9.2    | Use case description.....                      | 72 |
| 9.3    | Expected users (use case actors) .....         | 73 |
| 9.4    | Story board .....                              | 73 |
| 9.4.1  | Precondition .....                             | 73 |
| 9.4.2  | Flow of events .....                           | 73 |
| 10     | ANNEX 3 – DISASTER RECOVERY STORYBOARD .....   | 76 |
| 10.1   | Abstract.....                                  | 76 |
| 10.2   | Use case description.....                      | 76 |
| 10.3   | Expected users (use case actors) .....         | 76 |
| 10.4   | Story board .....                              | 77 |
| 10.4.1 | Precondition .....                             | 77 |
| 10.4.2 | Flow of events .....                           | 77 |
|        | BIBLIOGRAPHY.....                              | 79 |
|        | ACRONYMS .....                                 | 80 |

## TABLE OF FIGURES

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| Figure 1: Typical structuring of an EA into different levels (modified after [11]) ..... | 32 |
| Figure 2: Context, evolution and influences to NAF .....                                 | 34 |
| Figure 3: Inputs to OSSAF .....                                                          | 35 |
| Figure 4: Model elements according to the strategic and operational scope .....          | 43 |
| Figure 5: Model elements according to the operational, systems and technical scope ..... | 44 |
| Figure 6: Model elements according to the service oriented scope.....                    | 45 |

## TABLE OF TABLES

|                                                                                       |    |
|---------------------------------------------------------------------------------------|----|
| Table 1 – City Security use case – Operational and end-user requirements.....         | 9  |
| Table 2 – Needed capabilities for City Security use case .....                        | 12 |
| Table 3 – City Security – information flows.....                                      | 14 |
| Table 4 – Temporary Protection use case - Operational and end-user requirements ..... | 19 |
| Table 5 – Needed capabilities for the Temporary Protection use case .....             | 21 |
| Table 6 – Temporary Protection use case - Information flows .....                     | 23 |
| Table 7 – Disaster Recovery use case - Operational and end-user requirements.....     | 26 |
| Table 8 – Needed capabilities for Disaster Recovery use case .....                    | 28 |
| Table 9 – Disaster recovery – Information flows .....                                 | 28 |
| Table 10 – Additional security-related capabilities for the three use cases .....     | 30 |
| Table 11: Mapping of NAF templates to OSSAF views.....                                | 36 |
| Table 12: NAF Views: Purpose, contents and data.....                                  | 37 |
| Table 13 - List of users for the City Security use case .....                         | 68 |
| Table 14 - List of users for the Temporary Protection use case .....                  | 73 |
| Table 15 - List of users for the Disaster Recovery use case .....                     | 76 |

## 1 INTRODUCTION

This document provides a consolidated list of SALUS system level requirements expressed in the form of “needed capabilities” (see definition in 6.2.3.2) and “information” flows for the different SALUS scenarios (City Security, Temporary Protection and Disaster Recovery) and their underlying use case. The needed capabilities and information flows are derived based on inputs from WP2 expressed in the form of:

- Goal and Vision for each scenario,
- Story board of each use case (the flow of events for each scenarios and the eventual constraints),
- Actors and respective required interactions,
- Key applications that will be used to handle the mission.

The reader will find in annexes (sections 8 to 10) the storyboards that have been used as inputs to the identification of the system requirements.

It is to be noted that this document focuses on advanced capabilities that are in the scope of SALUS. These are the ones that will enable the efficient and secure support of advanced applications over multiple Public Protection and Disaster Relief (PPDR) networks including legacy systems (TETRA and TETRAPOL) and future systems (LTE private, LTE commercial, Wi-Fi private...).

The first three sections (section 2 to section 4) provide a systematic list of needed capabilities and information flows derived from the three use cases respectively. Section 5 provides additional and key transversal capabilities regarding security and availability. Section 6 describes the Enterprise Architecture (EA) methodology that will be applied in the next deliverables to translate the needed capabilities and information flows into an actual SALUS system architecture.

The last section (section 7), provides a summary of the document, its key achievements and future steps.

## 2 CITY SECURITY – SYSTEM REQUIREMENTS

### 2.1 Inputs

Overall context: Management of a public disorder event in a city context or urban location with permanently deployed PPDR infrastructure that escalates to a critical event which requires the involvement of a significant amount of additional resources and agencies.

A complete storyboard of the City Security use case is provided in Annex 1 (section 8). In summary, the use case starts with a Business As Usual (BAU) management of a planned riot with few police forces (8 officers, as stated in the storyboard) that severely deteriorates into major and violent riots and spreads to over locations with the contribution of interactions in social media. The management of these events necessitate the involvement and the coordination of a significantly higher amount of resources (20,000 more police forces involved across the 15 locations), multiple agencies (police, ambulance, fire brigades, special riot police teams...). Additional external information leveraged in the management of these events includes access to the Closed Circuit TV (CCTV) footage and screening of the social networks. Besides, in the area of the events, there are already in place a permanently deployed TETRA infrastructure and a LTE network with reserved resources for PPDR applications that can be extended on demand.

Table 1 summarizes the City Security use case analysis. Elements have been extracted from the storyboard and referenced for traceability. These elements are translated in the next subsection into needed capabilities and information flows for the future SALUS system.

Table 1 – City Security use case – Operational and end-user requirements

| Reference | Item from the storyboard                                                                                                                                             |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SC1_I1    | No trouble is expected as the same protest has taken place a number of times in the past with no incident. Therefore there is no need for police presence above BAU. |
| SC1_I2    | PPDR specific TETRA network, to be used by operational forces of police, ambulance services, fire brigades.                                                          |
| SC1_I3    | LTE network with reserved capacity for PPDR services. The system also caters public and other professional users.                                                    |
| SC1_I4    | 10 MHz of (LTE) spectrum is reserved for PPDR only.                                                                                                                  |
| SC1_I5    | 10 MHz of additional LTE spectrum is available for PPDR on demand.                                                                                                   |
| SC1_I6    | Control room facilities. However the room is initially staffed for BAU and therefore not staffed by commanders of police, fire brigade, ambulances.                  |
| SC1_I7    | PPDR communication facilities that allow role based access to information.                                                                                           |
| SC1_I8    | A small police team of 8 officers is deployed to maintain peace and ensure city centre access and security is maintained.                                            |
| SC1_I9    | The control room continuously tracks the location of the officers deployed via their GPS enabled handsets. Location updates are sent every 30s.                      |
| SC1_I10   | A group call is made requesting transport for the youth restrained who has now been arrested.                                                                        |
| SC1_I11   | The officer sensing the potential danger of the developing situation presses his emergency button to summon assistance.                                              |

|         |                                                                                                                                                                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SC1_I12 | The EM function automatically enables Video from the officer's phone to be transmitted back to control.                                                                                                                                                           |
| SC1_I13 | The bandwidth requirements of other users operating on the same radio cell are reduced to ensure the video has the radio resources needed.                                                                                                                        |
| SC1_I14 | ..., a police officer calls the control for more resources.                                                                                                                                                                                                       |
| SC1_I15 | A group call to the control room is made requesting more resources.                                                                                                                                                                                               |
| SC1_I16 | Using location tools the police control can see that there are response officers nearby that can immediately assist and dispatches them to the scene.                                                                                                             |
| SC1_I17 | These additional officers switch to the talk-group being used to manage the incident.                                                                                                                                                                             |
| SC1_I18 | A call is already in progress and their radios quickly attach and start receiving the communication.                                                                                                                                                              |
| SC1_I19 | They (the angry youths) have mobile phones and are sending messages via text and social media.                                                                                                                                                                    |
| SC1_I20 | Some (the angry youths) are capturing the scenes on video.                                                                                                                                                                                                        |
| SC1_I21 | They (the angry youths) had received Facebook and Tweet messages and also seen footage on YouTube.                                                                                                                                                                |
| SC1_I22 | The control calls for ambulance to be dispatched.                                                                                                                                                                                                                 |
| SC1_I23 | They (the police control) access local CCTV camera in the area.                                                                                                                                                                                                   |
| SC1_I24 | As not all the cameras covering the area are available due to maintenance, a suitable police officer is identified from his GPS coordinates to stream back to the control room video footage to supplement footage from the CCTV system.                          |
| SC1_I25 | With direction from the control room police officers at the incident are dispatched to arrest identified individuals including the "ring leader". Quality pictures captured from a video camera are sent to a small group of officers dispatched to arrest these. |
| SC1_I26 | A police officer on the ground dials 999/112 using telephony services to call for an ambulance.                                                                                                                                                                   |
| SC1_I27 | The officer is requested by ambulance control to carry out some basic assessment checks/treatment to help sustain life.                                                                                                                                           |
| SC1_I28 | The police use criminal intelligence databases to establish details of the offenders. They discover that they are known trouble makers.                                                                                                                           |
| SC1_I29 | Teams of riot police are called in.                                                                                                                                                                                                                               |
| SC1_I30 | More officers are dispatched.                                                                                                                                                                                                                                     |
| SC1_I31 | Some of the officers deployed are unfamiliar with the location and use Google Street Maps to familiarise themselves with the area.                                                                                                                                |
| SC1_I32 | The fire services are called in, as are more police and ambulance resources.                                                                                                                                                                                      |
| SC1_I33 | Reports received that trouble has broken out outside the police station in a neighbouring city centre police station.                                                                                                                                             |
| SC1_I34 | It is also evident that social media was used to start the second incident.                                                                                                                                                                                       |
| SC1_I35 | The police monitor Internet activity via the social networks.                                                                                                                                                                                                     |
| SC1_I36 | The police use augmented reality to help identify areas/shops that may come under                                                                                                                                                                                 |

|         |                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | attack and to help them to bring the situation under control.                                                                                                |
| SC1_I37 | A gold, silver, bronze command structure is established between police, fire and ambulance.                                                                  |
| SC1_I38 | Resources are also requested from neighbouring police forces.                                                                                                |
| SC1_I39 | Their (neighbouring police forces) radios are remotely programmed with the appropriate talk groups being used.                                               |
| SC1_I40 | A small group of officers in attendance at the scene are dispatched to protect ambulance and fire officers.                                                  |
| SC1_I41 | The fire officers consult a remote database of recommended places to cut the vehicle in order to gain access.                                                |
| SC1_I42 | Reports of more disturbances in other parts of the country.                                                                                                  |
| SC1_I43 | More police fire and ambulance resources are dispatched.                                                                                                     |
| SC1_I44 | Some are wearing body armour with sensors.                                                                                                                   |
| SC1_I45 | Fire arms unit are called and are instructed to switch their radios to Direct Mode of Operations (DMO) and remain in contact with the control via a gateway. |
| SC1_I46 | Police vans and officers from the Territorial Support Group attended the disorder.                                                                           |
| SC1_I47 | The incidents last for 4 days and spread in over 15 towns and cities across the country.                                                                     |
| SC1_I48 | In total, police additional police resources required increased to over 20,000.                                                                              |
| SC1_I49 | The ring leaders were identified using criminal intelligence databases.                                                                                      |
| SC1_I50 | Location services were used for tracking and directing of resources.                                                                                         |
| SC1_I51 | CCTV footage was broadcast to several resources.                                                                                                             |
| SC1_I52 | Wireless Body Area Networks (WBANs) were used to identify officers down and other users in trouble.                                                          |

### 2.1.1 Key applications

The list of key applications mentioned in Annex 1 is the following:

- Remote controlled CCTV access and dispatch (video broadcast) and control,
- Group communications (voice, picture and video),
- Direct mode of operations,
- Emergency button (voice and video),
- Telephony calls,
- Access to databases (for e.g. accessing criminal intelligence data),
- Access to Internet (including augmented reality),
- Location Services for Person and Vehicle,
- Body sensors to detect position and potential troubles,
- Dynamic grouping.

A more exhaustive list of applications required can be found in SALUS D2.2 [2].

### 2.1.2 Main actors

The list of main actors in the response to the incident is the following:

- Police forces (as initial resources involved before the situation escalates)
- Ambulance,

- Fire brigade,
- Special riot police teams,
- Terrestrial support groups,
- CCTV operators.

## 2.2 Needed Capabilities for City Security Use case

Needed capabilities include main and additional ones. Each capability is referenced for further traceability and to each capability is derived from one or multiple operational requirements from Table 1.

Table 2 – Needed capabilities for City Security use case

| Reference | Required capability                                                                                                                                                                                                                | Reference to operational requirements                                                                                                                             |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SC1-C1    | Provide interworking between PPDR communication networks based on different radio access technologies                                                                                                                              |                                                                                                                                                                   |
| SC1-C1.1  | Enable communications between PPDR users in different access networks (e.g. TETRA and LTE) for voice applications (e.g. group calls, one to one calls) and advanced features (late entry, dynamic reassignment, prioritisation...) | SC1_I2,<br>SC1_I3,<br>SC1_I10,<br>SC1_I14,<br>SC1_I15,<br>SC1_I17,<br>SC1_I18,<br>SC1_I22,<br>SC1_I25,<br>SC1_I26,<br>SC1_I27,<br>SC1_I39                         |
| SC1-C1.2  | Enable communications between PPDR users in different access networks (e.g. TETRA and LTE) for low data rates applications (e.g. short messages, status messages, location information, pictures...)                               | SC1_I9,<br>SC1_I16,<br>SC1_I25,<br>SC1_I50                                                                                                                        |
| SC1-C1.3  | Enable emergency communications between PPDR users in different access networks mixing voice and if possible video information from the emergency device                                                                           | SC1_I11,<br>SC1_I12,<br>SC1_I13                                                                                                                                   |
| SC1-C1.4  | Enable communications for a PPDR user across different access networks (agency's PPDR network, other agency's PPDR network and commercial network).                                                                                | SC1_I2,<br>SC1_I3,<br>SC1_I9,<br>SC1_I10,<br>SC1_I11,<br>SC1_I12,<br>SC1_I13,<br>SC1_I14,<br>SC1_I15,<br>SC1_I16,<br>SC1_I17,<br>SC1_I18,<br>SC1_I22,<br>SC1_I25, |

|            |                                                                                                                                                                                                   |                                                                                                                                                      |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
|            |                                                                                                                                                                                                   | SC1_I26,<br>SC1_I27,<br>SC1_I39,<br>SC1_I50                                                                                                          |
| SC1-C2     | Provision of a permanent PPDR system so that it can cope with extra capacity demand in case of major crisis in multiple locations at the same time for the duration to the event (multiple days). | SC1_I1,<br>SC1_I6,<br>SC1_I8,<br>SC1_I15,<br>SC1_I29,<br>SC1_I30,<br>SC1_I32,<br>SC1_I38,<br>SC1_I39,<br>SC1_I42,<br>SC1_I43,<br>SC1_I45,<br>SC1_I48 |
| SC1-C2.1   | Quickly and temporarily increase the capacity of the fixed system                                                                                                                                 | SC1-I4,<br>SC1-I5                                                                                                                                    |
| SC1-C3     | Sense the area to improve situational awareness in the command and control centre (CCC) and in the field                                                                                          |                                                                                                                                                      |
| SC1-C3.1   | Retrieve fixed CCTV footage in the CCC                                                                                                                                                            | SC1_I23                                                                                                                                              |
| SC1-C3.1.1 | Secured access to CCTV flows from the CCTV operator                                                                                                                                               | SC1_I7,<br>SC1_I23                                                                                                                                   |
| SC1-C3.2   | Use of aerial sensing systems (helicopters, fixed wings) to retrieve live video information                                                                                                       | ?                                                                                                                                                    |
| SC1-C3.3   | Use of mobile devices to stream live video from the field to the control room                                                                                                                     | SC1_I24                                                                                                                                              |
| SC1-C3.4   | Dispatching picture/video information to a selected set of PPDR users in the field (could be from different organizations)                                                                        | SC1_I25,<br>SC1_I51                                                                                                                                  |
| SC1-C4     | (Ad-hoc) integration of several agencies/organisations in order to manage a major crisis                                                                                                          |                                                                                                                                                      |
| SC1-C4.1   | (Ad-hoc) Inter-agency communications between CCC (bridging)                                                                                                                                       | SC1_I37                                                                                                                                              |
| SC1-C4.2   | Inter-agency communications between PPDR users in the field from different organisation and the lead CCC (dynamic grouping, delegation of coordinator role)                                       | SC1_I22,<br>SC1_I32,<br>SC1_I38,<br>SC1_I40                                                                                                          |
| SC1-C4.3   | Means to dispatch / access information to select users (role-based access to information)                                                                                                         | SC1_I17,<br>SC1_I45                                                                                                                                  |
| SC1-C4.4   | Means to allow closed group communications with controlled access to main CCC                                                                                                                     | SC1_I45                                                                                                                                              |
| SC1-C4.5   | Means to integrate mobile command posts deployed in the crisis area with the central CCC                                                                                                          | ?                                                                                                                                                    |
| SC1-C5     | Advanced scheduling / monitoring of resources in line with mission needs                                                                                                                          |                                                                                                                                                      |
| SC1-C5.1   | Advanced location of deployed resources (human and vehicles) using                                                                                                                                | SC1_I16,                                                                                                                                             |

|          |                                                                                                                                                                                        |                                                                                             |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
|          | tracking systems (outdoor and indoor)                                                                                                                                                  | SC1_I19,<br>SC1_I24,<br>SC1_I50                                                             |
| SC1-C5.2 | Advanced body sensors to track vital signs, movement, man-down.                                                                                                                        | SC1_I44,<br>SC1_I52                                                                         |
| SC1-C6   | Transmission and access to broadband information                                                                                                                                       |                                                                                             |
| SC1-C6.1 | Means to transmit and receive live video streams between the field and CCC                                                                                                             | SC1_I12,<br>SC1_I24                                                                         |
| SC1-C6.2 | Means to transmit and receive (high quality pictures) picture between the field and CCC                                                                                                | SC1_I25                                                                                     |
| SC1-C6.3 | Means to access Intranet applications and databases (e.g. criminal records, vehicle structural details...) from the field                                                              | SC1_I28,<br>SC1_I41,<br>SC1_I49                                                             |
| SC1-C6.4 | Means to (securely) access the Internet (e.g. Google street, augmented reality) from the field                                                                                         | SC1_I30,<br>SC1_I36                                                                         |
| SC1-C6.5 | Means to provide controlled (dynamic, tuneable), differentiated and guaranteed access to applications according to their characteristics, priority and pre-emption                     | SC1_I12,<br>SC1_I13,<br>SC1_I24,<br>SC1_I25,<br>SC1_I28,<br>SC1_I30,<br>SC1_I36,<br>SC1_I49 |
| SC1-C7   | Sensing Internet / social media to build intelligence of the situation (note: not is the scope of SALUS project but part of the intelligence / information to meet mission objectives) | SC1_I19,<br>SC1_I20,<br>SC1_I21,<br>SC1_I33,<br>SC1_I34,<br>SC1_I35                         |

## 2.3 Information flows for City Security Use case

Table 3 indicates the main characteristics of the information flows per each group of applications.

Table 3 – City Security – information flows

| <b>Location Services</b> |                                                                                                                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <b>Required capability</b>                                                                                                                                                                                                      |
| <b>Source</b>            | Resource Location: GPS receiver (or any other tracking means) in either a handheld or vehicle device                                                                                                                            |
| <b>Destination</b>       | Default: Authorised CCC<br>Option: Information can be sent back out to either a supervising officer in the field or to a selected group of field users (location sharing)                                                       |
| <b>Volume/Intensity</b>  | Small information. Typically few 100 bytes per set, but depending on the number of people on the ground, could amount to a few hundred bytes per second<br>Tuneable range between 10 seconds and 10 minutes to transmit/receive |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | updates of location information                                                                                                                                                                                                                                                                                                                                                     |
| Access Networks                                   | Any networks: e.g. TETRA, LTE private, LTE commercial, long range Wi-Fi                                                                                                                                                                                                                                                                                                             |
| Security level                                    | High on LTE commercial network, medium on private networks<br>Note: some PPDR (e.g. covert) user groups might be authorized to not be tracked                                                                                                                                                                                                                                       |
| Criticality                                       | In BAU low for persons, medium for vehicles; high in crisis situation                                                                                                                                                                                                                                                                                                               |
| <b>Emergency Button</b>                           |                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                                                          |
| Source                                            | Mobile unit in the field                                                                                                                                                                                                                                                                                                                                                            |
| Destination                                       | CCC and other units attached to the same group and/or in the vicinity of the emergency calling party                                                                                                                                                                                                                                                                                |
| Volume/Intensity                                  | Voice: Clear voice quality (at least better than TETRA voice with MOS of 3.6) typically resulting in data rates in the range of 5- 15 kbps depending on voice codec; Fast call set up (less than 200 ms as indicated in [3])<br><br>Data (e.g. standard definition video and location information): Depending on the quality of the video this will typically from 100 kbps -1 Mbps |
| Access Networks                                   | Any networks: TETRA (voice and data –location-), LTE private, LTE commercial and private Wi-Fi (voice, video and data)                                                                                                                                                                                                                                                              |
| Security level                                    | High                                                                                                                                                                                                                                                                                                                                                                                |
| Criticality                                       | Highest including pre-emption to gain immediate access                                                                                                                                                                                                                                                                                                                              |
| <b>Remote controlled CCTV: Data (audio/video)</b> |                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                                                          |
| Source                                            | Video data: Fixed cameras (High Definition flows) and mobile cameras (Standard Definition flows) (as e.g. body worn cameras, cameras mounted in drones, in helicopter, etc.)                                                                                                                                                                                                        |
| Destination                                       | Default: CCC<br>Option: Selected video streams may be directed to mobile devices either vehicles or handhelds                                                                                                                                                                                                                                                                       |
| Volume/Intensity                                  | Depending on the quality of the video (SD, HD but also frame rate per second...) this will typically range from 100 kbps to10 Mbps (refer to [4] and [5] for examples of video quality perception)                                                                                                                                                                                  |
| Access Networks                                   | For fixed cameras private wired LAN networks, complemented by dedicated Wi-Fi point-to-point links; for camera in helicopter and drones dedicated links operating in dedicated frequencies; for body worn cameras LTE private, 3G/LTE commercial                                                                                                                                    |
| Security level                                    | High, including Integrity protection, confidentiality and access control                                                                                                                                                                                                                                                                                                            |
| Criticality                                       | Priority over non-critical data flows                                                                                                                                                                                                                                                                                                                                               |
| <b>Remote controlled CCTV: control</b>            |                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                                                          |
| Source                                            | Default: CCC<br>Option: a mobile unit may have the capability to control a camera. For example a mobile control unit or mobile CCC                                                                                                                                                                                                                                                  |

|                                     |                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Destination</b>                  | Fixed cameras and mobile cameras (e.g. body worn cameras, cameras mounted in drones, in helicopter, etc.)                                                                        |
| <b>Volume/Intensity</b>             | Low volume (typically 0.1- 5 kbps) and low latency to provide real-time control experience                                                                                       |
| <b>Access Networks</b>              | Any broadband network: Private wired networks, dedicated Wi-Fi point-to-point links, dedicated aerial links, LTE private, 3G / LTE commercial                                    |
| <b>Security level</b>               | High, including integrity protection, confidentiality and access control                                                                                                         |
| <b>Criticality</b>                  | Priority over non-critical data flows                                                                                                                                            |
| <b>Data base searching</b>          |                                                                                                                                                                                  |
|                                     | <b>Required capability</b>                                                                                                                                                       |
| <b>Source</b>                       | Numerous, including: Health-care data centres, police data bases, intelligence forces data bases, fire service databases such as building plans, vehicle structural details etc. |
| <b>Destination</b>                  | Health-care professionals, control room, police, special forces, fire personnel                                                                                                  |
| <b>Volume/Intensity</b>             | Low volume for Request (< 255 bytes) , high volume for Result (up to few tens of Mbytes); low latency to provide quasi real-time end-user experience                             |
| <b>Access Networks</b>              | Any broadband network: Wi-Fi, LTE private, 3G/ LTE commercial                                                                                                                    |
| <b>Security level</b>               | End-to-end security; role based access control                                                                                                                                   |
| <b>Criticality</b>                  | Priority over non-critical data flows, pre-emption capabilities                                                                                                                  |
| <b>Internet Access</b>              |                                                                                                                                                                                  |
|                                     | <b>Required capability</b>                                                                                                                                                       |
| <b>Source</b>                       | Publically available data sources and applications via the internet (e.g. augmented reality, Google Maps, social networking sites etc)                                           |
| <b>Destination</b>                  | CCC, commander, public safety professionals (police, fire, medical, special forces)                                                                                              |
| <b>Volume/Intensity</b>             | Data rate like to range from kbps to tens of Mbps and low latency to provide quasi real-time end-user experience.                                                                |
| <b>Access Networks</b>              | Any broadband network: Private LTE, commercial LTE, Wi-Fi                                                                                                                        |
| <b>Security level</b>               | Low                                                                                                                                                                              |
| <b>Criticality</b>                  | Medium, although the source is publically available, the reliance on it could be high.                                                                                           |
| <b>Group communication for data</b> |                                                                                                                                                                                  |
|                                     | <b>Required capability</b>                                                                                                                                                       |
| <b>Source</b>                       | CCC, commander, public safety professional                                                                                                                                       |
| <b>Destination</b>                  | Multiple units simultaneously, including: CCC, commander, public safety professionals (police, fire, medical, special forces)                                                    |
| <b>Volume/Intensity</b>             | Data rate like to range from hundreds of bits to tens of Mbps to provide quasi-real time end-user experience.                                                                    |
| <b>Access Networks</b>              | Any broadband network: Private LTE, commercial LTE, Wi-Fi                                                                                                                        |

|                                      |                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security level                       | Medium for main users and high for specialist users such as coverts                                                                                                                                                                                                                                                                          |
| Criticality                          | Priority traffic, pre-emption capabilities depending on the content.                                                                                                                                                                                                                                                                         |
| <b>Group communication for voice</b> |                                                                                                                                                                                                                                                                                                                                              |
|                                      | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                   |
| Source                               | CCC, commander, public safety professional                                                                                                                                                                                                                                                                                                   |
| Destination                          | Multiple units simultaneously, including: CCC, commander, public safety professionals                                                                                                                                                                                                                                                        |
| Volume/Intensity                     | Clear voice quality required in a noisy environment (at least better than TETRA voice with MOS of 3.6), typical data rates in the range of 5- 15 kbps depending on voice codec;<br>Fast call set up required (< 200 ms [3]).                                                                                                                 |
| Access Networks                      | Any network: TETRA, Private LTE, commercial LTE, private Wi-Fi                                                                                                                                                                                                                                                                               |
| Security level                       | High                                                                                                                                                                                                                                                                                                                                         |
| Criticality                          | Prioritisation within group, only one person to speak; pre-emption capabilities in commercial network<br>Audio interrupt may be an optional requirement to enable more than one person to speak simultaneously.                                                                                                                              |
| <b>DMO</b>                           |                                                                                                                                                                                                                                                                                                                                              |
|                                      | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                   |
| Source                               | Mobile units                                                                                                                                                                                                                                                                                                                                 |
| Destination                          | Mobile units (without access to the infrastructure) and a control room when a gateway is deployed                                                                                                                                                                                                                                            |
| Volume/Intensity                     | For voice: Clear voice quality required in a noisy environment (at least better than TETRA voice with MOS of 3.6), typical data rates in the range of 5- 15 kbps depending on voice codec; Fast call set up required (< 200 ms [3]).<br>For data: Data rate up to typically 1 Mbps for quasi-real-time end-user experience and video quality |
| Access Networks                      | TETRA (voice and low data rate data such as location information) LTE Proximity Service (ProSe) (voice, data and video) and gateway devices                                                                                                                                                                                                  |
| Security level                       | Likely to be high as will be specialist users such as armed response or coverts                                                                                                                                                                                                                                                              |
| Criticality                          | High                                                                                                                                                                                                                                                                                                                                         |
| <b>WBAN</b>                          |                                                                                                                                                                                                                                                                                                                                              |
|                                      | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                   |
| Source                               | Mobile units in the field. Typically from a sensor worn on the body.                                                                                                                                                                                                                                                                         |
| Destination                          | CCC, another mobile unit or senior command                                                                                                                                                                                                                                                                                                   |
| Volume/Intensity                     | Data rate up to a few kbps (depending on the sensor information to be transmitted such as vital signs, environmental data –temperature, chemical sensors-, movement...)                                                                                                                                                                      |
| Access Networks                      | LTE, Wi-Fi, TETRA for backhauling the information from the end-user terminal to the CCC or another mobile unit or senior commander.                                                                                                                                                                                                          |

|                                               |                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | Wireless body area technology (e.g. Bluetooth, ZigBee...) for sensors to end-user terminal                                                                                                                                                                                                                                                               |
| Security level                                | High (both for body area network and backhaul)                                                                                                                                                                                                                                                                                                           |
| Criticality                                   | High (both for body area network and backhaul)                                                                                                                                                                                                                                                                                                           |
| <b>Interoperability</b>                       |                                                                                                                                                                                                                                                                                                                                                          |
|                                               | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                               |
| Source                                        | CCC or mobile units on one network type                                                                                                                                                                                                                                                                                                                  |
| Destination                                   | CCC or mobile units on a different network type                                                                                                                                                                                                                                                                                                          |
| Volume/Intensity                              | For voice: Clear voice quality required in a noisy environment (at least better than TETRA voice with MOS of 3.6), typical data rates in the range of 5- 15 kbps depending on voice codec; Fast call set up required (< 200 ms [3]).<br><br>For data: Data rate up (but not limited) to 1Mbps for quasi real-time end-user experience and video quality. |
| Access Networks                               | TETRA (voice and low data rate), LTE (voice, data and video), Private Wi-Fi (voice, data and video)                                                                                                                                                                                                                                                      |
| Security level                                | Low to medium                                                                                                                                                                                                                                                                                                                                            |
| Criticality                                   | Low to medium                                                                                                                                                                                                                                                                                                                                            |
| <b>Dynamic Group Number Assignment (DGNA)</b> |                                                                                                                                                                                                                                                                                                                                                          |
|                                               | <b>Required capability</b>                                                                                                                                                                                                                                                                                                                               |
| Source                                        | CCC                                                                                                                                                                                                                                                                                                                                                      |
| Destination                                   | Selected mobile units                                                                                                                                                                                                                                                                                                                                    |
| Volume/Intensity                              | Any service to be used in group communications                                                                                                                                                                                                                                                                                                           |
| Access Networks                               | Any networks: TETRA, LTE, Private Wi-Fi                                                                                                                                                                                                                                                                                                                  |
| Security level                                | High as you are remotely changing the configuration of a device                                                                                                                                                                                                                                                                                          |
| Criticality                                   | High                                                                                                                                                                                                                                                                                                                                                     |

### 3 TEMPORARY PROTECTION – SYSTEM REQUIREMENTS

#### 3.1 Inputs

Overall context: Management of public disorder in an Olympic style and sized event - a sports arena - with a combination of permanent and previously deployed temporary PPDR infrastructure. This use case is based on a 3-day high profile international event that occurs in multiple close proximity venues, involving near 50 thousand spectators, including VIP dignitaries. During the second day, just before the main event starts, threats are made to the event organizers and the media alert for the existence of multiple bombs. The PPDR Event Coordination Centre which coordinates with the multi-agency Command and Control Centres (CCC) informs all tactical units (police, ambulance services, fire brigade, event security, transport and road operator) to start a specific evacuation plan . On the outside, operational forces are instructed to restrict access to the stadium and special (covert) forces are instructed search for suspects. Air drones are deployed to have a better view over the terrain. Alerted by the media, some spectators start to panic and trigger a massive disorganized stadium evacuation. This abnormal behaviour is identified and information starts to flow on the screens in and around the venue, through loudspeakers, LTE broadcast services and social media. Meanwhile, the first bomb explodes, increasing the panic and a wave of people is trying to exit the stadium. Security guards use information on their head-up displays to assist one another to streamline the crowd. Security guards separate the injured and apply sensors to monitor vital signs. Disabled people are tagged and also monitored. Shortly after, one of the main exits is blocked by a second explosion, which is filmed and uploaded to social media by numerous spectators. The evacuation plan is adapted to take care of the new situation and is communicated to all operational teams, and partner organisations. Wireless ad-hoc networks are deployed to support the communication overload on specific locations. As the situation is being sorted out, progress on the operation is briefed to the strategic team, partner organisations and to media partners.

The complete storyboard of the Temporary Protection use case, which includes pre-condition and flow of events is provided in Annex 2 (section 9).

Table 4 summarizes the Temporary Protection use case analysis. Elements have been extracted from the storyboard and referenced for traceability. These elements are translated in the next sub-section into needed capabilities and information flows for the future SALUS system.

Table 4 – Temporary Protection use case - Operational and end-user requirements

| Reference | Item from the storyboard                                                                                                                                                                                                                                                               |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SC2-I1    | Previous knowledge on the event type and location (at least 3 to 6 months prior to the event date; for instance an annual event like the London's Notting Hill Carnival is planned 6 months in advance and for a major event like the Olympics the planning starts 3 years in advance) |
| SC2-I2    | Previous access to venue construction plans, exit routes and other relevant information to prepare PPDR operations.                                                                                                                                                                    |
| SC2-I3    | Voice and speech recognition technology for caller identification and translation of key words of interest like location, type of exploding device, time, and claiming terrorist group.                                                                                                |
| SC2-I4    | Application capable of context related information search in existing databases (e.g., criminal intelligence database, patient record database...)                                                                                                                                     |
| SC2-I5    | Multiple PPDR (police, special (covert) forces, ambulance services, fire brigade) and non-                                                                                                                                                                                             |

|         |                                                                                                                                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | PPDR (event security, transport and road operator) operational forces                                                                                                                                                              |
| SC2-I6  | Event Coordination Centre, to coordinate the multi-agency safety and security operations                                                                                                                                           |
| SC2-I7  | Command and Control Centre facilities with capacity to accommodate commanders/representatives (security staff leaders) for specific operational forces                                                                             |
| SC2-I8  | Gold, silver and bronze command structure is established at the Event Coordination Centre between operational (multi-agency) forces                                                                                                |
| SC2-I9  | Long term coverage from PMR networks (example TETRA/TETRAPOL) network, capable of role based communications (to be used by the operational forces)                                                                                 |
| SC2-I10 | Short term portable PMR (example TETRA/TETRAPOL) communication nodes, to increase the PPDR system capacity for the event dates.                                                                                                    |
| SC2-I11 | Secured LTE network with reserved capacity for PPDR services (the system is assumed to also support public and other professional users)                                                                                           |
| SC2-I12 | 10MHz of additional LTE spectrum for PPDR communications                                                                                                                                                                           |
| SC2-I13 | Private telecom operators capable of using broadcast services and to switch over to 'priority mode', in order to disseminate evacuation directions and to limit public access, including limiting bandwidth consuming applications |
| SC2-I14 | Secured IEEE 802.11n (Wi-Fi) network (to be used by operational forces in infra-structure or ad-hoc modes)                                                                                                                         |
| SC2-I15 | Wireless Body Area Networks (WBANs) capable vests for some of the operational forces (police, special (covert) forces, and fire brigade), to monitor health and environment status                                                 |
| SC2-I16 | Health monitoring sensors, to be used on injured spectators                                                                                                                                                                        |
| SC2-I17 | Secured camera enabled heads-up displays to upstream image/video data to the CCCs and to provide ease and seamless access to information to some operational forces (police, special (covert) forces and event security forces)    |
| SC2-I18 | Air drones/helicopters/balloons to provide secured aerial view over the multiple venues, to assist strategic Event Coordination Centre and CCCs' decisions                                                                         |
| SC2-I19 | On-demand capability to deploy additional PPDR resources to specific operational teams                                                                                                                                             |
| SC2-I20 | Outdoor and indoor secured location based services for operational redirection and assistance                                                                                                                                      |
| SC2-I21 | Access to stadium communication facilities (landline, Internet, advertising panels, large screens and loud speakers)                                                                                                               |
| SC2-I22 | Access to CCTV footage, to improve Event Coordination Centre and CCCs' awareness                                                                                                                                                   |
| SC2-I23 | Secure access to information databases (police, hospital)                                                                                                                                                                          |
| SC2-I24 | Video-based behaviour recognition and alerting system                                                                                                                                                                              |

### 3.1.1 Key applications

The following are the key applications identified in the Temporary Protection use case:

- Voice and speech recognition technology,
- Search engine capable of context related information search,
- Event Coordination Centre hosted application for correlation of multiple data sources and display,

- Group communications (voice, video and data such as messages, enhanced messages, pictures...),
- High speed access to data (patient records, criminal data, intelligence, specific knowledge, etc.),
- Fast deployable Wi-Fi infrastructure and ad-hoc networking for local broadband, communication and capacity extension,
- Camera enabled heads-up displays,
- Live video feeds from aerial sources,
- Body sensors for health and environment monitoring,
- Crowd control (loudspeakers, geo-cast of text alarms, evacuation procedures to mobile phones and screens in and out of the stadium, etc.),
- Outdoor and indoor location based capability,
- Remote controlled CCTV,
- Video-based behaviour recognition and alerting system.

A more exhaustive list of applications required can be found in SALUS D2.2 [2].

### 3.1.2 Main actors

The list of main actors in the response to the Temporary Protection use case is the following:

- Police forces,
- Special (covert) forces,
- Ambulance,
- Fire brigade,
- Event security,
- Transport operators,
- Road operator,
- City council.

## 3.2 Needed Capabilities for Temporary Protection Use case

Needed capabilities include main and additional ones. Each capability is referenced for further traceability and to each capability is derived from one or multiple operational requirements from Table 5.

Table 5 – Needed capabilities for the Temporary Protection use case

| Reference | Required capability                                                                                                                                                      | Reference to operational requirement |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| SC2-C1    | Provide interworking and synchronization between PPDR communication networks based on different access technology                                                        |                                      |
| SC2-C1.1  | Inter-agency communications between CCCs (bridging)                                                                                                                      | SC2-I5 to SC2-I7                     |
| SC2-C1.2  | Inter-agency communications between PPDR users in the field from different organisation and Event Coordination Centre (dynamic grouping, delegation of coordinator role) | SC2-I6, SC2-I8...                    |
| SC2-C1.3  | Means to dispatch / access information to select users (role-based access to information)                                                                                | SC2-I9, SC2-I10, SC2-I11             |

|          |                                                                                                                                                                 |                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| SC2-C1.4 | Enable communications between PPDR users in different access networks (LTE and Wi-Fi) for high data rate applications (e.g. video streaming, database access)   | SC2-I17,<br>SC2-I23                                                                                 |
| SC2-C1.5 | Enable communications between PPDR users in different access networks (TETRA/TETRAPOL, LTE and Wi-Fi) for voice applications.                                   | SC2-I16 to<br>SC2-I12,<br>SC2-I14,                                                                  |
| SC2-C1.6 | Enable communications between PPDR users in different access networks (TETRA/TETRAPOL, LTE and Wi-Fi) for low data rate applications (e.g. text based messages) |                                                                                                     |
| SC2-C1.7 | Provide end-to-end secure communications between PPDR users in different access networks                                                                        | SC2-I16 to<br>SC2-I12,<br>SC2-I14,<br>SC2-I17,<br>SC2-I23                                           |
| SC2-C2   | ICT infra-structure capable of advanced services                                                                                                                |                                                                                                     |
| SC2-C2.1 | Voice and speech recognition system                                                                                                                             | SC2-I3                                                                                              |
| SC2-C2.2 | Context related information search                                                                                                                              | SC2-I4                                                                                              |
| SC2-C2.3 | Secure Internet access                                                                                                                                          | SC2-I21                                                                                             |
| SC2-C2.4 | Video-based behaviour recognition and alerting system                                                                                                           | SC2-I24,<br>SC2-I22,<br>SC2-I23                                                                     |
| SC2-C2.5 | CCC hosted application for correlation of multiple data sources and display                                                                                     | SC2-I7,<br>SC2-I8,<br>SC2-I9,<br>SC2-I10,<br>SC2-I14,<br>SC2-I15<br>SC2-I24,<br>SC2-I22,<br>SC2-I23 |
| SC2-C3   | Quickly and temporarily increase the capacity of the installed PPDR system by deploying additional Wi-Fi hotspots                                               | SC2-I14                                                                                             |
| SC2-C4   | Sense the area to improve situational awareness in the CCC and in the field                                                                                     | SC2-I17,<br>SC2-I18,<br>SC2-I22                                                                     |
| SC2-C4.1 | Retrieve CCTV footage in the control room                                                                                                                       | SC2-I22                                                                                             |
| SC2-C4.2 | Upstream image/video information to a selected set of PPDR users in the field                                                                                   | SC2-I23                                                                                             |
| SC2-C4.3 | Use of secured aerial view (drones/helicopters/balloons) to retrieve live image/video information                                                               | SC2-I18                                                                                             |
| SC2-C5   | Provide tracking and monitoring technology                                                                                                                      | SC2-I15,<br>SC2-I16,<br>SC2-I20                                                                     |
| SC2-C5.1 | Health and environmental status for PPDR users                                                                                                                  | SC2-I15                                                                                             |
| SC2-C5.2 | Health on injured spectators                                                                                                                                    | SC2-I16                                                                                             |

|          |                                       |         |
|----------|---------------------------------------|---------|
| SC2-C5.3 | Outdoor and indoor PPDR user location | SC2-I20 |
|----------|---------------------------------------|---------|

### 3.3 Information flows for Temporary Protection Use case

Table 6 indicates the main characteristics of the information flows per each group of applications.

Table 6 – Temporary Protection use case - Information flows

| <b>Remote controlled CCTV: Data (audio/video)</b> |                                                                                                                                                                                                                                                                       |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                            |
| <b>Source</b>                                     | Video data: Fixed cameras and mobile cameras (as e.g. body worn cameras, cameras mounted in drones, in helicopter, etc.)                                                                                                                                              |
| <b>Destination</b>                                | Default: CCC<br>Option: Selected video streams may be directed to special forces                                                                                                                                                                                      |
| <b>Volume/Intensity</b>                           | Depending on the quality of the video (SD, HD but also frame rate per second...) this will typically range from 100 kbps to 10 Mbps (refer to [4] and [5] for examples of video quality perception)                                                                   |
| <b>Access Networks</b>                            | For fixed cameras private wired LAN networks, complemented by dedicated Wi-Fi point-to-point links;<br>For camera in helicopter and drones, dedicated broadband links operating in dedicated frequencies;<br>For body worn cameras, LTE private, or 3G/LTE commercial |
| <b>Security level</b>                             | High, including integrity protection, confidentiality and access control                                                                                                                                                                                              |
| <b>Criticality</b>                                | Priority over non-critical data flows                                                                                                                                                                                                                                 |
| <b>Remote controlled CCTV: control</b>            |                                                                                                                                                                                                                                                                       |
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                            |
| <b>Source</b>                                     | CCC                                                                                                                                                                                                                                                                   |
| <b>Destination</b>                                | Fixed cameras and mobile cameras (as e.g. body worn cameras, cameras mounted in drones, camera in helicopter, etc.)                                                                                                                                                   |
| <b>Volume/Intensity</b>                           | Low volume (typically 0.1-5 kbps), low latency to achieve real-time experience for the end-user in the CCC                                                                                                                                                            |
| <b>Access Networks</b>                            | Any broadband network: Private wired networks, dedicated Wi-Fi point-to-point links, dedicated aerial links, LTE private, 3G/LTE commercial                                                                                                                           |
| <b>Security level</b>                             | High, including integrity protection, confidentiality and access control                                                                                                                                                                                              |
| <b>Criticality</b>                                | Priority over non-critical data flows                                                                                                                                                                                                                                 |
| <b>Data base searching</b>                        |                                                                                                                                                                                                                                                                       |
|                                                   | <b>Required capability</b>                                                                                                                                                                                                                                            |
| <b>Source</b>                                     | Health-care data centres, police data bases, intelligence forces data bases                                                                                                                                                                                           |
| <b>Destination</b>                                | Health-care professionals, control room, police, special forces                                                                                                                                                                                                       |
| <b>Volume/Intensity</b>                           | Low volume for Request (< 255 bytes), high volume for Result (typically up to few tens of Mbytes); low latency to provide quasi real-time experience to end-                                                                                                          |

|                                               |                                                                                                                                                                                                        |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | users                                                                                                                                                                                                  |
| Access Networks                               | Any broadband network: Wi-Fi, LTE private, 3G/LTE commercial                                                                                                                                           |
| Security level                                | End-to-end security; role based access control                                                                                                                                                         |
| Criticality                                   | Priority over non-critical data flows, pre-emption capabilities                                                                                                                                        |
| <b>(Mobile) Ad-hoc networks communication</b> |                                                                                                                                                                                                        |
|                                               | <b>Required capability</b>                                                                                                                                                                             |
| Source                                        | Public safety professionals, cameras, sensors (microphones, detection of harmful substances, explosives, etc.), local data bases                                                                       |
| Destination                                   | Health-care professionals, control room, police, special forces, back office, control room                                                                                                             |
| Volume/Intensity                              | Diverse, from low data rate for sensor information (typically 0.1-20 kbps) to high data rate for large resolution images and video (typically 1 -20 Mbps) to provide real-time experience to end-users |
| Access Networks                               | Wi-Fi, LTE (proximity services) for ad-hoc network; optional, (private) LTE, WLAN, for communication with infrastructure                                                                               |
| Security level                                | End-to-end security, access control also at link layer                                                                                                                                                 |
| Criticality                                   | Priority classes in ad-hoc network, priority and pre-emption capabilities for access to the infrastructure                                                                                             |
| <b>Crowd Control</b>                          |                                                                                                                                                                                                        |
|                                               | <b>Required capability</b>                                                                                                                                                                             |
| Source                                        | CCC                                                                                                                                                                                                    |
| Destination                                   | Public screens in the stadium and outside, mobile phones, alarms, loudspeakers (in specific locations, geo-cast)                                                                                       |
| Volume/Intensity                              | low (in the range of 5-150 bits for e.g. audio alarms, text message alarm, audio) to large ( >1 MB for e.g. evacuation maps)                                                                           |
| Access Networks                               | Any broadband network: Public LTE, Private LTE, Wi-Fi                                                                                                                                                  |
| Security level                                | High; access control is critical; flexible access control facilities (that allow secure transfer of the control of screens from private operator of the stadium to public safety forces)               |
| Criticality                                   | Highest priority; pre-emption rights in public networks                                                                                                                                                |
| <b>Group communication for data</b>           |                                                                                                                                                                                                        |
|                                               | <b>Required capability</b>                                                                                                                                                                             |
| Source                                        | CCC, commander, public safety professional                                                                                                                                                             |
| Destination                                   | CCC, commander, public safety professionals (police, fire, medical, special forces)                                                                                                                    |
| Volume/Intensity                              | Medium to large, from 100 bits to 100's of Mbytes, or larger for high resolution images and video with transmission capabilities to provide quasi-real-time experience to end-users                    |
| Access Networks                               | Any broadband network: Private LTE, commercial LTE                                                                                                                                                     |
| Security level                                | High                                                                                                                                                                                                   |

|                                      |                                                                                                                                                                                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Criticality</b>                   | Priority traffic, pre-emption capabilities depending on the content (as e.g. for update evacuation plans)                                                                                                                       |
| <b>Group communication for voice</b> |                                                                                                                                                                                                                                 |
|                                      | <b>Required capability</b>                                                                                                                                                                                                      |
| <b>Source</b>                        | CCC, commander, public safety professional                                                                                                                                                                                      |
| <b>Destination</b>                   | CCC, commander, public safety professionals                                                                                                                                                                                     |
| <b>Volume/Intensity</b>              | Clear voice quality required in a noisy environment (at least better than TETRA voice with MOS of 3.6), typical data rates in the range of 5- 15 kbps depending on voice codec;<br><br>Fast call set up required (< 200 ms [3]) |
| <b>Access Networks</b>               | Any network: TETRA, Private LTE, commercial LTE                                                                                                                                                                                 |
| <b>Security level</b>                | High                                                                                                                                                                                                                            |
| <b>Criticality</b>                   | Prioritisation within group, only one person to speak; pre-emption capabilities in commercial network                                                                                                                           |
| <b>Location based information</b>    |                                                                                                                                                                                                                                 |
|                                      | <b>Required capability</b>                                                                                                                                                                                                      |
| <b>Source</b>                        | Device attached to a tracking sensor (device can be held by a human or integrated in a vehicle)                                                                                                                                 |
| <b>Destination</b>                   | Default: Authorised CCCs (location of PPDR users might be made available to different CCCs in case of multi-agencies operations);<br><br>Option: Authorized PPDR users devices (held by a human or integrated in a vehicle)     |
| <b>Volume/Intensity</b>              | Small information (typically a few 100 bytes) sent regularly (tuneable – typically 10 seconds to 10 minutes according to mission requirements)                                                                                  |
| <b>Access Networks</b>               | Any network: TETRA, LTE private, LTE commercial, local private (stadium) Wi-Fi network                                                                                                                                          |
| <b>Security level</b>                | High on LTE commercial network/public Wi-Fi , medium on private networks                                                                                                                                                        |
| <b>Criticality</b>                   | Medium (tracking can be complemented with images from cameras); priority traffic in commercial LTE                                                                                                                              |

## 4 DISASTER RECOVERY – SYSTEM REQUIREMENTS

### 4.1 Inputs

The overall context contains the following major event and resulting failure or degradation of networks, and how to restore services for the applications that are required to provide effective public protection and disaster relief.

In this case the event is about a major flooding that extends over the borders of Country A and Country B. Cities in the area are not anymore accessible by roads, and buildings are flooded. Due to the land sliding, the rail infrastructure became severely damaged, and as a result of this, a high speed train has derailed with 200+ citizens being severely injured.

The large scale disruption and high number of casualties and injured people require many PPDR agencies to work together to prevent further casualties and limit further damage to properties and environment. To control the access to the disaster area and prevent looting, the police will have a role to restore and maintain order. Ambulance services will be needed to carry injured people to hospitals, whereby helicopter flights will be required to evacuate people from the affected area and carry injured people from the train disaster area. Help of the fire brigades is needed to rescue people from the train wreckage as well as reduce the burden of flooding within the cities. Public transport organisations are in charge of rescheduling of train, bus and metro services, and communication to vehicles that are stuck in the affected area. The military are tasked for disaster relief, as well as environmental agencies that play a role in the management of water and waste. In addition, the delivery of power, gas and water need to be protected and quickly restored to reduce the economic and health damage by coordinating the work between PPDR organisations and utility companies operating within the area.

Communication networks are severely damaged by the major flooding. Both the coverage and capacity of the public radio (cellular) network and the permanent radio TETRA / TETRAPOL networks for public safety is lost due to power outages and flooding of (cellular) base stations. Even high sites will fail within one or two days period due to the fact that generators cannot be refuelled.

To restore communication there is a need to deploy a temporary and transportable infrastructure based on the same technologies as end users have to use their day-to-day devices. The capacity must also be increased compared to normal day-to-day operation in order to cope with the large number of radio users.

The complete storyboard of the Disaster Recovery use case, which includes pre-condition and flow of events is provided in Annex 3 (section 10).

Table 7 summarizes the Disaster Recovery use case analysis. Elements have been extracted from the storyboard and referenced for traceability. These elements are translated in the next sub-section into needed capabilities and information flows for the future SALUS system.

Table 7 – Disaster Recovery use case - Operational and end-user requirements

| Reference | Item from the storyboard                                                            |
|-----------|-------------------------------------------------------------------------------------|
| SC3-I1    | Need of voice, data and video capable networks to replace destroyed networks        |
| SC3-I2    | Limited time of installation associated with regular training sessions or events    |
| SC3_I3    | Use of day-to-day radio equipment                                                   |
| SC3-I4    | Multiple agencies to interoperate on a national basis and across the border (voice) |

|         |                                                                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | services)                                                                                                                                             |
| SC3-I5  | Local operations command and control but need to report to HQ and Ministries                                                                          |
| SC3-I6  | Various PPDR units (local police, national police, fire brigades, military forces...) to interoperate (voice services)                                |
| SC3-I7  | Group communications voice services including outside the radio network coverage                                                                      |
| SC3-I8  | Consultation of multi-media database including detailed maps of industrial buildings (storage of hazardous material) or plans of the high speed train |
| SC3-I9  | Medium/high quality video services from the field to the local command and control room                                                               |
| SC3-I10 | High quality video services from the field towards experts (not necessary located close to operation theatre)                                         |
| SC3-I11 | Videoconferencing between the field and the local command and control room but also between this control room and the HQ (remote control centre)      |
| SC3-I12 | Deployed networks shall be "consistent" with permanent network when this one will come back to normal mode of operation                               |

#### 4.1.1 Key applications

The list of key applications is the following:

- Voice group communications including interoperability between users in country A or country B but also between users across the border;
- Video services including interoperability between users in country A or country B but also between users across the border;
- Access to databases (high speed train technical information, available rooms into neighbouring hospitals...);
- Videoconferencing between local command and control centre and remote control centre.

A more exhaustive list of applications required can be found in SALUS D2.2 [2].

#### 4.1.2 Main actors

The list of main actors in response to the disaster recovery case is the following:

- Police forces (local and regional organisations);
- Ambulances;
- Fire Brigades;
- Public Transport;
- Military;
- Environmental agencies;
- All sorts of utility (Power, Gas, Water...).

### 4.2 Needed Capabilities for Disaster Recovery Use case

Needed capabilities include main and additional ones. Each capability is referenced for further traceability and each capability is derived from one or multiple operational requirements from Table 8.

Table 8 – Needed capabilities for Disaster Recovery use case

| Reference | Required capability                                                                                                                        | Reference to operational requirement |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| SC3-C1    | Transportable radio solutions with limited time set-up. Similar technologies than the one used for permanent infrastructure                | SC3-I1, SC3-I2, SC3-I3               |
| SC3-C2    | Interconnection of the various transportable and temporary solutions: interconnection between them and also with permanent infrastructures | SC3-I4, SC3-I6                       |
| SC3-C3    | PMR group communications voice services                                                                                                    | SC3-I4, SC3-I6, SC3-I7               |
| SC3-C4    | Device to device communications                                                                                                            | SC3-I7                               |
| SC3-C5    | Non-real time High Speed Data Services                                                                                                     | SC3-I8                               |
| SC3-C6    | Real time High Speed Data Services; video quality and latency as parameters of the end-user application                                    | SC3-I9, SC3-I10, SC3-I11             |
| SC3-C7    | Connection towards remote equipments as central database servers, HQ and remote control centres                                            | SC3-I5, SC3-I8, SC3-I11              |
| SC3-C8    | Needed Capacity for the operation management may be greater than the one designed for routine day-to-day applications.                     |                                      |

### 4.3 Information flows for Disaster Recovery Use case

Table 9 indicates the main characteristics of the information flows per each group of applications.

Table 9 – Disaster recovery – Information flows

| <b>Group Communications for Voice</b> |                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | Required capability                                                                                                                                                                                                                                                                                                      |
| Source                                | Mobile (e.g. vehicular) and handset devices                                                                                                                                                                                                                                                                              |
| Destination                           | Other devices involved in the same “sub-operation” management or mission (attachment to the same talk-group or listen the same direct mode channel)                                                                                                                                                                      |
| Volume/Intensity                      | Limited per device (typically 20 mErI) but could lead to a full time resource allocation<br>Clear voice quality required in a noisy environment (at least better than TETRA voice with MOS of 3.6), typical data rates in the range of 5- 15 kbps depending on voice codec;<br>Fast call set up required (< 200 ms [3]). |
| Access Networks                       | Any network: TETRA, TETRAPOL or private LTE with possible interoperability between the 3 bearers                                                                                                                                                                                                                         |
| Security level                        | From limited level (no ciphering) to ease the interoperability between forces from different agencies up to high level (ciphering and access control for                                                                                                                                                                 |

|                                                      |                                                                                                                                                                                                                                                                           |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                      | management talk-groups)                                                                                                                                                                                                                                                   |
| <b>Criticality</b>                                   | High but may require priority management between the “sub-operations” or missions having in mind that the radio resources may be limited.                                                                                                                                 |
| <b><i>Non-real time High Speed Data Services</i></b> |                                                                                                                                                                                                                                                                           |
|                                                      | <b>Required capability</b>                                                                                                                                                                                                                                                |
| <b>Source</b>                                        | Data servers (request initiated by mobile and handset devices or by a dispatcher position)                                                                                                                                                                                |
| <b>Destination</b>                                   | Mobile and handset devices                                                                                                                                                                                                                                                |
| <b>Volume/Intensity</b>                              | Several 10's of kbps per transaction (down-link) to provide quasi-real-time experience to end-users.                                                                                                                                                                      |
| <b>Access Networks</b>                               | Mainly through Private LTE<br>Through TETRA or TETRAPOL in case of limited size (e.g. still pictures)                                                                                                                                                                     |
| <b>Security level</b>                                | May require authentication when accessing the data servers (as a function of stored data)                                                                                                                                                                                 |
| <b>Criticality</b>                                   | Non-real time constraint but delivery in more than 5 (TBC) minutes to be avoided                                                                                                                                                                                          |
| <b><i>Real time High Speed Data Services</i></b>     |                                                                                                                                                                                                                                                                           |
|                                                      | <b>Required capability</b>                                                                                                                                                                                                                                                |
| <b>Source</b>                                        | Video-capable devices (video camera and accurate display)                                                                                                                                                                                                                 |
| <b>Destination</b>                                   | Video-capable devices or Control room dispatch positions                                                                                                                                                                                                                  |
| <b>Volume/Intensity</b>                              | Several 100's of kbps, up to 1 Mbps per video stream (down-link);<br>Depending on the quality of the video (SD, HD but also frame rate per second...) this will typically range from 100 kbps to 10 Mbps (refer to [4] and [5] for examples of video quality perception). |
| <b>Access Networks</b>                               | Broadband network: Mainly through Private LTE                                                                                                                                                                                                                             |
| <b>Security level</b>                                | May require insurance that the received video stream is the original one (stamping)                                                                                                                                                                                       |
| <b>Criticality</b>                                   | Quality, latency to be defined according to targeted services (high quality for expert consultation, medium quality for reporting videoconference)                                                                                                                        |

## 5 ADDITIONAL SYSTEM REQUIREMENTS ON SECURITY

The previous sections provide an analysis of the needed capabilities and information flows for each use case. They illustrate that most of the needed capabilities and information flows to be considered in the SALUS project are common to the use cases and therefore are relevant to different scenarios and missions that PPDR organisations are and will be facing. Nevertheless, there are certain capabilities which are applicable only to a particular use case. This does not create any sort of impediment. On the contrary, it enhances the variety of proposed solutions and indicates that a specific type of mission requires and involves specific means, organisations and procedures.

However, if the analysis of the use cases and associated storyboards allowed to identify most of the main needed capabilities; SALUS meetings and workshop discussions allowed identifying a major transversal requirement.

Indeed, one of the most critical attributes is related to the security aspects which are a main theme of the SALUS project and the PPDR ecosystem in general. The security aspects can be split in different categories:

- (Mutual) Authentication,
- Confidentiality,
- Integrity,
- Availability.

These needed capabilities are captured in the following table.

Table 10 – Additional security-related capabilities for the three use cases

| Reference | Required capability                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| SCx-C1    | Provide means for mutual authentication of the devices (and users) connecting to the PPDR communication networks...                           |
| SCx-C1.1  | ... when the PPDR user roams between different access networks of the PPDR communication system.                                              |
| SCx-C1.2  | ... when the PPDR user roams onto the PPDR network of another organisation (in country or in a neighbouring country).                         |
| SCx-C1.3  | ... when a PPDR user roams onto a commercial network.                                                                                         |
| SCx-C2    | Provide means to enable additional confidentiality for the communications on different access networks...                                     |
| SCx-C2.1  | ... that can be specific to PPDR agencies and specific PPDR user groups                                                                       |
| SCx-C2.2  | ... that can be specific per applications                                                                                                     |
| SCx-C3    | Provide means to enable integrity (such as video information, access to databases...) for the communications on the different access networks |
| SCx-C3.1  | ... that can be specific to PPDR agencies and specific PPDR user groups                                                                       |
| SCx-C3.2  | ... that can be specific per applications                                                                                                     |
| SCx-C4    | The PPDR communication network must ensure a system availability between typically 99.9 and 99.999%                                           |

## 6 ENTERPRISE ARCHITECTURE METHODOLOGY

### 6.1 Introduction

#### 6.1.1 Core concepts and definitions

In order to establish a common understanding of Enterprise Architecture (EA) in the context of SALUS, a base set of definitions and core concepts has to be introduced. The architecture is the first concept to be introduced. For SALUS the two following definitions are suitable.

*Architecture is:*

1. The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution [6].
2. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time [7].

The second definition is more general than the first one. It encompasses not only a single system view but also takes System-of-System groupings into account. Both definitions state that architecture reveals an evolutionary component.

In aligning architecture and enterprise, one has to define the concept of enterprise. For SALUS the definition in [9] is best suited:

*“Enterprise” is taken here in its broadest sense, defined as the joint undertaking of one or more organizations that operate across a distributed and often complex environment.”*

This definition clearly states that, in SALUS, enterprises are mainly seen as non profit-oriented organizations or complex structures of organizations (inter-organizational aspect of enterprise definition) such as national PPDR organizations, for example national police or fire-fighter organizations. In addition, the definition is general enough for incorporation of profit-oriented organisations such as private security services in the PPDR context.

The third concept to be introduced is the concept of an Enterprise Architecture. As with the previous concepts there also exist a huge number of definitions on what enterprise architecture is. The following lists three definitions suitable for SALUS.

*Enterprise Architecture is:*

1. In the broadest sense the discipline to align people, processes and assets to the strategic objectives of an organization... [8].
2. The organizing logic for business process and IT capabilities reflecting the integration and standardization requirements of the firm's operating model [9].
3. A method that incorporates strategic business thinking, information assets, and the technical infrastructure of an enterprise to promote information sharing across agency and organizational boundaries [10].

In summarizing these three definitions, one can look at enterprise architecture as the attempt to align people, processes and information technology (IT) according to the enterprise goals in a structured and holistic approach.

Nevertheless, trying to align people, processes and IT accordingly leads to highly complex relationships to be explored, analysed and described. One typical approach for tackling these

complexities is to subdivide an EA into different levels or viewpoints/perspectives, representing different stakeholder interests and architecture aspects. A typical structuring is shown in Figure 1 [11].

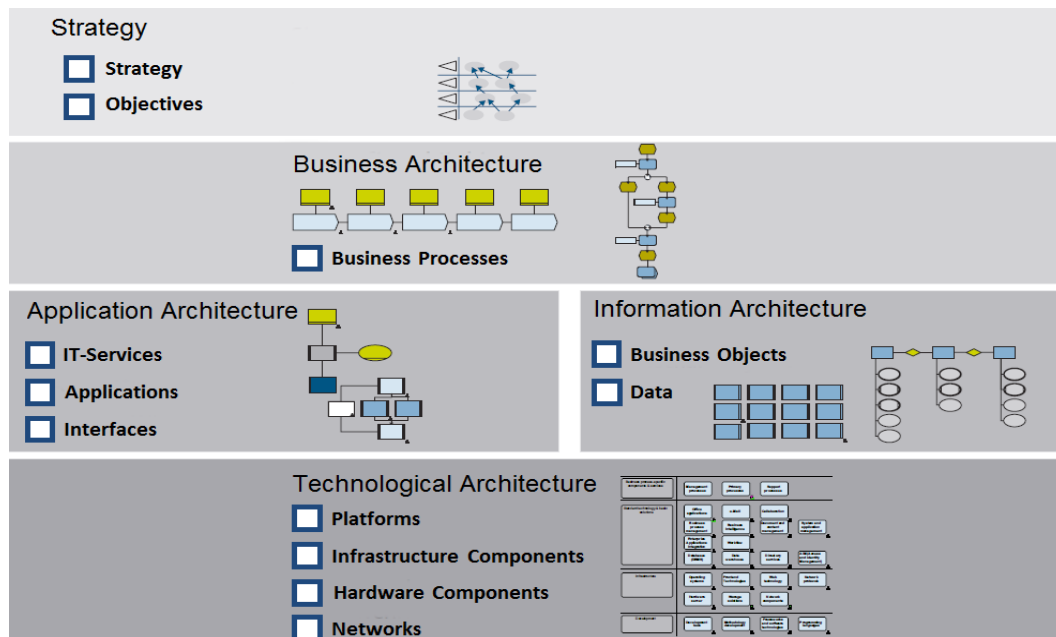


Figure 1: Typical structuring of an EA into different levels (modified after [11])

According to this, an EA is developed and described at a 5 level approach. The Strategic perspective describes the enterprise vision(s) and models objectives (goals) as substantial elements of an overall business strategy. The Business perspective describes the tasks/activities level of an enterprise. It provides a view on organization, resources and business processes with different degrees of abstraction. In addition it aligns capabilities envisaged with dedicated business processes. The Application perspective focuses on the intended or as is application landscape defined at logical and system level. It also links application landscape components to dedicated business process steps. Closely coupled to the Application perspective is the Information perspective. This perspective includes business objects and data models defined at logical and data level and also depicts dependencies between the various data and business objects. The last perspective is the Technological perspective. It describes enterprise daily operations, focuses on physical components - like computers, devices or networks – and represents protocols, service levels, service providers as well as their regional distribution.

### 6.1.2 Problem addressed by an EA

The application of EA is not an end in itself. It receives its “raison d'être” from the challenges of modern IT landscapes. Inherent to modern IT and communication systems is the constant increase of complexity. For example the introduction of network enabled concepts in order to improve mission effectiveness requires the consideration of highly complex System-of-System solutions rather than single systems. This is further complicated by the fact, that more and more cross-border or even international missions (for example in the PPDR domain) are going to be executed, putting more emphasis on the aspect of interoperability. In addition to the alignment of different systems it is necessary to deal with a diversity of users (aka stakeholders, e.g. Nations, Agencies, End-Users, Industry, and Research etc.) and their different interests being involved in modern IT solutions. This requires approaches to structure, communicate and visualize the complexity according to different stakeholder capabilities. In providing those approaches it is even possible to compare different solutions addressing the same problem.

Taking special account of Non Governmental / Governmental Organisations (NGO/GO), the application of EA by providing agency-wide directives for development and use of architectures and the standardization of model and products (architecture artefacts), can according to [8]:

- Create a basis for coherent, consistent and technically reasonable decisions in supporting for example Programme - and Technology- Management by enabling a repeatable decision making process in order to govern capital invests.
- Support stakeholder communications providing a common language, processes and structure for the establishment of continuous communication among strategic, operational and tactical leadership.
- Master complexity through different perspectives and modelling steps supporting Information-Management concerning the architecture itself but also supporting Information-Management related to information contained in SOPs by defining the underlying Information model.
- Create a basis for tools and reusability supporting interoperability, understanding interoperability as “the capability of two or more organizations or discrete parts of the same organization to exchange decision-critical information and to use the information that has been exchanged” [8].

Because of its importance, one additional note on interoperability has to be made. EA deals with interoperability in a holistic approach. That means, that interoperability is not only addressed at the technical and device level but also on the level of information systems, information models or communication systems and even up to organizational level dealing with interoperability of knowledge, aligned procedures and operations or even harmonized strategies and high level objectives.

### 6.1.3 Overview on EA frameworks

Supporting the development of dedicated enterprise architecture is the task of Enterprise Architecture Frameworks (EAF). According to [12], in 2011 it existed more than 50 published frameworks for this purpose, for example ADS, AGATE, EAF, GERAM, MODAF, PERA, TISAF, E2AF, CIMOSA, SABASA, OBASHI, ARIS etc. to name a few. The most well known frameworks are the The Open Group Architecture Framework (TOGAF) [7] and Zachman Architecture Framework (ZAF) [13] and the NATO Architecture Framework (NAF) [14].

In general EA frameworks have different characteristics concerning intension and content. Some provide a methodology, others provide templates and meta-models, some provide governance aspects, others also provide tool support and some provide combinations of parts or all of them. The intensions covered range from management support through Government & Agencies, Military, Interoperability and Manufacturing-specific to pure technically oriented frameworks. EAF have usually an evolutionary development over time incorporating several influences/concepts from other frameworks. Figure 2 provides an example for the context, evolution and influences of the NATO Architecture Framework (NAF). NAF is shown as an example because parts of its concepts play an essential role in describing the EA for SALUS (see 6.2.2) using the proposed **Open Safety & Security Architecture Framework (OSSAF)** [8].

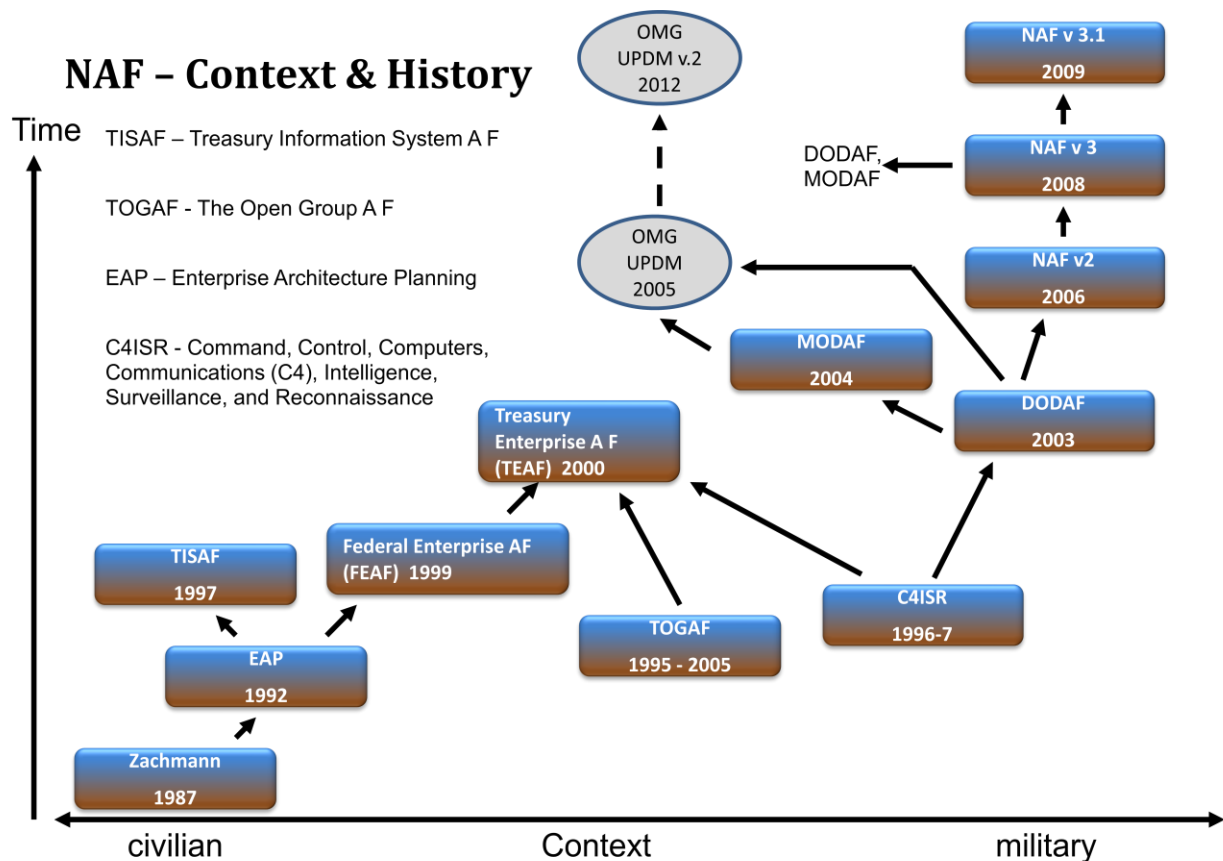


Figure 2: Context, evolution and influences to NAF

#### 6.1.4 Open Safety & Security Architecture Framework (OSSAF)

OSSAF is chosen as enterprise architecture framework for SALUS since it addresses Public Safety & Security agencies directly. Details can be found in the OSSAF whitepaper [8]. Being in a proposal state, the framework incorporates concepts of several mature enterprise architecture frameworks such as the Zachman Architecture Framework (ZAF), the TOGAF framework and the NATO Architecture Framework (NAF) [13]. Reusing fundamental concepts provides a sound foundation to OSSAF. There is also an explicit statement within the whitepaper, that a mapping between OSSAF and other existing frameworks is possible. Nevertheless OSSAF builds mainly on (see Figure 3):

1. The methodology of collecting information and artefacts contributing to the architecture from TOGAF.
2. The two dimensional matrix representation of the framework for structuring the different perspectives.
3. The NAF meta-model and views for the description of the individual templates describing the content of the different perspectives.

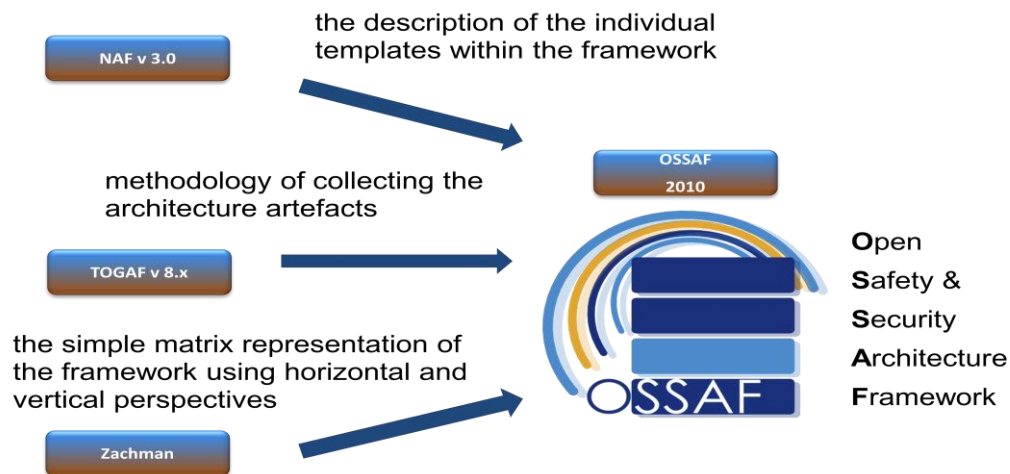


Figure 3: Inputs to OSSAF

OSSAF proposes a total of four perspectives and twenty views. In general, it depends on the intention of the architecture under development which views are actually instantiated. In other words the views can be tailored to the specific needs of the architecture under consideration.

## 6.2 Methodology

### 6.2.1 EA derivation process

The process for the derivation of the SALUS enterprise architecture follows a pragmatic approach, taking the SALUS project volume under consideration. Therefore the OSSAF proposed Architecture Development Method (ADM) [7] (see 6.1.4) is tailored to a lean custom approach.

This approach uses the use cases as main input. Since the use cases were developed in close cooperation with users, it is assumed that they reflect user's needs in a sufficient manner. In case that they don't provide enough input to the development of the perspectives/views the OSSAF Engagement Questionnaire (Appendix H) will be used to obtain the required information.

After definition of a common modelling vocabulary (see 6.2.2) the next steps include:

- Define scope and principles of the architecture (e.g. use SOA paradigm),
- Tailor the views,
- Define Vision and Goals,
- Define stakeholders addressed,
- Analyze Scenarios/Use Cases on functional requirements,
- Analyze Scenarios/Use Cases on operational Capabilities required,
  - Starting point are the 6 top-level Capabilities of OSSAF,
- Derive Capability taxonomy and dependencies,
- Identify operational Context including Nodes, Players, Activities, Information flows, Processes and Constraints (e.g. operational rules),
- Identify Services and Systems in order to support the Capabilities and operational requirements,
- Design Services and Systems as well as their interactions (logical definition),
- Define technical implementation of Services and Systems (physical definition).

## 6.2.2 Definition of the Modelling Vocabulary

The first step in developing the enterprise architecture is to define a common vocabulary/meta-model in order to describe the architecture, i.e. its components and relationships, in a consistent and coherent way. This also supports the use of tools for architecture modelling. Since the OSSAF framework already proposes to use NAF views where suitable as templates for describing the OSSAF views and the NAF views defines a vocabulary, the SALUS approach is going to use NAF as the modelling vocabulary where suitable. In general NAF provides a mature common meta-model to describe the contents of the corresponding views. Every view contains a section of the overall meta-model in order to describe view-specific contents and relations. In addition to the concepts and relationships the meta-model also defines the semantics of each of these elements [14]. It is intended to reuse the meta-model respectively the views in SALUS where suitable. Being in proposal state, OSSAF actually does not define the contents of the NAF meta-model being part of the corresponding OSSAF views; only general hints are given. Therefore, at first, a mapping between OSSAF views and NAF views has to be established. The following table summarizes the first results of a general mapping for use in SALUS. Each column represents a perspective defined by the OSSAF framework. The rows represent the views per perspective and their representation using NAF. For example to describe the “Capability Planning” view of the “Strategic” perspective it is suggested to use the NAF Capability View-2 (“NCV-2”) and Capability View-4 (“NCV-4”) view accordingly.

Table 11: Mapping of NAF templates to OSSAF views

| O<br>S<br>S<br>A<br>F<br><br>V<br>I<br>E<br>W<br>S | OSSAF PERSPECTIVE      |                    |                            |                                     |                            |                                                          |                           |                            |
|----------------------------------------------------|------------------------|--------------------|----------------------------|-------------------------------------|----------------------------|----------------------------------------------------------|---------------------------|----------------------------|
|                                                    | Strategic              |                    | Operational                |                                     | Functional                 |                                                          | Technical                 |                            |
|                                                    | Vision & Goals         | NAV-1<br>NCV-1     | Use Case Scenarios         | No proper NAF view -> textual       | Systems & Services         | NSOV-1<br>NSOV-2<br>NSOV-3<br>NSOV-4<br>NSOV-5<br>NSV-12 | Solution Context          | No proper NAF view         |
|                                                    | Capability Planning    | NCV-2<br>NCV-4     | Operational Concepts       | NCV-4<br>NCV-5<br>NCV-6<br>NOV-1    | Functional Requirements    | NSV-2d<br>NSV-4<br>NSV-5<br>NSV-6<br>NSV-7<br>NSV-10a    | Standards & Protocols     | NTV-1                      |
|                                                    | Funding Model          | No proper NAF view | Operational Nodes Model    | NOV-2                               | Systems Connectivity Model | NSV-1<br>NSV-2a<br>NSV-2b                                | Device Connectivity Model | NSV-2a<br>NSV-2b<br>NSV-2d |
|                                                    | Laws & Regulations     | No proper NAF view | Organization Chart         | NOV-4                               | Systems Interface Model    | NSV-1<br>NSV-2<br>NSV-3                                  | Product Specification     | (NTV-1)                    |
|                                                    | Local Market Landscape | No proper NAF view | Process Model              | NOV-5<br>NOV-6a<br>NOV-6b<br>NOV-6c |                            |                                                          | Product Configuration     | NTV-3                      |
|                                                    |                        |                    | Information Exchange Model | NOV-3<br>NOV-7                      |                            |                                                          |                           |                            |

As the table shows, a direct mapping between OSSAF and NAF views is not always possible. For example the OSSAF “Funding Model” could not directly be mapped to a corresponding NAF view. In such cases suitable representations will be proposed by SALUS. But this holds true only for such views that will be instantiated in developing SALUS EA. For example, if during the tailoring step the decision is made not to instantiate the “Solution Context” view, for which actually no NAF representative exists, then no representation will be developed.

One has also to keep in mind that this mapping is preliminary based on the expertise gathered in previous projects using the NAF framework. It may be altered according to new findings during the SALUS architecture development.

The NAF documentation [14] provides the complete definition of the NAF meta-model and the NAF views. The first is provided in CHAPTER 5 “NATO Architecture Framework Meta-model (NMM) and Architecture Data Exchange Specification (ADES)” of the documentation, the latter in CHAPTER 4 “Architecture Views and Subviews”. Therefore it is not repeated in the context of this document. One should refer to these documents in order to get a detailed insight and understanding. Nevertheless in order to get an overview on what the intention of a specific view is, the following table lists the name of the view, its purpose and gives some of the content and model elements that could be incorporated. All information is taken and compiled from [14].

Table 12: NAF Views: Purpose, contents and data

| Name                                 | Purpose                                                                                                                                                                                                                          | Content                                                                                                                                                                                                                                                                    | Data (may) Included                                                                                            |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| NAV-1 Overview & Summary Information | provides an executive-level summary information allowing referencing and comparison between architectural descriptions                                                                                                           | overarching aspects of architectures that relate to all views                                                                                                                                                                                                              | usually a structured text product                                                                              |
| NCV-1, Capability Vision             | provides strategic context for the capabilities described in the architecture, also provides a high-level scope for the architecture; high-level, description of capabilities in terminology understood by non-technical readers | information provides guidance on future capabilities and allows acquisition specialists to identify future needs<br><br>more general than the scenario-based scope defined in an NOV-1<br><br><b>not intended to specify the system requirements, or user requirements</b> | Operational objective, Capability<br><br>usually presented as text, with accompanying illustrations, if needed |
| NCV-2, Capability Taxonomy           | provides a structured list of capabilities and sub-capabilities required within a capability area during a certain timeframe                                                                                                     | used to capture and organize capabilities required for the vision established in the Capability Vision; capabilities can show the required capabilities for current and future enterprises                                                                                 | Capability, Capability Specialization (relationship between capabilities)                                      |
| NCV-4, Capability Dependencies       | provides a means of analyzing the dependencies between capabilities                                                                                                                                                              | describes the dependencies between capabilities and also defines their logical groupings;<br><b>not intended to represent individual systems or items of equipment, a</b>                                                                                                  | Capability, Capability Dependency (relationship), Capability Composition (relationship)                        |

| Name                                                | Purpose                                                                                                                                                          | Content                                                                                                                                                                                                                   | Data (may) Included                                                                                                                                |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     |                                                                                                                                                                  | capability may be satisfied by a group of systems                                                                                                                                                                         |                                                                                                                                                    |
| NCV-5, Capability to Organisational Deployment      | used to support the capability management process, addresses the fulfilment of capability requirements                                                           | shows deployment of resources (organizational elements and Systems) to satisfy certain capabilities                                                                                                                       | Capability, Capability Configuration, Resource Interaction (between Capability Configurations or their components)                                 |
| NCV-6, Capability to Operational Activities Mapping | describes the mapping between capability elements and the operational activities that those capabilities support                                                 | identifies how operational activities can be performed using various available capability elements                                                                                                                        | Capability, Operational Activity                                                                                                                   |
| NOV-1, High-Level Operational Concept Description   | can be used to orient and focus detailed discussions utility as a facilitator of human communication, is intended for presentation to high-level decision makers | the most general of the architectural views and the most flexible in formal; describes the tasks and activities, operational elements, and information exchanges required to conduct operations                           | Operational Nodes i.e. Headquarters, Systems, Organisations, Information Flows, Environmental context objects ...                                  |
| NOV-2, Operational Node Connectivity Description    | illustrates the operational domain's needs for information exchange in support of operational activities                                                         | depicts required exchanges of different types of information (e.g. data, voice, and video) between nodes, or particular services required at different nodes; illustrates operational needs and not the systems solutions | Nodes, Needlines (bundles of information exchanges), Node Connections (flows of materiel, people or energy), Operational Activities, Locations ... |
| NOV-3, Operational Information Requirements         | depicts the operational characteristics of the information                                                                                                       | describe who exchanges what information, with whom, why the information is necessary, and with what quality the information exchange must occur                                                                           | Information Exchanges (associated with a Needline), Information Elements (carried by one or more Information Exchange)                             |
| NOV-4, Organisational Relationship Chart            | identifies the key players in the operational domain subject to architecture; illustrates the organizational relationships among them                            | players may be deployed to the nodes of an NOV-2; adds details how key players interact to conduct their operational activities; players best described as role-based descriptions                                        | Organisation Types, Resource Composition relationships, Resource Interaction relationships, Post Types, Roles, Competences ...                     |
| NOV-5, Operational Activity Model                   | provides a clear picture of how operations are performed and thereby support analysis and design of services and systems                                         | describes operational activities (or operational tasks) and Input/Output (I/O) flows between activities                                                                                                                   | Operational Activities, Standard , Operational Activity Flow Objects, Swimlanes (each associated with a Node)                                      |

| Name                                               | Purpose                                                                                                                                             | Content                                                                                                                                                                                                             | Data (may) Included                                                                                                                                  |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOV-6a, Operational Rule Model                     | specifies operational constraints on an enterprise, a mission, or an operation, business, or on an architecture                                     | constraints on different levels, i.e. mission level, operation level, or lower levels                                                                                                                               | rules can be expressed in a textual form, for example, If (conditions) exist, and (this event) occurs, then (perform these actions)                  |
| NOV-6b, Operational State Transition Description   | describes how an operational node or activity responds to various events by changing its state                                                      | represents the sets of events to which the architecture responds                                                                                                                                                    | Operational Activity, Node, Operational State                                                                                                        |
| NOV-6c, Operational Event-Trace Description        | provides the next level of detail from the initial operational concepts; allows the tracing of actions in a scenario or critical sequence of events | provides a time-ordered examination of the information exchanges between participating operational nodes as a result of a dedicated scenario                                                                        | Operational Message, Operational Exchange, Node...; each event-trace diagram has an accompanying description that defines the corresponding scenario |
| NOV-7, Information Model                           | analyzes the information aspects of the operational domain and to guide the design of information systems                                           | a representation of a domain object model according to its information aspect, a model of the information about the concepts in the universe of discourse;<br><b>not intended to reflect data storage solutions</b> | Entity, Information Element, Business rule                                                                                                           |
| NSOV-1, Service Taxonomy                           | to organise knowledge according to the service perspective, and to facilitate harmonization of services across multiple domains                     | classes of services, rather than the service implementations, classified according to a specific criterion                                                                                                          | Service                                                                                                                                              |
| NSOV-2, Service Definitions                        | specifies the properties of services and defines the interface of the service explicitly                                                            | list of service definitions                                                                                                                                                                                         | Service, Service Interface, Service Operation, Service Attribute, Service Policies ...                                                               |
| NSOV-3, Services to Operational Activities Mapping | shows which operational activities are supported by which services                                                                                  | forms a line of reasoning that interrelates capabilities, operational activities, services and systems through the use of traceability links                                                                        | services should be in direct or indirect support of operational activities<br>Service, Operational Activity                                          |
| NSOV-4, Service Orchestration                      | shows how services can be combined and sequenced to provide a 'higher level' service                                                                | set of services, used in conjunction, capable of satisfying certain operational objectives that cannot be achieved by any of the services alone                                                                     | Service, Service Composition, Service Interface ...                                                                                                  |
| NSOV-5, Service Behavior                           | specifies the function and behaviour of individual services to fully define the sequencing of messages and                                          | model of the sequencing and timing of interactions between services                                                                                                                                                 | Service, Service State Machine, Service Interface ...                                                                                                |

| Name                                                                | Purpose                                                                                                                                                                            | Content                                                                                                                                                                                      | Data (may) Included                                                              |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
|                                                                     | operations that form part of the service                                                                                                                                           |                                                                                                                                                                                              |                                                                                  |
| NSV-1, System Interface Description                                 | addresses composition and interaction of resources, both technical systems and also organisational resources                                                                       | <b>NSV-1 is NOT intended for detailed descriptions</b> , a system's structural design addressed in more detail in other views                                                                | System, Capability Configuration, Physical Asset, Resource Interaction ...       |
| NSV-2a, System Port Specification                                   | shows the ports of a system and the protocols supported by each of those ports, provide a specification for how a client in the environment of a system can connect to that system | defines the ports on each system, and the protocol / hardware stack that is specified or implemented for each of those ports                                                                 | System, System Port, Protocol                                                    |
| NSV-2b, System to System Port Connectivity                          | specifies the physical, infrastructural nature of a connection between two systems                                                                                                 | defines the connections between individual ports and shows the protocols and hardware spec used for each connection                                                                          | System, System Port, Port Connection, Protocol                                   |
| NSV-2d, Systems Communication Quality Requirements                  | specifies specific quality requirements applicable to communications between systems                                                                                               | defines the systems that communicate primarily through the radio and uses various portions of the radio spectrum                                                                             | System, System Port, Port Connection, Protocol, Spectrum Allocation              |
| NSV-3, Systems to Systems Matrix                                    | tabular summary of the resource interactions specified in the NSV-1                                                                                                                | allows a quick overview of all the resource interactions specified                                                                                                                           | Resource, Resource Interaction                                                   |
| NSV-4 System Functionality description                              | assigns system functions to specific systems, system components and/or nodes and therefore delineate lines of responsibility                                                       | describes systems (NSV-1) in terms of structure (functional decomposition) and behaviour (data flows between system components realizing system functions)                                   | Function, Function Decomposition, Function Flow, Data Element                    |
| NSV-5, Systems Function to Operational Activity Traceability Matrix | shows how the system function supports the conducting of the operational activity<br>NSV-5 is an explicit link between the NOV and NSV                                             | a mapping of operational activities to system functions                                                                                                                                      | Function, (Functional), Resource, Operational Activity                           |
| NSV-6, Systems Data Exchange Matrix                                 | describes the characteristics of the system data exchanged between systems, it focuses on automated information exchanges                                                          | System data exchanges express the relationship across systems, system functions, and system data flows and focus on the specific aspects of the system data flow and the system data content | System, System Port, Data Element with additional data attributes and properties |
| NSV-7, System                                                       | communicates which                                                                                                                                                                 | specifies the quality                                                                                                                                                                        | Functional Resource (system,                                                     |

| Name                               | Purpose                                                                                                                                                                        | Content                                                                                                                                                                                                       | Data (may) Included                                                                                                                                                                                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quality Requirements Description   | quality characteristics are considered most crucial for the successful achievement of the mission goals assigned to the system                                                 | characteristics of systems, system hardware/ software items, their interfaces (system data carried by the interface as well as communications link details that implement the interface), and their functions | role, or capability configuration), Measurable Property, Qualitative Property                                                                                                                                |
| NSV-10a, Systems Rule Model        | specifies functional and non-functional constraints on their implementation aspects of the architecture (for example, the structural and behavioural elements of the NSV views | describes constraints on the resources, functions, data and ports that make up the NSV physical architecture                                                                                                  | rules may be expressed in natural language, as with NOV-6a:<br><i>Imperative</i> – a statement of what shall be under all conditions – e.g. —B shall be less than 6.0ll<br><br><i>Conditional Imperative</i> |
| NSV-12, Service Provision          | purpose of NSV-12 is to illustrate which systems contribute to the provision of which services                                                                                 | describes how a service is implemented by one or more systems; a particular implementation of a service can be seen as a capability configuration that is associated with this service                        | Service, Capability Configuration                                                                                                                                                                            |
| NTV-1, Technical Standards Profile | governs what hardware and software may be implemented and on what system                                                                                                       | defines the technical and non-technical standards, guidance and policy applicable to the architecture                                                                                                         | Standard, Protocol                                                                                                                                                                                           |
| NTV-3, Standard Configurations     | describes standard configurations that are applied to or emerge from the architecture effort used or encountered in any of the views developed in the architecture effort      | intended to capture and explicitly describe configurations that are of value to the ongoing or to future architecture projects                                                                                | Node, Location, System, Resource Interaction                                                                                                                                                                 |

### 6.2.3 Proposed Model for SALUS

It is the proposed approach for SALUS to reuse the NATO Architecture Framework (NAF) meta-model and NAF views where suitable to represent the different OSSAF views included in the different OSSAF perspectives. As previously stated NAF is in a very mature state, is widely used in military and non-military domain, provides a very powerful and expressive vocabulary (meta-model) and has proven its holistic approach in order to describe architecture in an organisational context. Therefore the reuse of the NAF meta-model and NAF views is a valid approach for SALUS.

#### 6.2.3.1 Overall model

The following chapter provides a simplified overview on the core concepts and their relationships as defined in the meta-model of the NATO Architecture Framework (NAF) in order to be used in SALUS. Not all concepts, relationships and the corresponding attributes are

shown. Neither is the cardinality of the relationships shown. A detailed meta-model description as well as the description of the semantics of each concept and relationship can be found in [14]. It is not replicated here. In general for SALUS only a subset of the NAF meta-model is used. The extent to which this NAF meta-model is used may change due to further findings during EA construction.

One has to keep in mind, that dedicated views actually represent a section of the overall model. In combining different views and due to the interlinked model, one can trace architecture elements from the enterprise context (visions, goals and capabilities) down to the systems and technical level.

The following three figures provide an overview of the overall model. A separated representation according to thematic priorities is done for reasons of simplicity, while the overall model is still interlinked.

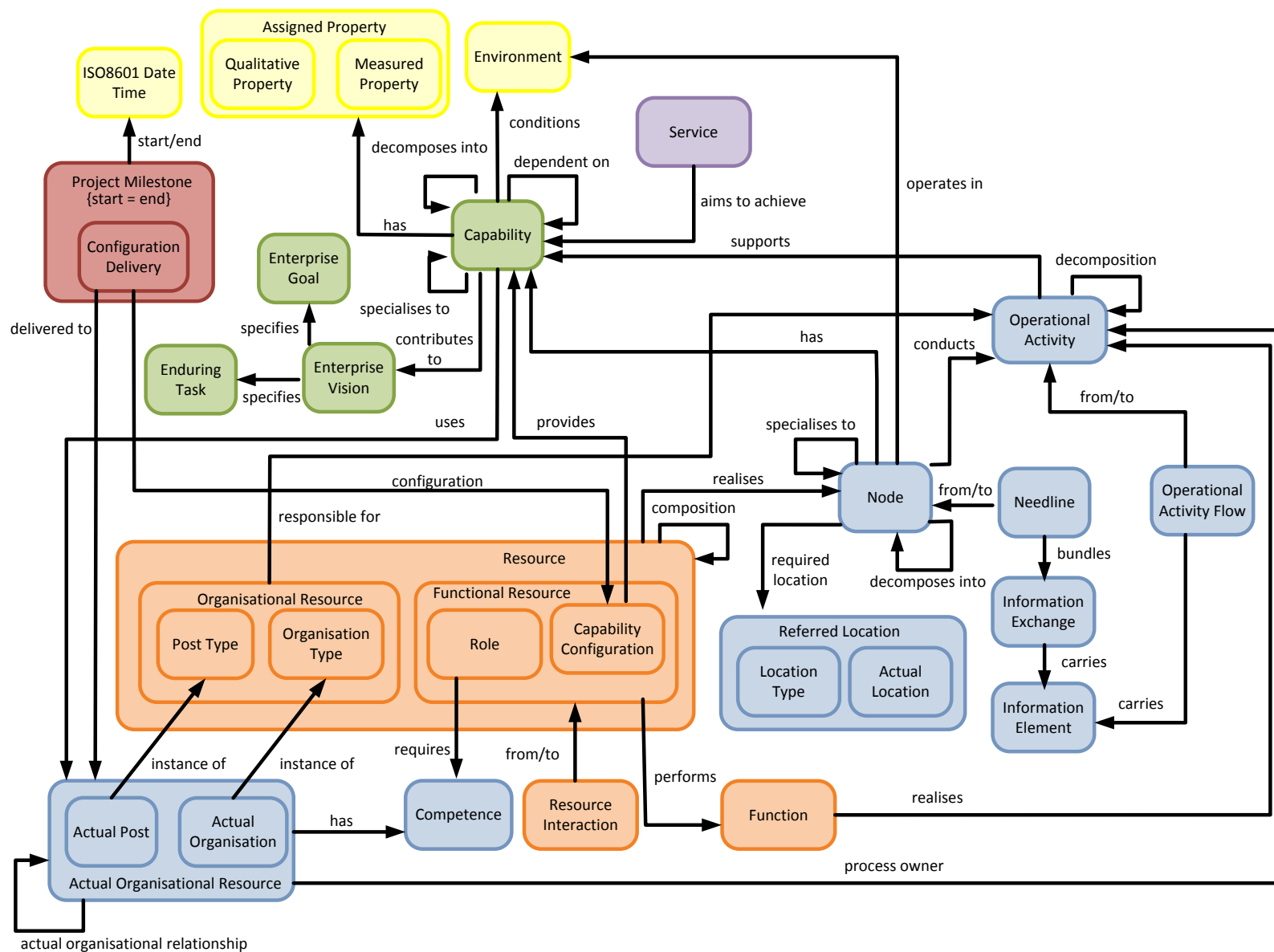


Figure 4: Model elements according to the strategic and operational scope

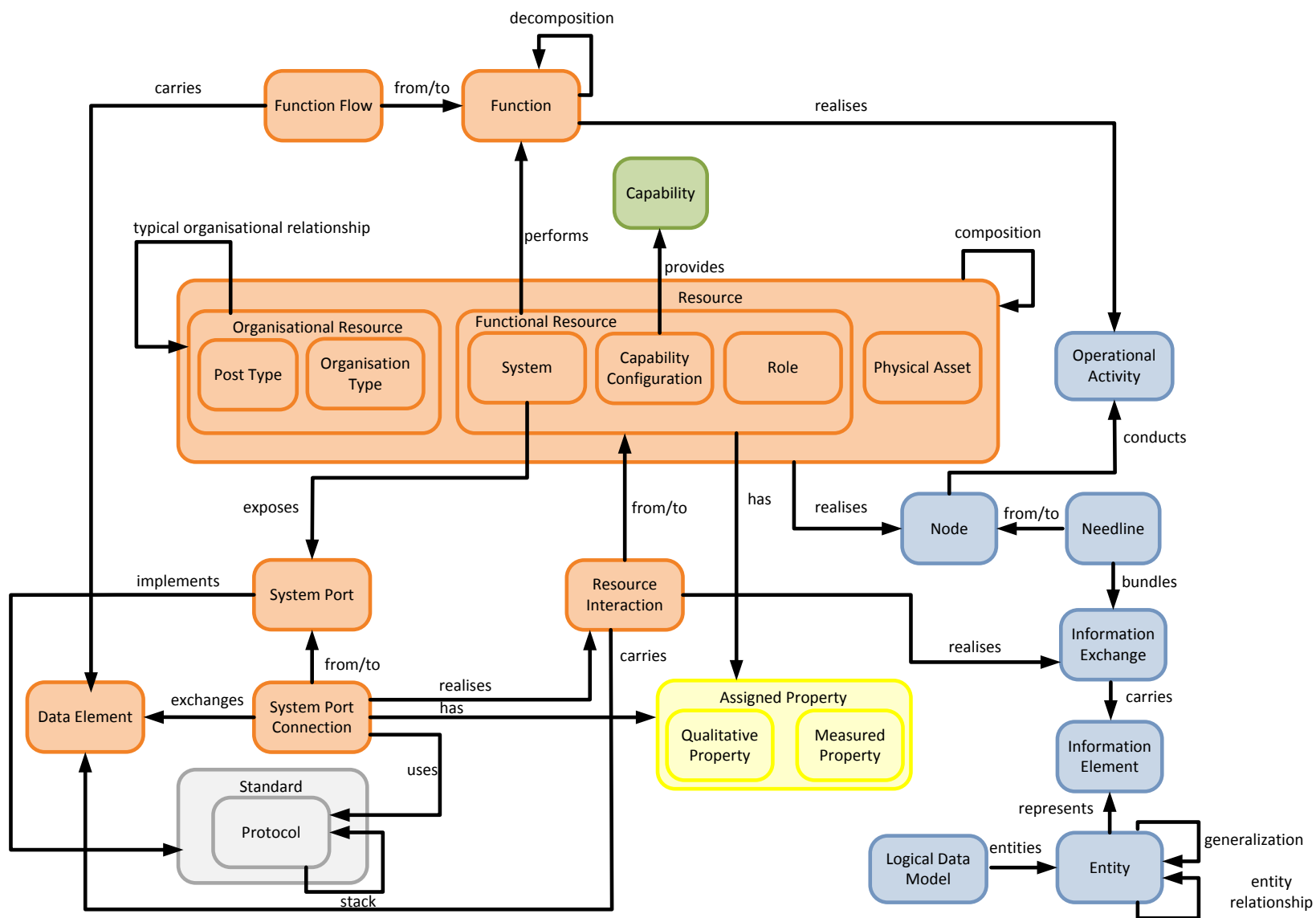


Figure 5: Model elements according to the operational, systems and technical scope

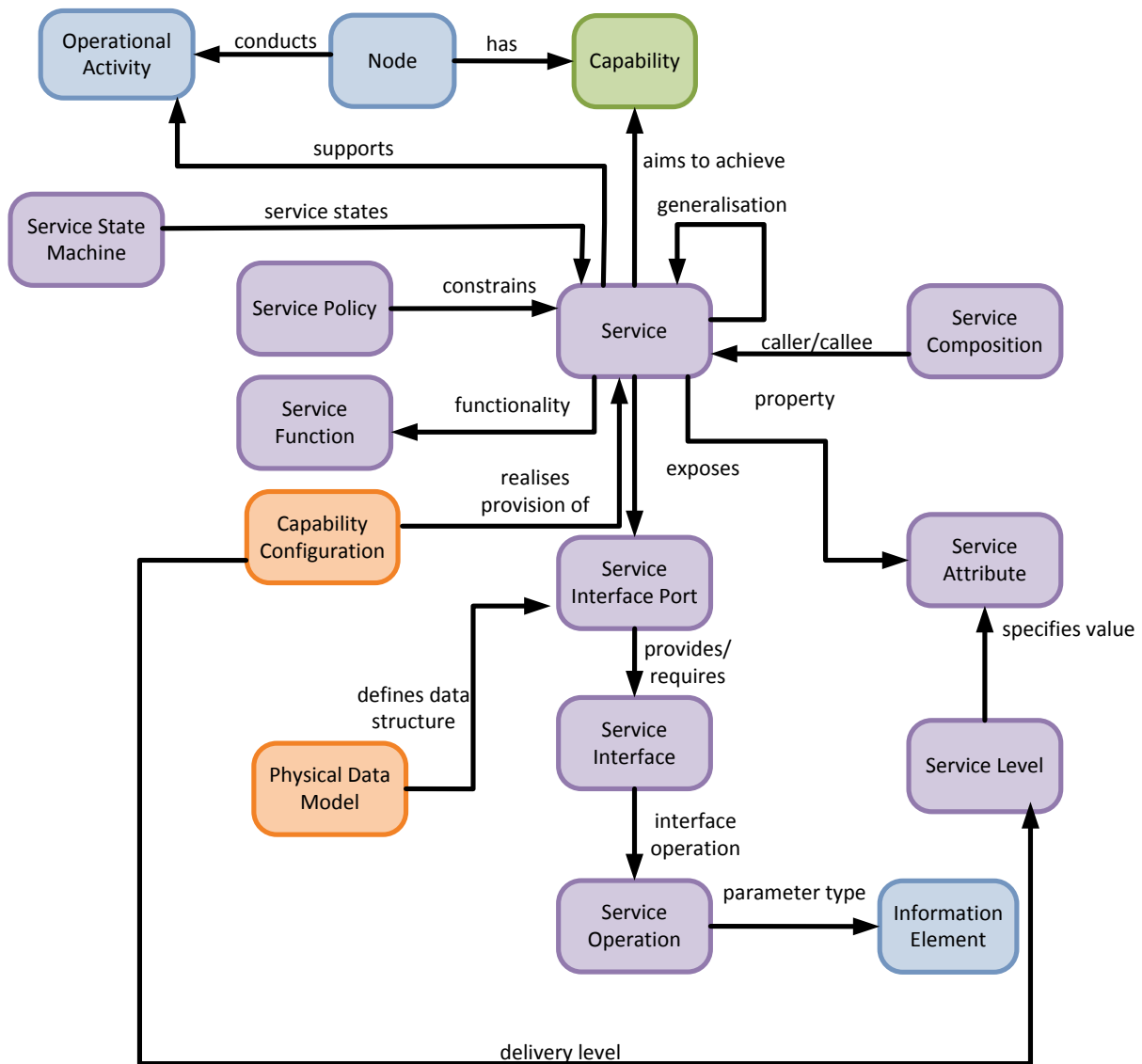


Figure 6: Model elements according to the service oriented scope

### 6.2.3.2 Views - contents and representation

According to the approach in describing OSSAF views via single or combinations of suitable NAF-views (see chapter 6.2.2 for mapping), the following chapter describes the contents of the dedicated NAF-views for use in SALUS. The description contains the model elements captured in the corresponding view (that is actually a section of the overall model presented in the previous chapter), proposes a suitable representation (i.e. graphical, textual etc.) and may give hints in order to support the development of the view under consideration. This is done in a way agnostic to any tool, but refers to Unified Modelling Language (UML) modelling concepts where suitable.

#### NAV-1 Overview & Summary Information

Type of Representation: Report, textual

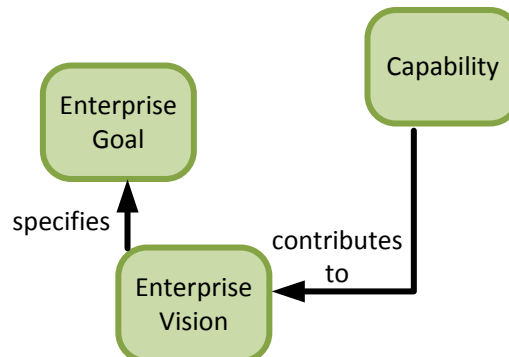
Template:

1. Introduction
2. Architecture Purpose and Objectives
  - 2.1 Motivation
  - 2.2 Problem Domain
  - 2.3 Topics of Consideration
  - 2.4 Architecture Classification
  - 2.5 Stakeholders
3. Architecture Scope
  - 3.1 In Scope – Out of Scope
  - 3.2 Tailoring of Perspectives, Views and Products
4. Conditions and Context
  - 4.1 Conventions
  - 4.2 Naming Conventions
  - 4.3 Tools
5. Findings

### NCV-1, Capability Vision

Type of Representation: graphical, based on UML Class Diagram, textual description

Model elements to be considered:



Hint: There may arise some confusion on capabilities in relationship to requirements.

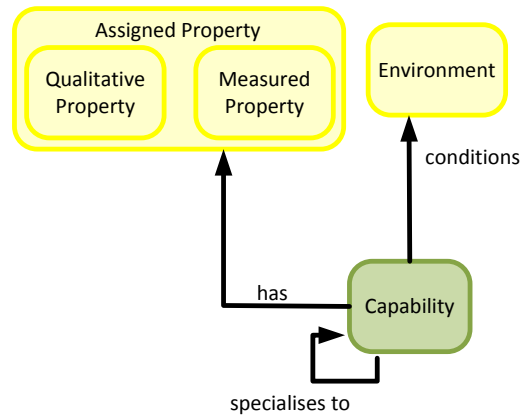
**A capability must be understood as “an ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology to achieve. For example, marketing, customer contact, or outbound telemarketing.”** [7]. This is the TOGAF definition of capability, but this definition also fits into the NAF definition of a capability which states: **“a high level specification of the enterprise’s ability”** [14] .

In contrast **a requirement must be understood as “a singular documented physical and functional need that a particular design that identifies a necessary attribute, characteristic, or quality of a system for it to have value and utility to a customer, organisation, internal user, or other stakeholder”** [15].

## NCV-2, Capability Taxonomy

Type of Representation: graphical, based on UML Class Diagram, textual annotations.

Model elements to be considered:

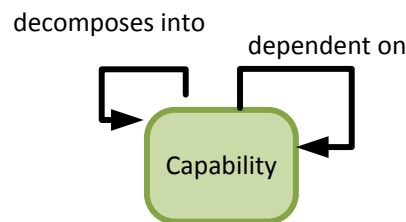


Hint: In order to express under which environmental conditions an assigned property is valid, both concepts (Assigned Property, Environment) have to be instantiated and attached to a dedicated capability.

## NCV-4, Capability Dependencies

Type of Representation: graphical, based on UML Class Diagram

Model elements to be considered:



## NCV-5, Capability to Organisational Deployment

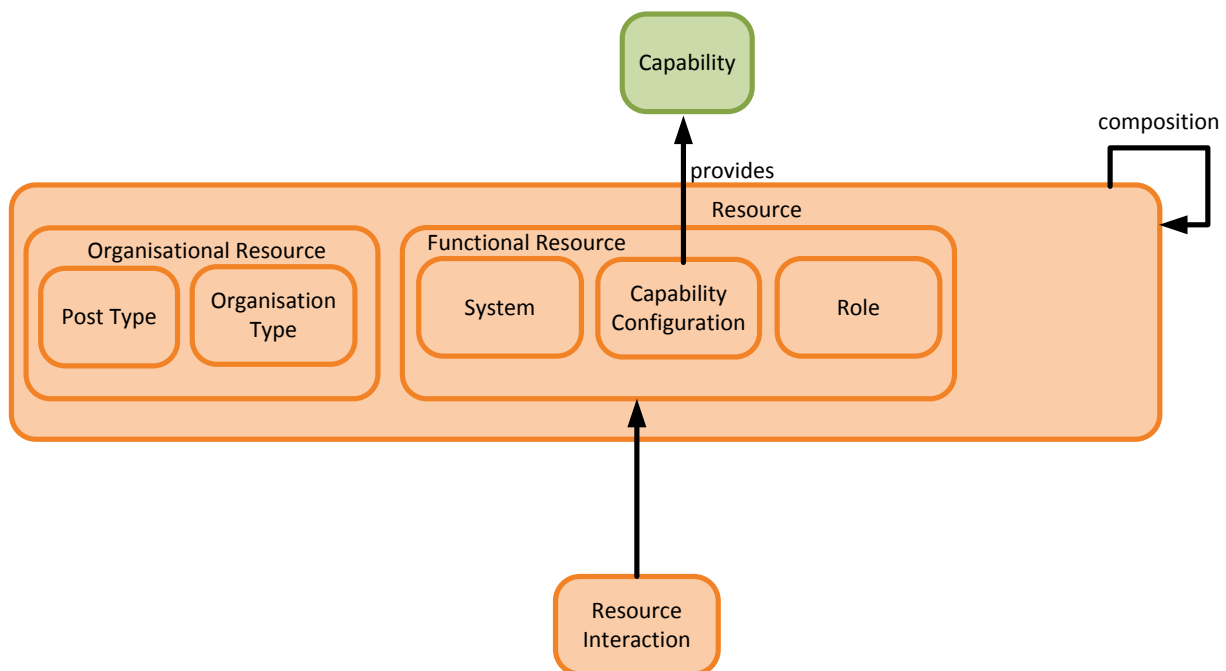
Type of Representation: Provision Matrix (or graphical via UML Class diagram, stereotyped accordingly).

Template:

| Time Frame<br>Start:{ISO8601 Date Time}<br>End:{ISO8601 Date Tim } | {Capability 1}                                    | {Capability 2}                                         | {Capability n}                                    |
|--------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------|---------------------------------------------------|
| {Organisational Structure 1}                                       | {Resource Composition},<br>{Resource Interaction} |                                                        | {Resource Composition},<br>{Resource Interaction} |
| {Organisational Structure 2}                                       | ↑                                                 |                                                        |                                                   |
| {Organisational Structure n}                                       |                                                   | ↑<br>{Resource Composition},<br>{Resource Interaction} | ↑                                                 |

The arrows in the matrix cells indicate the direction of reading. That means an Organisational Structure provides a Capability.

Model elements to be considered:



Hint: This view aims to depict the deployment relationship of organisational elements and systems (resources) and the ability they have to satisfy organisational capabilities for a particular timeframe.

Hint: Several NCV-5 view instances are created to represent the timeframes that are being analyzed if necessary.

Hint: The organizational structures are defined in NOV-4, Organisational Relationship Chart (see NOV-4 description for details). In order to express more than the provision-relationship in this matrix, functional resources (predominantly systems) or compositions of functional resources (predominantly system-of-system compositions) may be added to the corresponding matrix cells. Sources of the functional resources or its compositions are mainly the NSV-1, System Interface Description artefact (see NSV-1, System Interface Description for more details) describing, amongst others, these resources or its compositions.

## NCV-6, Capability to Operational Activities Mapping

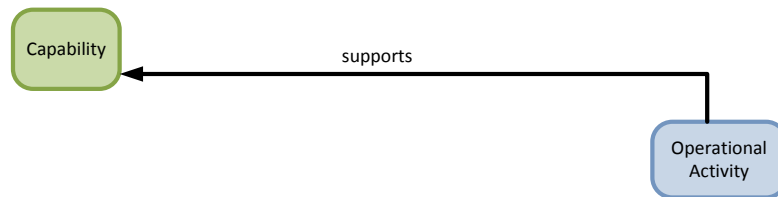
Type of Representation: Dependency Matrix

Template:

|                        | {Capability} | {Capability} | {Capability} |
|------------------------|--------------|--------------|--------------|
| {Operational Activity} | ↓            |              | ↓            |
| {Operational Activity} |              | ↓            |              |
| {Operational Activity} | ↓            |              |              |

The arrows in the matrix cells indicate the direction of reading. That means a Capability depends on an Operational Activity.

Model elements to be considered:

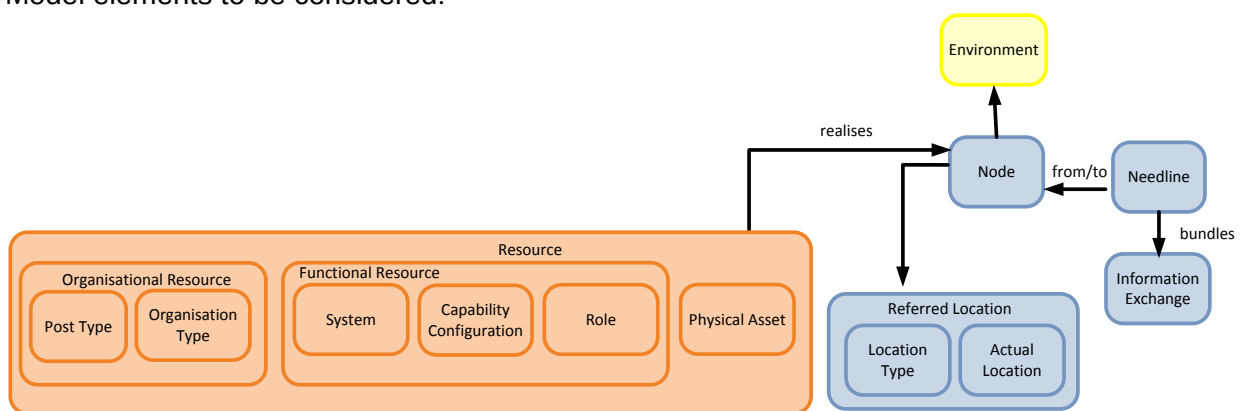


Hint: A Capability can be supported by multiple Operational Activities.

### NOV-1, High-Level Operational Concept Description

Type of Representation: Free Form diagram which is based on the UML Class diagram, optionally enriched with graphical elements (for example describing locations environment more demonstrative) or textual descriptions.

Model elements to be considered:

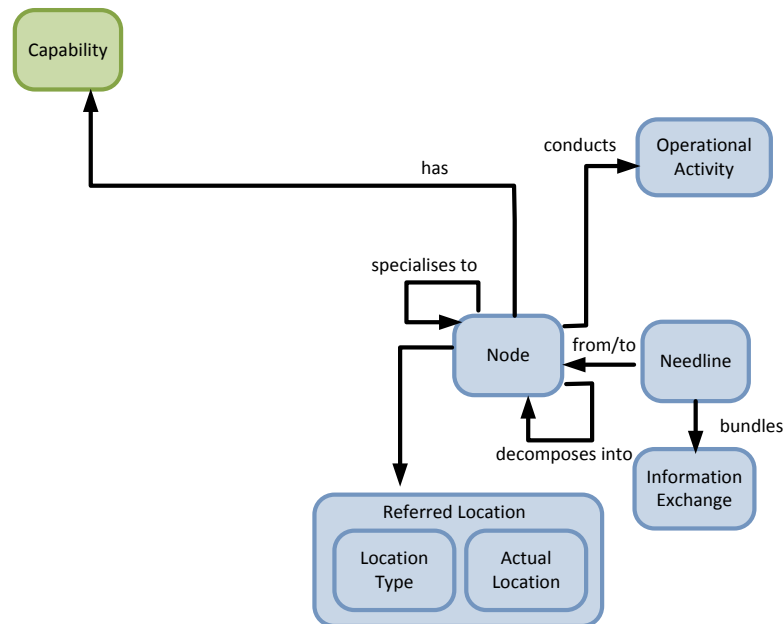


Hint: According to the diagrams intention, not all of these model elements have to be represented in the diagram. All model elements that can be used in principle are shown.

### NOV-2, Operational Node Connectivity Description

Type of Representation: diagram which is based on the UML Composite Structure diagram enriched with textual annotations to needlines in order to describe non-information flows (see Hints)

Model elements to be considered:



Hint: Node and Needline are recommended, the other elements are optional.

Hint: Depending on the complexity there may exist several instances of a NOV-2 diagram/table, for example in order to represent nodes with different levels of abstraction (specialisations).

Hint: Exchanges can be annotated (textual) in order to show flows of materiel, energy, or people between nodes as these exchanges are not needlines and therefore do not appear in an NOV-3 view.

Hint: A single Needline represents one-to-many information exchanges (information elements and their attributes – see NOV-3 for details).

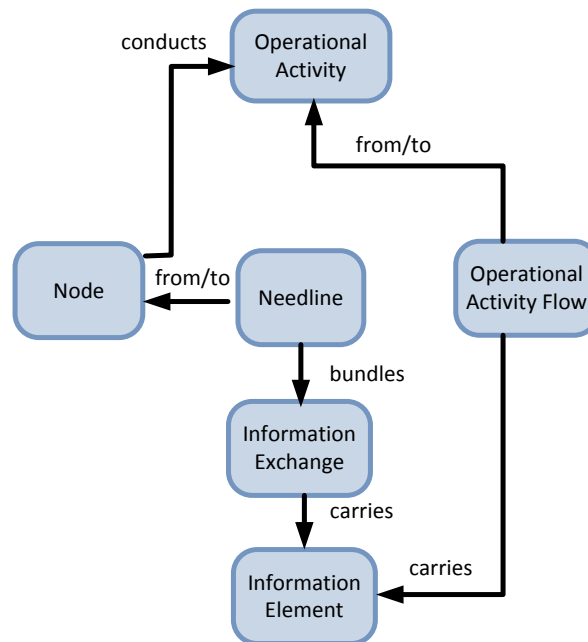
### NOV-3, Operational Information Requirements

Type of Representation: Table

Template:

| Description of Information | Sending Node | Receiving Node | Producing Operational Activity | Consuming Operational Activity | Required Information Exchange Attributes |                                                |                               |                                                     |
|----------------------------|--------------|----------------|--------------------------------|--------------------------------|------------------------------------------|------------------------------------------------|-------------------------------|-----------------------------------------------------|
|                            |              |                |                                |                                | Media (text, video, voice, data etc.)    | Quality (frequency, timelines, security, etc.) | Quantity (volume, speed etc.) | Abilities (communication, processing, display etc.) |
| {Information Element}      | {Node}       | {Node}         | {Operational Activity}         | {Operational Activity}         | {text}                                   | {text}                                         | {text}                        | {text}                                              |

Model elements to be considered:



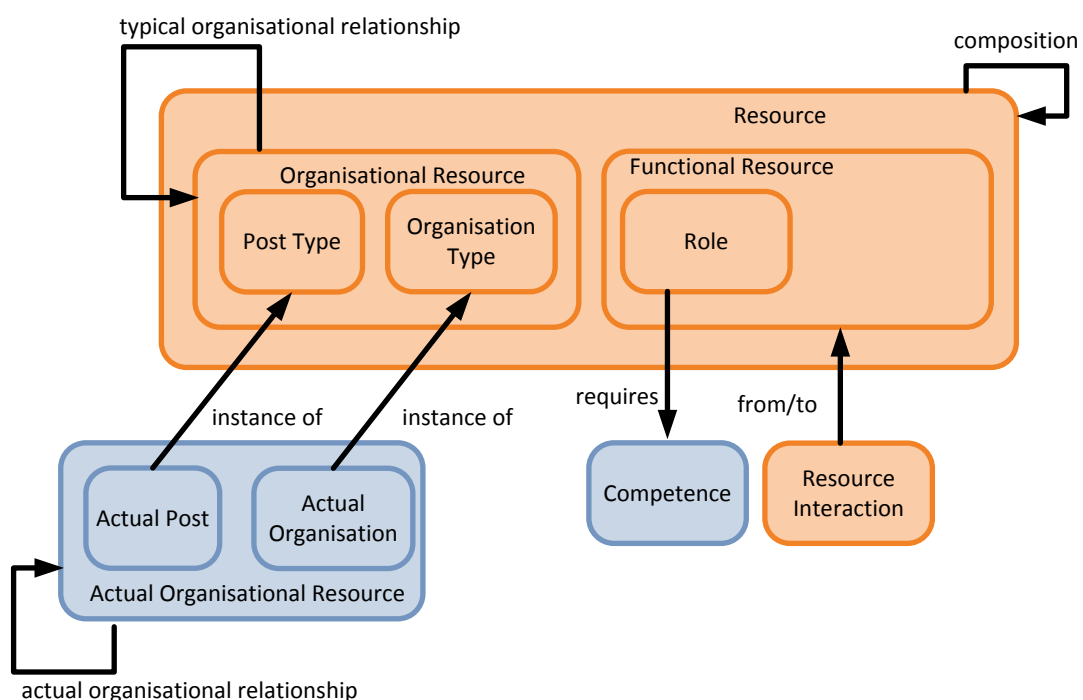
Hint: Additional information concerning Needline characteristics/attributes captured in textual form: Each Needline describes the characteristics of the data or information, i.e. its substantive content, format (voice, imagery, text and message format, etc.), throughput requirements, security or classification level, timeliness requirement, and the degree of interoperability required for the exchange.

Hint: The attributes Media and Abilities yields input in order to identify services (at technical level)

#### NOV-4, Organisational Relationship Chart

Type of Representation: Diagram which is based on the UML Composite Structure diagram

Model elements to be considered:



Hint: Instances of *typical/actual organisational relationship*-Relationships must specify the type of relationship (for example: Command and Control, hierarchical, reporting, collaboration etc.) via a dedicated attribute *organisationalRelationshipType*.

Hint: In NOV-4, allowable Resource compositions are:  
 OrganisationType to PostType - i.e. a post in an organisation  
 OrganisationType to Role - i.e. a role in an organisation  
 OrganisationType to OrganizationType - i.e. a sub-organisation

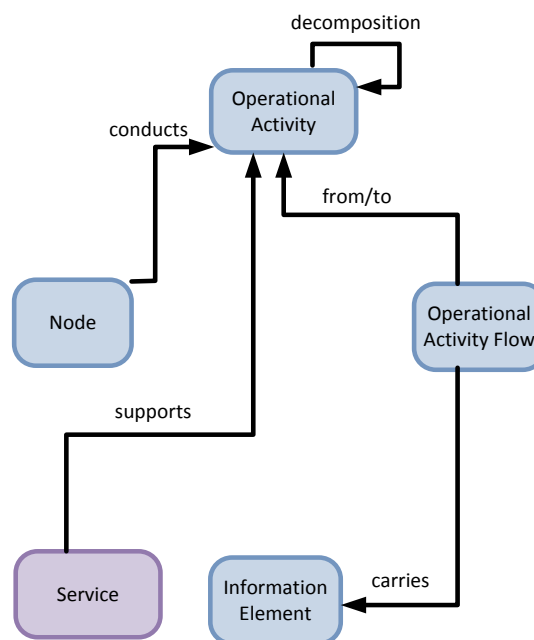
Hint: NOV-4 product particularly identifies the key players.

Hint: Organisational Relationships can be modelled both as generic organisational relationships and as actual organisational relationship. In principal there can be several instances of these products.

### NOV-5, Operational Activity Chart

Type of Representation: Diagram based on the UML Class diagram for Operational Activity compositions (functional decompositions) and UML Activity diagram for Operational Activity flows.

Model elements to be considered:



Hint: NOV-5 focuses on operational activities (in contrast to NOV-2 -> operational Nodes), Nodes can be shown as swim-lanes (Activity diagram) or notes (Nodes or Operational Rules) for composition diagrams.

Hint: One can describe the explicit sequencing of activities in response to external and internal events using the activity diagram representations.

### NOV-6a, Operational Rules Model

Type of Representation: Table

Template:

| Rule No. | Applies to Operational Activity or Node | Rule Specification | Rule Type |
|----------|-----------------------------------------|--------------------|-----------|
| {#}      | {Node}<br>{Operational Activity}        | {text}             | {text}    |

Model elements to be considered (optional):



Hint: the rules outlined in NOV-6a are operational (i.e. mission-oriented) while systems-oriented rules are defined in NSV-10. They describe what the business must do, or what it cannot do.

### NOV-6b, Operational State Transition Description

Type of Representation: UML State Machine Diagram

Model elements to be considered:



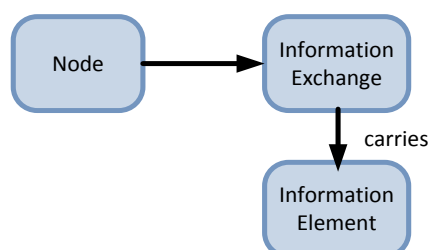
Hint: Even if not contained in the meta-model, one has to introduce an additional model element: State and State Machine respectively.

Hint: Used to describe how an operational node or activity responds to events by changing its state by reflecting the explicit sequence of actions internal to a single operational activity or by reflecting the sequence of operational activities with respect to a dedicated operational node (if not fully covered in NOV-5)

### NOV-6c, Operational Event Trace Description

Type of Representation: Diagram which is based on the UML Sequence diagram

Model elements to be considered:

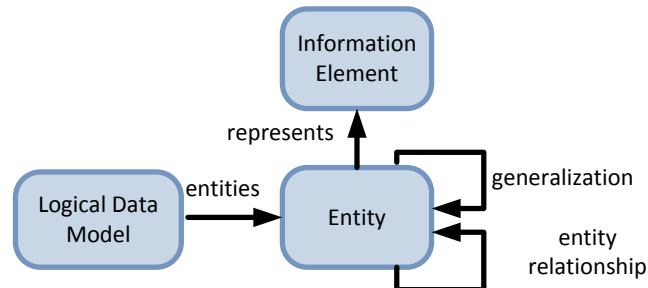


Hint: Provides a time-ordered examination of the information exchanges between participating operational nodes on a particular scenario. Different scenarios will be depicted by separate diagrams.

## NOV-7, Information Model

Type of Representation: Diagram which is based on the UML Class diagram

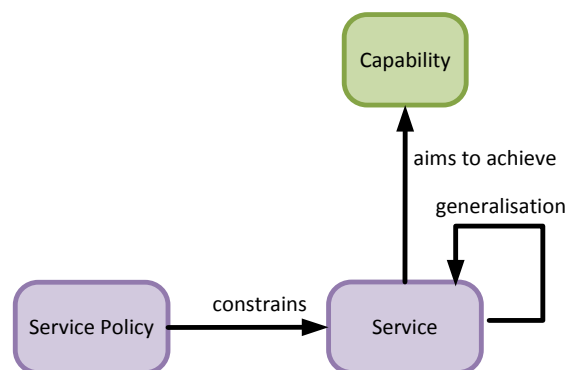
Model elements to be considered:



## NSOV-1, Service Taxonomy

Type of Representation: UML Class diagram

Model elements to be considered:



Hint: The taxonomy describes a specialisation hierarchy of services. These services have to be treated as classes of services, not as service implementations.

Hint: Services may have an additional classification into Operational-, Information- and Application-Service.

Hint: Service policies may be attached as textual annotations to a dedicated Service. They address security, commercial conditions, applicable laws, etc., under which a service is provided.

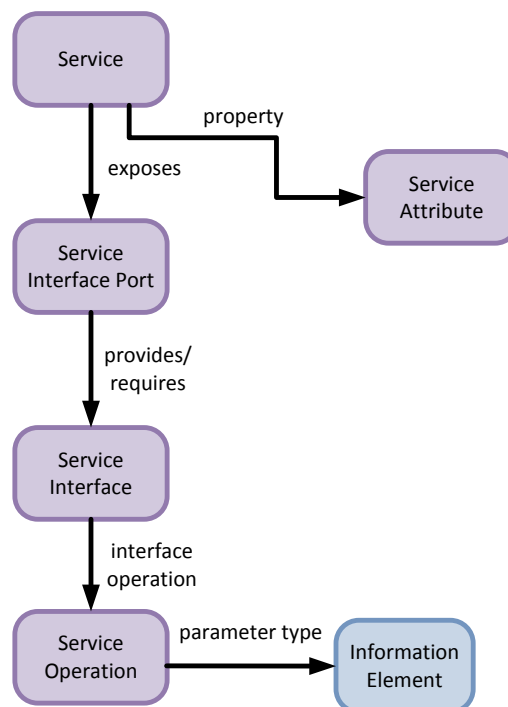
## NSOV-2, Service Definitions

Type of Representation: Table (or UML Composite diagram)

Template:

| Service   | Service Interface   | Interface Exposure     | Service Operation   | Service Operation Parameter Type | Service Attributes |
|-----------|---------------------|------------------------|---------------------|----------------------------------|--------------------|
| {Service} | {Service Interface} | {provided or required} | {Service Operation} | {Information Element}            | {text}             |

Model elements to be considered:



Hint: A service may provide/require several interfaces, an interface may provide/require several operations and operations may exchange multiple information elements.

Hint: Service attributes identify specific properties of a service that may differ from instance to instance or from implementation to implementation of a service. A special set of attributes are the Quality of Service (QoS) attributes. These contain: security, confidentiality, availability, performance, latency, reliability, integrity and maintainability.

### NSOV-3, Services to Operational Activities Mapping

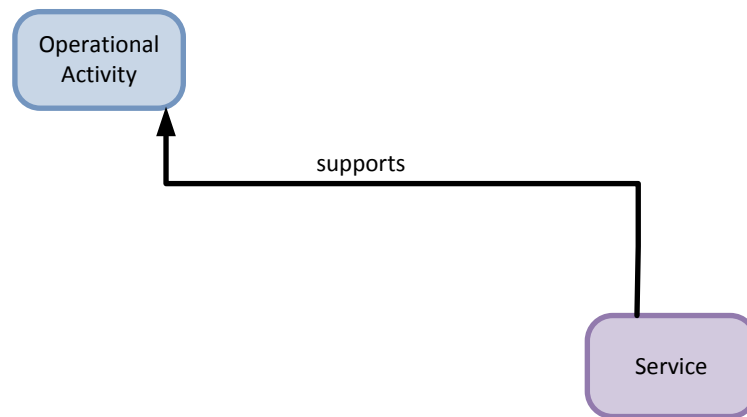
Type of Representation: Mapping Matrix

Template:

|           | {Operational Activity} | {Operational Activity} | {Operational Activity } |
|-----------|------------------------|------------------------|-------------------------|
| {Service} | ↑                      |                        | ↑                       |
| {Service} |                        | ↑                      |                         |
| {Service} | ↑                      |                        |                         |

The arrows in the matrix cells indicate the direction of reading. That means a Service maps/supports on an Operational Activity.

Model elements to be considered:

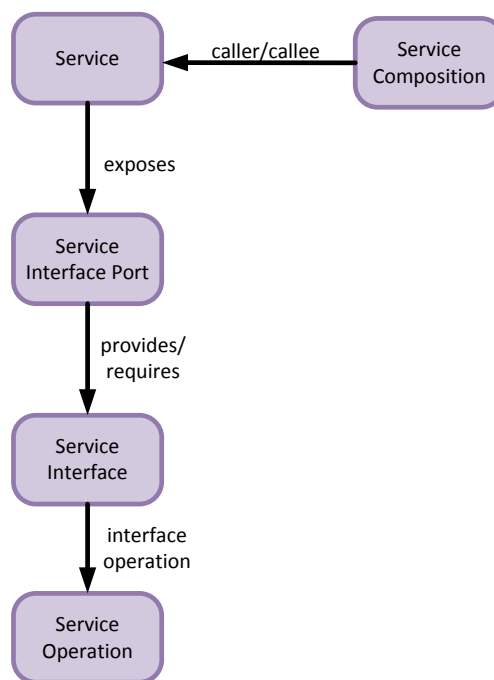


Hint: Matrix must contain all operational activities defined in NOV-5, cross linked with all services as defined in NSOV-2.

#### NSOV-4, Service Orchestration

Type of Representation: Diagram which is based on the UML Sequence diagram

Model elements to be considered:

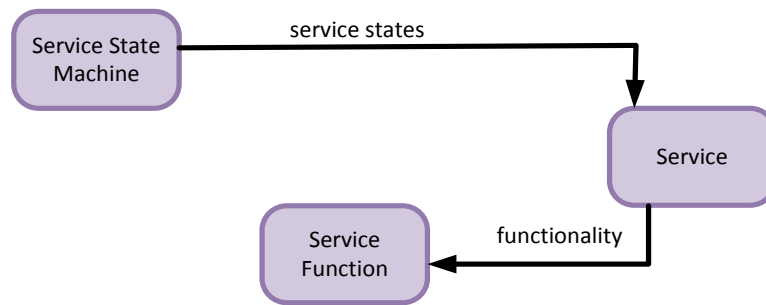


Hint: In a SOA context this view can be used to show the sequence of interactions required to support operational activities. It then shows lifelines for services and the sequence of interactions between those services.

#### NSOV-5, Service Behavior

Type of Representation: UML State Machine Diagram

Model elements to be considered:



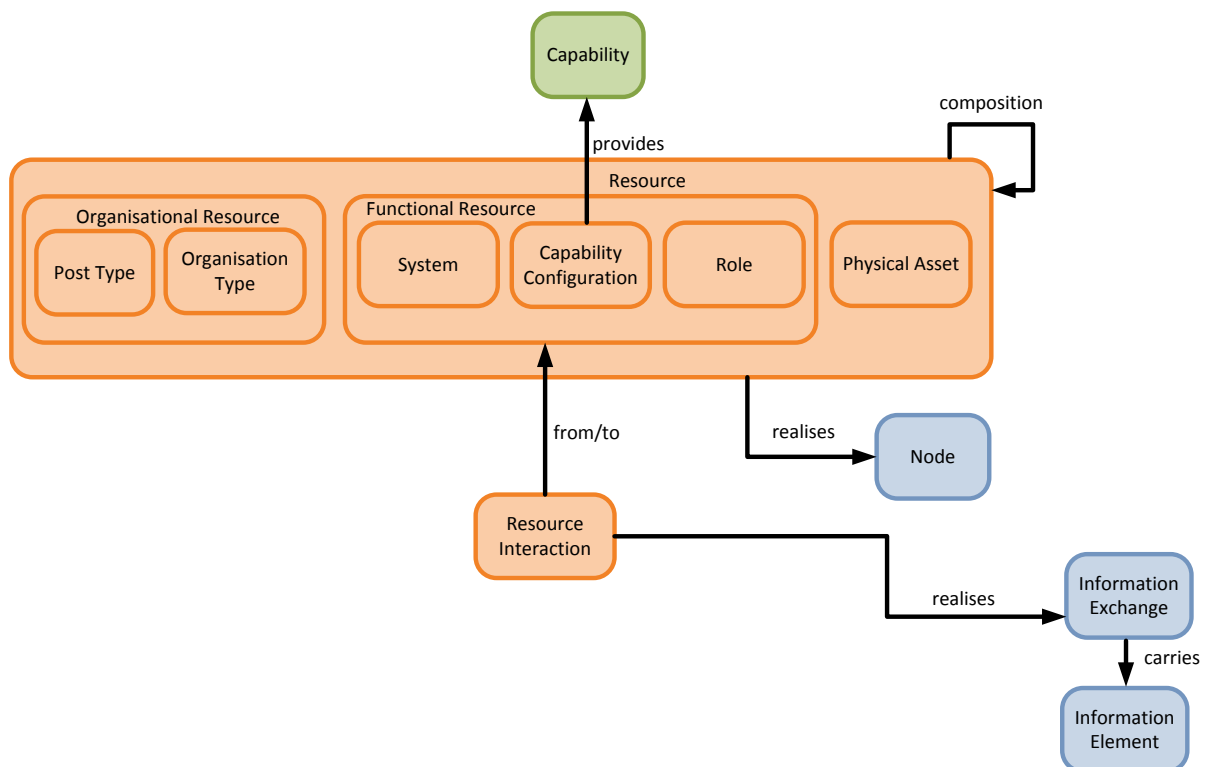
Hint: Even if not contained in the meta-model, one has to introduce an additional model element: *State*.

Hint: Used to describe the sequence of messages/operations of a service interface and to define the internal handling of the operations (possible state changes and internal function executions).

### NSV-1, System Interface Description

Type of Representation: Diagram based on the UML Composite Structure diagram

Model elements to be considered:



Hint: This view addresses the composition (whole-part relationship) and interaction of systems or resources, incorporating human elements (posts, organizations and roles) as types of performers. It describes which systems/resources interact in order to support the information and information exchange needs of the operational domain.

Hint: The purpose of the NSV-1 view is to describe the composition and interaction between resources. **Resource interactions can only be established between functional resources** and may carry information exchanges.

Hint: The following compositions are allowed:

- Physical Asset (whole) to Physical Asset (part) – e.g. a sub-platform or facility
- Physical Asset (whole) to System (part) – e.g. installation
- Physical Asset (whole) to Organisational Resource (part) – e.g. deployment of personnel to facilities or platforms
- Organisation Type (whole) to Organisational Resource (part) – e.g. a sub-organisation or post in an organisation
- Organisational Resource (whole) to System (part) – e.g. a person carrying a system
- System (whole) to System (part) – e.g. a sub-system
- Organisational Resource (whole) to Role (part) – e.g. a functional role that a post may have

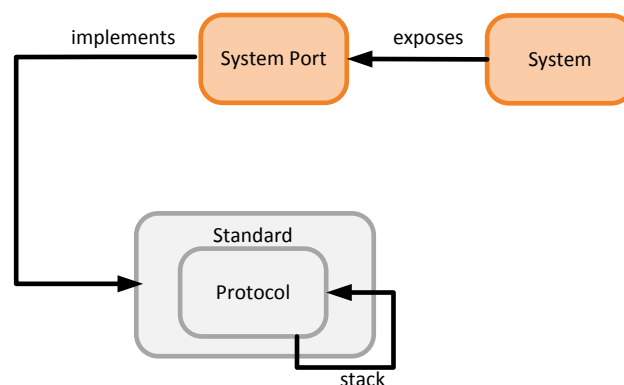
Hint: An additional concept **Capability Configuration** is introduced. It aggregates (in form of a composition) resources in order to satisfy a certain capability. As such it is a physical asset or an organizational resource “equipped” with functional resources in order to provide a certain capability. The presence of either a physical asset or an organizational resource (or both) in addition to a functional is recommended for a capability configuration. In order to describe a valid capability configuration the following composition must be satisfied:

Capability Configuration (whole) to [[Physical Asset (part)] OR [Organisational Resource (part)]] AND [Functional Resource (part)]

## NSV-2a, System Port Specification

Type of Representation: Diagram based on the UML Composite Structure diagram

Model elements to be considered:



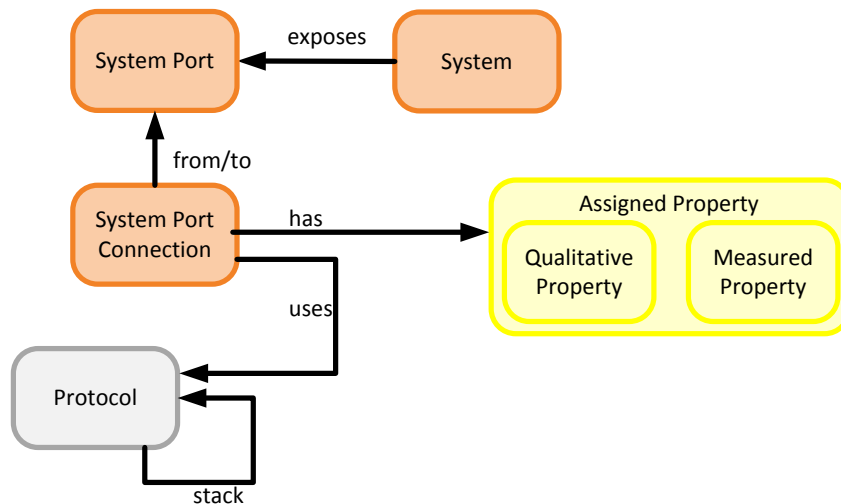
Hint: Used to describe system’s port(s) and the protocols supported by each of those ports.

Hint: A (physical) port may support more than one protocol in parallel.

## NSV-2b, System to System Port Connectivity

Type of Representation: Diagram based on the UML Composite Structure diagram

Model elements to be considered:



Hint: Specifies the physical, infrastructural nature of a connection between two systems either an existing connection or a connection that has to be established (for example during runtime).

Hint: The quality requirements applicable to the connection may also be described. This is done via a textual annotation of the connection element. This is not true for quality requirements concerning the electromagnetic (EM) spectrum. EM is addressed solely in NSV-2 (see following paragraph):

### NSV-2d, Systems Communication Quality Requirements

Type of Representation: Diagram based on the UML Composite Structure diagram (the same as in NSV-2b, System to System Port Connectivity)

Model elements to be considered: the same as in NSV-2b, System to System Port Connectivity view.

Hint: In addition to NSV-7 (offering specification of quality requirements for systems in general) and NSV-2b, this view addresses the specification of quality requirements on specific categories of quality requirements for systems communication. Actually only one category shall be recognized:

- Electromagnetic Spectrum and Bandwidth

Therefore **the NSV-2d view is essentially an electromagnetic spectrum and bandwidth description**, describing primarily those systems communicating through the radio in order to assist with spectrum analysis and management. One characteristic of the communication may be the waveform supported/required further characterized by the following parameters:

- data rate
- modulation
- coding
- figure of merit

Hint: As described in the NSV-2b, System to System Port Connectivity view, the quality requirements applicable to EM is done via a textual annotation of the connection element.

### NSV-3, Systems to Systems Matrix

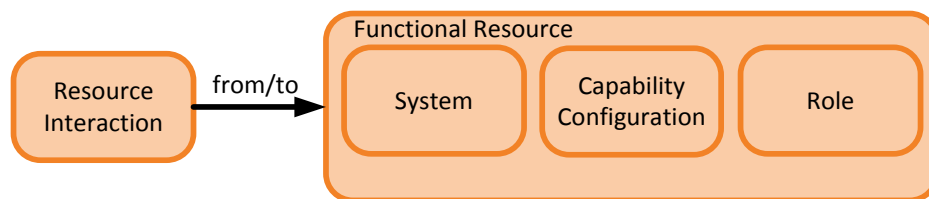
Type of Representation: Dependency Matrix

Template:

|                         | {Functional Resource 1} | {Functional Resource 2} | {Functional Resource n} |
|-------------------------|-------------------------|-------------------------|-------------------------|
| {Functional Resource 1} |                         | ↑                       |                         |
| Functional Resource 2}  | ↑                       |                         |                         |
| {Functional Resource n} | ↑                       | ↑                       |                         |

The arrows in the matrix cells indicate the direction of reading. That means a Functional Resource depends on another Functional Resource.

Model elements to be considered:

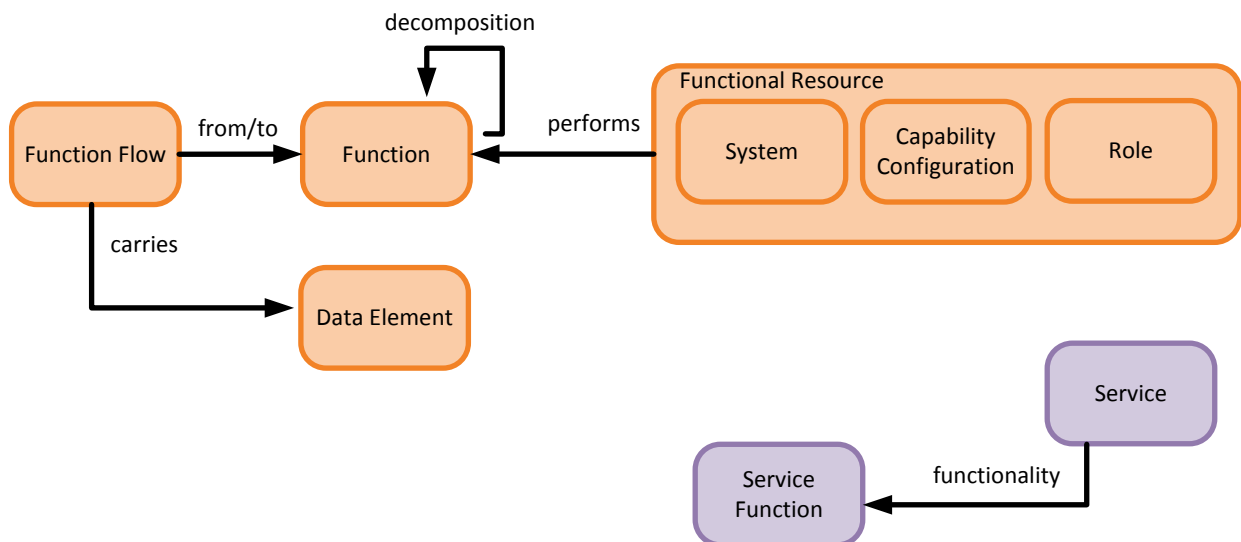


Hint: Allows a quick overview of all the resource interactions specified in one or more NSV-1 diagrams.

#### NSV-4, System Functionality Description

Type of Representation: Diagram for Function hierarchies (hierarchical composition) based on the UML Class diagram and a diagram for Function flows based on the UML Activity diagram.

Model elements to be considered:



Hint: Used to describe the functional aspects of a system (from NSV-1) in a more detailed way by their functional decomposition and behaviour that is, the data flows between system components (sub-systems) that realize certain system functions. Further, one can depict allocation of system functions to specific systems, and thus clearly outline responsibility.

Hint: When using SOA, the NSV-4 view can be used as a start for the development of the system centric views by relating system-level service functions from the NSOV-5 Service Behaviour view to system functions in NSV-4.

### NSV-5 Systems Function to Operational Activity Traceability Matrix

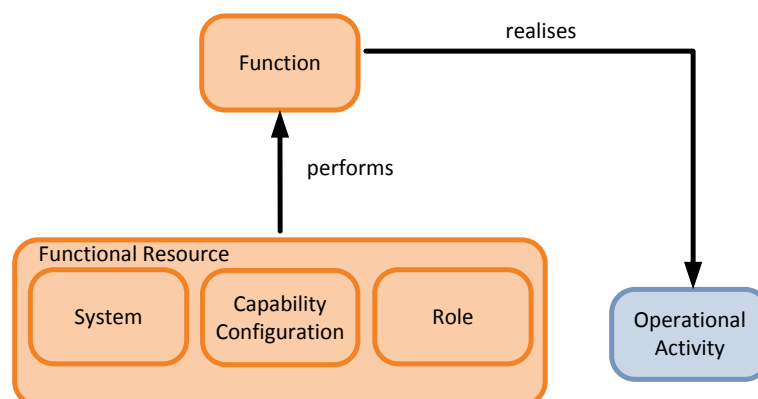
Type of Representation: Traceability Matrix

Template:

|              | {Operational Activity 1} | {Operational Activity 2} | {Operational Activity n} |
|--------------|--------------------------|--------------------------|--------------------------|
| {Function 1} | ↑                        |                          | ↑                        |
| {Function 2} | ↑                        |                          |                          |
| {Function n} |                          | ↑                        |                          |

The arrows in the matrix cells indicate the direction of reading. That means a Function somehow supports an Operational Activity.

Model elements to be considered:



Hint: This view interlinks the functions described in an NSV-4 view and the operational activities specified in an NOV-5 view.

Hint: Optionally the functional resources providing those functions to the operational activities may also be represented describing how an operational need may be transformed into an action performed by a system or solution. In order to do that, the matrix representation has to be extended by an additional column to the left containing the resources. The functions have to be rearranged according to the resource providing them.

### NSV-6, Systems Data Exchange Matrix

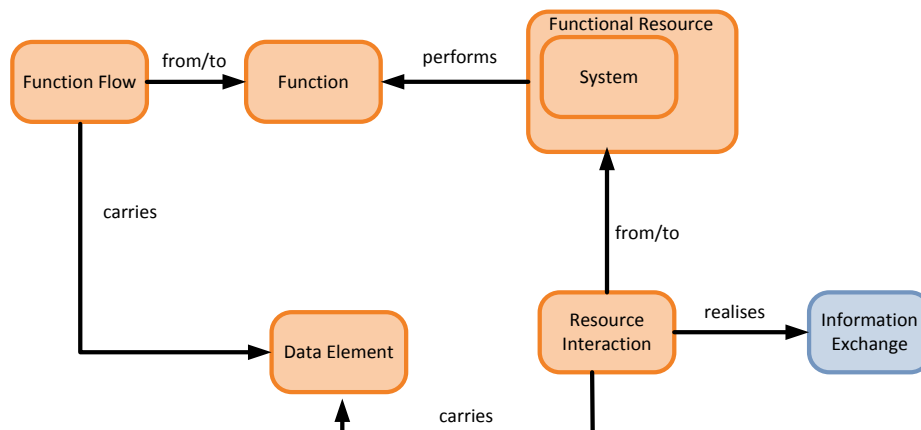
Type of Representation: Table (the table is similar to that in NOV-3 Operational Information Requirements)

Template:

| Descripti<br>on of<br>Informati | Sending<br>System | Receiving<br>System | Producing<br>Function | Consuming<br>Function | Data Element<br>Attributes | Required Data<br>Exchange<br>Attributes |
|---------------------------------|-------------------|---------------------|-----------------------|-----------------------|----------------------------|-----------------------------------------|
|---------------------------------|-------------------|---------------------|-----------------------|-----------------------|----------------------------|-----------------------------------------|

|                       |          |          |            |            |                                                                                               |                                                                                            |
|-----------------------|----------|----------|------------|------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| on (from NOV-3        |          |          |            |            | system data element, format, media type, accuracy, units of measurement, system data standard | periodicity, timeliness, throughput, size, information assurance, security characteristics |
| {Information Element] | {System} | {System} | {Function} | {Function} | {text}                                                                                        | {text}                                                                                     |

Model elements to be considered:



Hint: This view specifies data exchanges between systems according to automated information exchanges from NOV-3. Non automated information exchanges, such as verbal orders, are only described in the operational views.

Hint: The performance attributes for the operational information exchanges may be replaced by the actual system data exchange performance attributes for the automated portion(s) of the information exchange.

## NSV-7, System Quality Requirements Description

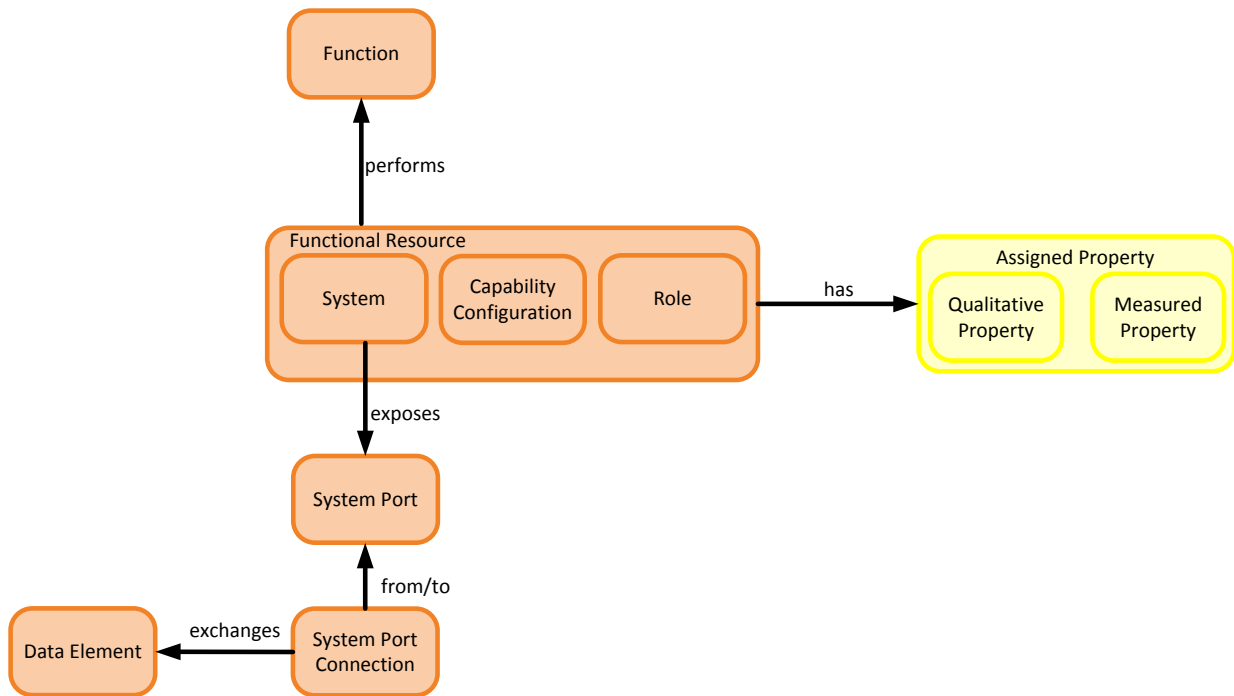
Type of Representation: Table

The columns of the table represent the dedicated quality categories (properties) (see Hints) captured and a refined description of the category concerning the containment of values, ranges of values, concrete values, estimated values, or soft values. The rows represent the dedicated items under consideration (e.g. functional resources, functions etc.).

Example table:

| Functional Resource/Function/Connection | Requirements description | Quality Category |        |        |
|-----------------------------------------|--------------------------|------------------|--------|--------|
|                                         |                          | Measure          | Metric | Value  |
|                                         | {text}                   | {text}           | {text} | {text} |

Model elements to be considered:



Hint: This view may describe the required quality characteristics of systems, their functions, communication links implementing the interface(s) and the data inherent to these links as well as their hardware. It is obvious that not all of the mentioned items have to be represented in this view. It's up to the architect's i to decide which of the mentioned items (functions, systems ...) are being part of the dedicated view instantiation.

Hint: **Quality requirements are categorized** and the corresponding categories/properties (e.g. latency, timeliness, throughput, availability, reliability, confidentiality, integrity, frequency, periodicity, format, volume etc.) are selected by the architect in conjunction with the end user community.

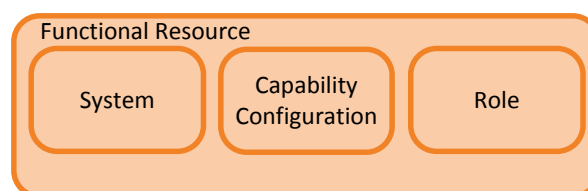
### NSV-10a, Systems Rule Model

Type of Representation: Table

Template:

| Rule No. | Applies to Functional Resource | Rule Specification | Rule Type |
|----------|--------------------------------|--------------------|-----------|
| {#}      | {Functional Resource}          | {text}             | {text}    |

Model elements to be considered:



### NSV-12, Service Provision

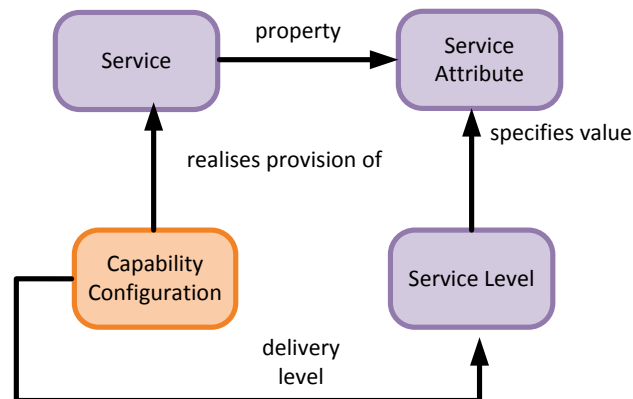
Type of Representation: Provision Matrix

Template:

|                              | {Service 1} | {Service 2} | {Service n} |
|------------------------------|-------------|-------------|-------------|
| {Capability Configuration 1} | ↑           |             |             |
| {Capability Configuration 2} |             | ↑           |             |
| {Capability Configuration n} |             | ↑           | ↑           |

The arrows in the matrix cells indicate the direction of reading. That means a Capability Configuration is a combination of resources that provide a Service.

Model elements to be considered:



Hint: A dedicated capability configuration may provide/implement several services; one service may be provided by several capability configurations.

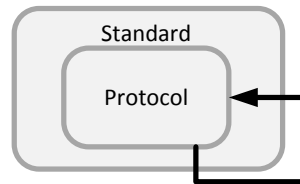
Hint: In addition, it is possible to specify to which service level the dedicated capability configuration supports specific service properties/attributes. The corresponding matrix cell has to be further extended to capture these items.

### NTV-1, Technical Standards Profile

Type of Representation: Table

| Standard No. | Applies to Functional Resource or Service | Standard Specification | Constraint on how to apply the standard to the resource -> <b>guidance and policy</b> |
|--------------|-------------------------------------------|------------------------|---------------------------------------------------------------------------------------|
| {#}          | {Functional Resource, Service}            | {text}                 | {text}                                                                                |

Model elements to be considered (optional):



Hint: This view provides a list of standards guiding and constraining the implementation of systems as defined in the various system views.

### **NTV-3, Standards and Configurations**

Type of Representation: Diagram based on the UML Composite Structure diagram

Model elements to be considered:

Same as in NSV-1, with focus on Capability Configurations

Hint: Architectures must explicitly state reusable and proven configurations as standard configurations; otherwise they will not be recognized as such and therefore may not be considered for future architecture efforts.

Hint: A standard configuration of systems is best described using the method of description used in NSV-1.

## 7 CONSIDERATIONS AND FUTURE STEPS

This document provides a set of high-level system requirements that should be taken into account in the design of the future PPDR system, and the preliminary SALUS Enterprise Architecture methodology. System requirements were obtained through the analysis of the interim SALUS use cases description and their story boards (provided by WP2). As for the SALUS Enterprise Architecture methodology, core concepts, definitions and frameworks were described and a methodology to derivate the SALUS Enterprise Architecture was proposed. It is expected the provided methodology to evolve in order to reach a stable version for D3.2 (Enterprise and System Architecture – Intermediate) and that this document will be used as a basis for cross-work-package discussions.

### **Key achievements:**

#### **High-level system requirements for each SALUS use case**

- Operational and end-user requirements
- Key applications that are expected to be used to handle each SALUS use case
- Main actors involved
- Needed capabilities
- Information flows
- Story board (in partnership with WP2)

#### **Enterprise Architecture methodology**

- Common understanding of Enterprise Architecture (EA) in the context of SALUS
- SALUS Enterprise Architecture common vocabulary
- SALUS initial Enterprise Architecture model

## 8 ANNEX 1 – CITY SECURITY STORYBOARD

### 8.1 Abstract

The City Security use case is based on the City Security scenario, which considers the management of a public disorder event with permanently deployed PPDR infrastructure in a city location. The development of this use case builds on the secure communications needs for voice, video and data applications-services capabilities used by Police, Fire and Ambulance during normal day to day activities, typically supported today by a combination of their current PMR solution (TETRA or TETRAPOL) and commercial network technologies (2G/3G/LTE).

This use case identifies the services used and the technologies and suppliers that the PPDR end users are reliant upon, and how the availability of these services is impacted upon by a significant security Incident in the city. These services will include remote controlled closed-circuit television (CCTV), aerial surveillance from a helicopter or fixed wing, automatic vehicle and personnel location, finger print scanning, and database searching for example.

This use case addresses the interoperability with state-of-the-art technologies (e.g. LTE, long range Wi-Fi ad-hoc networks, body area networks (BAN), and private mobile radio (PMR) broadband) in order to provide novel operational capabilities, and how these address the shortfall in necessary mission critical services as a consequence of the security incident. In defining the restoration of services, this use case will identify the security, interoperability, system integration and quality of service requirements as the Incident develops and evolves. This will provide a baseline for the candidate technologies and actors to be validated in Task 7.2.

### 8.2 Use case description

Trigger: Government's continued austerity drive increasingly impacting on people's lives

- High unemployment, high inflation, reduced wage packets, reduced social benefits, reduced central/local government support.
- Social media communications escalates as a result of a new government money saving initiative.
- Police aware as a result of social media scanning of planned demonstration and resources deployed accordingly.
- Originally a peaceful protest.
- Police crowd control tactics aggravate the crowd and protest escalates into violence.
- Public dislike to government response therefore protests organised for subsequent days and nights.
- Criminal elements join in with looting and arson being increasingly prevalent.
- Police increase their resources to help combat the existing violence.
- Protesters become increasingly better organised through the use of social media, ring leaders emerged and started to co-ordinate some of the rioting activity.
- Many casualties and fire damage to properties.
- Certain areas become no-go areas for emergency services.
- Innocent members of the public impacted, frightened to leave their homes.
- There will be several governmental and first responder organisations in action. Some will use some central control room structure (maybe a joint one), others an additional mobile command post. Efficient wireless communications between those command structures is

key for success, cross-agency communication an important aspect in dealing with the incident(s).

### 8.3 Expected users (use case actors)

In the City Security use case, the following users have been identified:

Table 13 - List of users for the City Security use case

|                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ Police (Gendarmerie) <ul style="list-style-type: none"> <li>○ Overt</li> <li>○ Covert</li> <li>○ Mutual aide/out of area forces</li> </ul> </li> <li>▪ Ambulance services, including volunteer organizations as red cross</li> <li>▪ Fire Brigades</li> </ul> | <ul style="list-style-type: none"> <li>▪ Security Services (covert)</li> <li>▪ Transport</li> <li>▪ CCTV operators</li> <li>▪ Traffic management</li> <li>▪ Mayor's office in the City Hall,</li> <li>▪ Defence, civil defence</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 8.4 Story board

#### 8.4.1 Precondition

- The protest starts off very peacefully.
- The protesters have notified the police of their intent as a courtesy as they have previously done.
- No trouble is expected as the same protest has taken place a number of times in the past with no incident. Therefore there is no need for police presence above BAU
- The use case takes place in a country where public CCTV is accepted and used by public organisations such as the police and local councils.
- Strategic command not required for initial protest.
- In order to accommodate public safety communications and control the following facilities are in place:
  - PPDR specific TETRA network, to be used by operational forces of police, ambulance services, fire brigades.
  - LTE network with reserved capacity for PPDR services. The system also caters public and other professional users.
    - 10 MHz of spectrum is reserved for PPDR only.
    - 10 MHz of additional spectrum is available for PPDR on demand.
  - Control room facilities. However the room is initially staffed for BAU and therefore not staffed by commanders of police, fire brigade, ambulances.
  - PPDR communication facilities that allow role based access to information.

#### 8.4.2 Flow of events

1. A small well planned (including the deployment of marshals) peaceful protest held, organised by a small group protesting against the latest set of government austerity measures. The route goes through popular shopping areas terminating at government buildings in the city centre.
2. Authorities had prior warning of the protest. Intelligence sources did not anticipate any trouble and that the number of protesters attending would be small. Consequently, a small police team of 8 officers is deployed to maintain peace and ensure city centre access and security is maintained. The control room continuously tracks the location of

- the officers deployed via their GPS enabled handsets. Location updates are sent every 30s [person location].
3. 200 protesters attend
  4. Mid route, a group of 20 noisy youths appear and start to argue with the peaceful protesters.
    - Despite a small altercation between one of the youths and a protester which involved a punch being thrown, the 8 officers quickly calm the situation deciding not to make any arrests.
    - The youths disperse. The officers feel the situation is under control and so additional support is not called for.
  5. Out of sight of the police and the protesters, one of the angry youths texts and tweets message to his friends.
    - The text message is telling them to come to the protest for some 'fun'.
    - Some friends in a nearby pub have been drinking all day and they notify their friends who may be in the vicinity to come and join in for some 'fun' encouraging them to also invite their friends to the 'party'.
  6. Within 10 minutes some 40 youths have gathered and start heckling the protesters.
  7. Another one of the angry youths lunges at the protesters
    - 2 of the police officers intervene and restrain him.
    - This angers the other youths as the officers refuse to release their friend.
    - A group call is made requesting transport for [group voice calling] the youth restrained who has now been arrested.
  8. One of the police officers has become separated from his colleagues. The youths become aware of this and start to surround the officer. The officer sensing the potential danger of the developing situation presses his emergency button to summon assistance. The EM function automatically enables Video from the officers phone to be transmitted back to control. The bandwidth requirements of other users operating on the same radio cell are reduced to ensure the video has the radio resources needed [emergency button with voice and video plus pre-empt and network prioritisation].
  9. More youths start to arrive and the police notice some of them are starting to arm themselves with anything that they can readily lay their hands on including stones, bottles and glasses taken from the pub.
  10. Realising that the youths were not going to calm down a police officer calls the control for more resources [group voice calling].
    - A group call to the control room is made requesting more resources [group voice calling]
    - Using location tools the police control can see that there are response officers nearby [person and vehicle location] that can immediately assist and dispatches them to the scene to assist.
    - These additional officers switch to the talk-group being used to manage the incident. A call is already in progress and their radios quickly attach and start receiving the communication [late entry into group call].
  11. The presence of additional officers arriving angers the youths further
  12. More angry youths have responded to the text message.
    - Many have been in local bars and join in the trouble.
    - These youths are armed with beer bottles and other weapons
    - Some are armed with knives
    - They have mobile phones and are sending messages via text and social media

- Some are capturing the scenes on video
  - One of them throws a bottle at the police and the protesters causing some injuries
  - More youths appear from other pubs and surrounding buildings. They had received Facebook and Tweet messages and also seen footage on YouTube
  - The control call for ambulance to be dispatched
13. Some of the youths see an opportunity in the developing situation to steal high value electrical goods displayed in a shop window and smash the window.
14. The police control consider the situation to be more serious now
- There are now more than 400 youths and protesters on the street
  - They access local CCTV camera in the area [CCTV access]
  - As not all the cameras covering the area are available due to maintenance, a suitable police officer is identified from his GPS coordinates [person location] to stream back to the control room video footage [live video streaming] to supplement footage from the CCTV system.
  - They can now see the full extent of the situation
  - With direction from the control room police officers at the incident are dispatched to arrest identified individuals including the “ring leader”. Quality pictures captured from a video camera are sent to a small group of officers dispatched to arrest these individuals [group picture].
  - The arrested youths are detained in a police vehicle but in the struggle one of the youths becomes seriously hurt and is unconscious. A police officer on the ground dials 999/112 using telephony services [telephony] to call for an ambulance. The officer is requested by ambulance control to carry out some basic assessment checks/treatment to help sustain life.
  - The police use criminal intelligence databases [database access] to establish details of the offenders. They discover that they are known trouble makers
15. Teams of riot police are called in
- The police realise that the crowds are growing
  - More officers are dispatched and more rioters also appear
  - Some of the officers deployed are unfamiliar with the location and use Google Street Maps to familiarise themselves with the area [internet access]
16. A full scale riot is declared
- Youths start looting local shops and start setting fires to cars and other property
  - The fire services are called in, as are more police and ambulance resources
17. Reports received that trouble has broken out outside the police station in a neighbouring city centre police station
- It is clear that the incident is linked to the first incident
  - It is also evident that social media was used to start the second incident
  - The police monitor internet activity via the social networks [internet access]
  - The police use augmented reality to help identify areas/shops that may come under attack [augmented reality] and to help them to bring the situation under control.
  - A gold, silver, bronze command structure is established between police, fire and ambulance
  - Resources are also requested from neighbouring police forces. Their radios are remotely programmed with the appropriate talk groups being used [DGNA]

18. A small group of officers in attendance at the scene are dispatched to protect ambulance and fire officers [interoperability between different networks] attempting to affect the rescue of a person trapped in a smouldering car that was intentionally driven into the front of a locked shop displaying high value electrical items. The fire officers consult a remote database [database access] of recommended places to cut the vehicle in order to gain access.
19. Reports of more disturbances in other parts of the country. Now further afield
  - More police fire and ambulance resources are dispatched
  - Some are wearing body armour with sensors [WBAN]
  - A gang of youths burned down a local post office.
  - Use of firearms suspected. Fire arms unit are called and are instructed to switch their radios to DMO and remain in contact with the control via a gateway [DMO gateway]
  - Attacks were carried out on police cars, a double-decker bus and local businesses and homes.
  - Police vans and officers from the Territorial Support Group attended the disorder.
  - The police set up various cordons around the trouble spots
  - Shops windows were smashed and the shops looted by rioters.
  - Fireworks, petrol bombs and other missiles were thrown at police
  - Twenty-six officers are now injured, including one who sustained head injuries.
  - Fire-fighters experienced difficulty reaching a burning building because of the disorder.
20. A News correspondent said his news crew and vehicle came under attack from youths throwing missiles.
  - Some news crews left the scene due to the threat of violence.
  - Newspaper photographer was beaten and mugged.
21. The incidents last for 4 days and spread in over 15 towns and cities across the country
  - In total, police additional resources required increased to over 20,000
  - They eventually managed to regain control making several arrests
  - The ring leaders were identified using criminal intelligence databases
  - Location services were used for tracking and directing of resources [person and vehicle location]
  - CCTV footage was broadcast to several resources [video broadcast]
  - WBANs were used to identify officers down and other users in trouble [WBAN]

## 9 ANNEX 2 – TEMPORARY PROTECTION STORYBOARD

### 9.1 Abstract

The Temporary Protection use case is based on the Temporary Protection scenario which considers the management of public disorder in a sports arena with a combination of permanent and temporary PPDR infrastructure. The development of this use case will define the technologies used to provide portable secure communications needs for voice, video and data applications-services capabilities at major events. This use case defines the services that remain private to the Public Safety at the venue, such as remote controlled cameras, detection of threats (chemicals, explosives etc), criminal intelligence and patient records, whilst also addressing the need to share and interoperate with local PMR solutions where appropriate.

This use case addresses the interoperability with state-of-the-art technologies (e.g. LTE, long range Wi-Fi ad-hoc networks, BANS, and PMR broadband) and emerging technologies in order to provide novel operational capabilities that meet the security and privacy needs of the relevant event management and support. This will provide a baseline for the candidate technologies and actors to be validated in Task 7.4.

### 9.2 Use case description

This use case is based on an Olympic style and sized event featuring the following:

- Two or more days in duration.
- High profile international event.
- Many VIP dignitaries from various countries and organisations attending
- Multiple venues in close proximity.
- In addition to the event stadia, large TV screens erected at a number of public areas.
- Approximately 1 Million people daily coming and going to the events and in and around the area.
- Screening of spectators revealed potential explosives resulting in the possibility to evacuate the stadium.
- Day 1, steady state. Everything goes according to plan.
- Day 2 Intelligence received that explosives have been planted somewhere at the main venue (could be elsewhere) resulting in the need to evacuate one or all venues. The alert occurs just prior to the most popular sporting event starts. Panic breaks out.
- Authorities try to control the crowd using evacuation procedures aided by several means such as loudspeakers, geo-casting alarms to the mobile phones and making use of the large TV screens in the public areas.
- An extension to this scenario could be that in addition of the above, explosions or other attacks take place in several neighbourhoods of the city, increasing the panic even further. Authorities make use of context information for rapid detection and localization of the attack. Information from pre-installed cameras may be complemented with information from social media (using suitable filters) and sound analysis.
- Communication facilities at the location of the incidents due to the large concentration of forces may be insufficient and need to be complemented with ad-hoc networks for local data communication

### 9.3 Expected users (use case actors)

In the Temporary Protection use case, the following users have been identified:

Table 14 - List of users for the Temporary Protection use case

|                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ Police <ul style="list-style-type: none"> <li>○ Overt</li> <li>○ Covert</li> <li>○ Mutual aide/out of area forces</li> </ul> </li> <li>▪ Ambulance</li> <li>▪ Fire Brigades</li> <li>▪ Security Services (covert)</li> <li>▪ Transport</li> <li>▪ Civilian/event security</li> <li>▪ City Councils</li> </ul> | <ul style="list-style-type: none"> <li>▪ CCTV operators</li> <li>▪ Traffic management</li> <li>▪ Hospitals</li> <li>▪ Road operators</li> <li>▪ Weather institutes</li> <li>▪ Nature conservation institutes</li> <li>▪ Utilities companies (power, gas, water)</li> <li>▪ Telecom operators</li> </ul> |
| <p>Note: Fire brigades and Ambulance involvement is low until Day2 scenario occurs</p>                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                         |

### 9.4 Story board

#### 9.4.1 Precondition

- A large scale multi-day sports event is taking place, spread over a number of venues.
- The total number of daily visitors to the complete event is around 1 million.
- The storyboard event occurs at single venue, which can hold 50.000 spectators. The venue is filled before the event commences.
- Evacuation plans are predefined.
- An enhanced command and control structure is in place for the duration of the event.
- A dedicated national coordination centre (e.g. the National Olympic Coordination Centre) is established for the coordination of the multi-agency safety and security operations throughout the country for the duration of the event.
- Teams, on an operational, tactical and strategic level, are in place and continuously available.
- In order to accommodate public safety communications and control, the following facilities are in place:
  - PPDR specific TETRA network with additional capacity, to be used by operational forces of police, ambulance services, and fire brigades.
  - LTE network with reserved capacity for PPDR services. The system also caters to public and other professional users.
    - 10 MHz of spectrum is reserved for PPDR only.
    - 10 MHz of additional spectrum is available for PPDR on demand.
  - Control room facilities. The room is staffed by commanders of police, fire brigade, ambulances, and the venue security organisation.
  - PPDR communication facilities that allow role-based access to information.

#### 9.4.2 Flow of events

1. A 112-call comes in at the local dispatch room, indicating that multiple bombs are placed at a specific venue. According to the message each bomb is said to explode after 30 minutes.
  - All 112-calls are recorded. Speech recognition technology analyzes the call and identifies key words of interest, such as location, type of device, time, and the

- claiming group. A search engine searches for context related information in existing databases.
2. The call-taker informs his superior (tactical level) of the threat, by calling and referring to the recorded data.
  3. The tactical level officer informs the strategic team of the national coordination centre, including reference to the recorded data.
  4. The strategic team searches for other relevant information and evaluates the situation. The national coordination centre takes the decision to start the evacuation of the venue.
  5. The local command and control centre coordinates the evacuation procedure. The overall operation is under the management of the national coordination centre.
  6. In parallel, the bombers have communicated their bomb threat through social media. The first spectators receive information on the threat.
    - A part of the visitors get nervous and start to go to the exit.
    - This abnormal behaviour is detected by video cameras.
  7. The predefined evacuation plan is started, including the following actions:
    - Inform all tactical units that evacuation will take place, according to plan X. Units to be informed include police, ambulance services, fire brigade, event security, transport, and the road operator.
    - The city council is briefed about the current situation.
    - Telecom facilities are switched over to 'priority mode'. (Public access is limited, bandwidth consuming applications are limited.)
    - Media partners are briefed, including a set of instructions on what is expected.
  8. Operation units are instructed.
    - Operational staff at the outer checkpoints is instructed to stop people coming in. The instruction includes the message they have to give to the visitors, saying that "the next match is postponed for security reasons".
    - Gathering points are staffed.
    - Buses with visitors are directed to leave the area immediately.
    - Additional ambulances and fire trucks are directed to the venue.
    - Special (covert) forces are instructed to watch out for suspects. They have received the briefing, including descriptions of possible suspects based on the analysis of the strategic team.
    - Some additional drones are airborne, to have a better view over the terrain.
  9. The sports event is stopped. The visitors are informed that the stadium will be evacuated for security reasons.
    - To inform the visitors the following media are used: Screens in and around the venue, loudspeakers, LTE broadcast services, and social media.
  10. The first (small) bomb explodes creating limited damage.
  11. Panic breaks out. People start to rush to the exits, with continuous very loud shouting.
    - Venue security guards try to streamline the crowd, but with little success.
    - Security guards need to assist one another to streamline the crowd. They see each other's positions and activities in their head-up displays so that they can cooperate more easily.
    - Some people get injured. Security guards separate the injured. In a number of cases they apply sensors to monitor the vital signs of the injured.
    - Disabled people are tagged. The amount of assistance for these people is monitored. Where needed, security personnel are directed to assist.

12. Special Forces have identified suspects based on their behaviour. A combination of drones and fixed cameras start following these persons, and plot their position on maps. Intervention by Special Forces is delayed in order to gather more evidence and avoid halting the wrong people.
13. A second bomb explodes, blocking one of the entrances. An important evacuation route can no longer be used. The location of the explosion is filmed by numerous visitors. Videos are uploaded to social media.
  - The control room instructs a team to go the specific location to video the conditions.
  - The evacuation plan is rearranged to take care of the new situation.
  - The new plans for the evacuation are distributed to all operational teams, and partner organisations.
  - Due to the rearrangements, ad-hoc network capacity is needed at unforeseen locations.
14. The identified suspects are tracked down and taken into custody.
15. The complete venue is being search systematically for explosives. A third bomb is found and disarmed.
  - During this search the location of all personnel involved is plotted.
  - Cleaned areas are plotted on the map.
  - Progress on the operation is briefed to the strategic team, partner organisations, and media partners.

## 10 ANNEX 3 – DISASTER RECOVERY STORYBOARD

### 10.1 Abstract

The Disaster Recovery use case is based on the Disaster Recovery which considers the management of a major flooding that extends over the border of Country A and Country B. Cities in the area cannot be reached anymore over roads, and buildings are flooded by water. Due to the land sliding, the rail infrastructure became severely damaged, and as a result of this, a high speed train has derailed with 200+ citizens being severely injured.

This use case addresses the need for transportable radio solutions based on similar technologies than permanent infrastructures and capable to offer voice, high speed data and video services.

### 10.2 Use case description

This use case is based on:

- Prolonged heavy rain and heavy winds gives rise to flooding and landslides and power outages
- Flooding as a result of prolonged rain over several days causing rivers and reservoirs to fill and ground becoming waterlogged. Intensity of rain increases causing floods.
- High speed train derailed due to rail damage caused by land slide (Despite rail-checks on a daily basis to avoid derailling because of stolen tracks, stolen copper wiring, etc.). 200+ citizens are being severely injured.
- If energy fails, water level monitoring at upstream dams (embankments) is not reported. This issue may cause further flooding unawareness.
- Setting – low lying (valley) sub-urban totally surrounded by rural area, possibly across geographical boundaries, country or PPDR regional boundaries
- Population assumed to be between 50,000 to 300,000. The maximum impact depends on the considered country but the response needs to be scalable.
- Loss of communications – first public communications, then PPDR communications as PPDR communications resilience is stretched beyond design limits
- Transport access to sites difficult due to flooding, therefore ability to refuel generators lost resulting in PPDR networks going down.

### 10.3 Expected users (use case actors)

In the Disaster Recovery use case, the following users have been identified:

Table 15 - List of users for the Disaster Recovery use case

|                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>▪ Police (High involvement)</li> <li>▪ Overt</li> <li>▪ Mutual aide/out of area forces</li> <li>▪ Ambulance (High involvement)</li> <li>▪ Fire (High involvement)</li> <li>▪ Transport</li> <li>▪ Military</li> <li>▪ Environment agency,</li> <li>▪ Volunteer mountain rescue type units or</li> </ul> | <ul style="list-style-type: none"> <li>▪ CCTV operators</li> <li>▪ Traffic management</li> <li>▪ NGO/Volunteers</li> <li>▪ Charity based services (eg RNLI in the UK)</li> <li>▪ Critical Infrastructure Operators:</li> <li>▪ Public Transport</li> <li>▪ All sort of Utility (Power, Gas, Water, ...)</li> <li>▪ Telecom Operators</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                |                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>organisations like Red Cross</li> <li>highways agency,</li> <li>network rail</li> </ul> | <ul style="list-style-type: none"> <li>Defence</li> <li>Civil defence</li> <li>Hospitals</li> <li>City councils</li> <li>Weather institutes</li> <li>Nature conservation institutes</li> </ul> |
|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 10.4 Story board

### 10.4.1 Precondition

- Country A has rolled out a permanent TETRAPOL-based radio network completed with dedicated overlay (LTE-based) to offer mission critical high speed data services (including video) to end users. Those users can also rely on commercial radio networks for non-mission critical high speed data services.
- Country B has rolled out a permanent TETRA-based radio network. Country B security forces are relying on commercial networks for any high speed data services.
- Both dedicated networks are designed to be “state-of-the art” resilient but such a resiliency (e.g. fuel for power generators) is time-limited.
- Both countries A and B are equipped with state-of-the-art carrier networks.

### 10.4.2 Flow of events

- Following a major flood that extends over the border of Country A and Country B, plenty of houses, shops, and buildings are flooded, some roads are flooded too with drivers blocked in their car or waiting for rescue services on top of it.
  - Plenty of 112-calls (thru fixed lines or carrier networks) are received at the different control rooms (Country A and B)
  - After two hours, carrier networks become out of order (power outage) leading to the situation that some people in danger are no more able to join call taking centres. Operations managers decide to deploy additional first responders on the field.
  - Carrier networks radio sites will remain out of order for several days.
- Between 24 to 36 hours after the crisis beginning, PPDR radio sites in both country A and B are falling down (no more fuel for power generators and no possibility to access the radio site to re-fuel)
  - Field forces are trying to work using DMO capabilities but due to limited coverage, operation management begins to be really challenging.
- Operation managers decide (both in country A and B) to deploy transportable solutions to compensate the disappearance of dedicated PPDR networks.
  - End-users will continue to use their day-to day equipment's
  - Deployed capacity will be significantly less than the one offered by the permanent infrastructure leading to reserve the resource access to high priority sub-operations and to limit some first responders to DMO.
- 6 hours later, a high speed train derailed due to rail damage caused by land slide. 200+ citizens are being severely injured.
  - Operations managers take the decision to “re-route” some first responders to manage this event and rescue injured citizens.

- Compared to the other operations in progress, this one becomes the one having the highest priority
- 5. The day after, PPDR networks are coming back to a normal mode of operation. Technical staff has been able to re-fuel power generator prior to the electricity power back
- 6. Two days after, carrier networks are back the normal situation.

## BIBLIOGRAPHY

- [1] SALUS Deliverable 2.1 "SALUS PPDR use cases – Intermediate", November 2013.
- [2] SALUS Deliverable 2.2 "SALUS PPDR user requirements", December 2013.
- [3] ETSI TR 102 022-1 v1.1.1, "User Requirement Specification; Mission Critical Broadband Communication Requirements", August 2012.
- [4] M. H. Pinson, S. Wolf, R.B. Stafford, "Video Performance Requirements for Tactical Video Applications", IEEE conference on Technologies for Homeland Security, 2007.
- [5] Department of Homeland Security, "Tactical and Surveillance Video Quality Experiments", Public Safety Communications Technical Report, November 2007.
- [6] Website IEEE Std 1471-2000, <http://www.iso-architecture.org/ieee-1471>
- [7] Website TOGAF, <http://www.opengroup.org/togaf/>
- [8] Open Safety & Security Architecture Framework (OSSAF),  
<http://www.openssaf.org/download>
- [9] Website MIT CISR, <http://cistr.mit.edu/research/research-overview/classic-topics/enterprise-architecture/>
- [10] Website Federal Enterprise Architecture (FEA), <http://www.whitehouse.gov/omb/e-gov/fea>
- [11] BITKOM "Leitfaden EAM Enterprise Architecture Management",  
[http://www.bitkom.org/files/documents/EAM\\_Enterprise\\_Architecture\\_Management\\_-\\_BITKOM\\_Leitfaden.pdf](http://www.bitkom.org/files/documents/EAM_Enterprise_Architecture_Management_-_BITKOM_Leitfaden.pdf)
- [12] D. Mattes „Enterprise Architecture Frameworks Kompendium“, Springer-Verlag Berlin Heidelberg, 2011
- [13] Website Zachman Framework, <http://zachman.com/>
- [14] NATO Architecture Framework Version 3, ANNEX 3 TO AC/322(SC/1-WG/1)N(2007)0004
- [15] Website Wikipedia, <http://en.wikipedia.org/wiki/Requirement>

## ACRONYMS

|       |                                               |
|-------|-----------------------------------------------|
| BAN   | Body Area Network                             |
| BAU   | Business As Usual                             |
| CCC   | Command and Control Centre                    |
| CCTV  | Closed Circuit Television                     |
| DMO   | Direct Mode of Operations                     |
| EA    | Enterprise Architecture                       |
| EAF   | Enterprise Architecture Framework             |
| GPS   | Global Positioning System                     |
| HQ    | Head Quarter                                  |
| IT    | Information Technology                        |
| LTE   | Long Term Evolution                           |
| NAF   | NATO Architecture Framework                   |
| NAV   | NAF All View                                  |
| NCV   | NAF Capability View                           |
| NSOV  | NAF Service Oriented View                     |
| NSV   | NAF System View                               |
| NOV   | NAF Operational View                          |
| NTV   | NAF Technical View                            |
| OSSAF | Open Safety & Security Architecture Framework |
| PMR   | Private Mobile Radio                          |
| PPDR  | Public Protection and Disaster Relief         |
| ProSe | Proximity Services                            |
| SOA   | Service Oriented Architecture                 |
| TETRA | Terrestrial Trunked Radio Access              |
| TOGAF | The Open Group Architecture Framework         |
| UML   | Unified Modelling Language                    |
| WBAN  | Wireless Body Area Network                    |
| Wi-Fi | Wireless Fidelity                             |
| ZAF   | Zachman Architecture Framework                |