Security **A**nd Interoperabi**L**ity in Next Generation PPDR Comm**U**nication Infrastructure**S**

Project Number: 313296

Deliverable 7.2

SALUS use cases validation – Intermediate

Scope	Scheduled deliverable
Lead Beneficiary	ADS
Dissemination level	Public
Document creation date	18/Mar/2015
Document release date	03/Aug/2015
Contractual Date of Delivery	30/May/2015
Version	1.2
Status	Final

***Abstract**: Deliverable 7.2 describes the approach and methodologies used to validate the three SALUS Use Cases (City Security, Temporary Protection, Disaster Recovery) described in the D2.3 deliverable.*

AUTHORS

Name	Organisation	Email
Daniel ZERBIB	**ADS**	daniel.zerbib@airbus.com
Paulo Simões	ONE	psimoes@onesource.pt
Edmundo Monteiro	ONE	edmundo.monteiro@gmail.com
Luis Cordeiro	ONE	cordeiro@onesource.pt
Bruno Sousa	ONE	bmsousa@onesource.pt
Konstantia Barbatsalou	ONE	konstantia@dei.uc.pt
Hugo Fonseca	ONE	htfonseca@onesource.pt
Georgios Charalampopoulos	UPAT	giwrgoscharalampopoulos@gmail.com
Panagiotis Galiotos	UPAT	pgaliot@gmail.com
Frank Brouwer	FIGO	frank.brouwer@figonet.com
Dragan Olcan	UB	olcan@etf.rs
Branko Kolundzija	UB	kol@etf.rs
Rick Hofstede	UTWENTE	r.j.hofstede@utwente.nl
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Hugo Marques	IT	hugo.marques@av.it.pt
Georgios Mantas	IT	gimantas@av.it.pt
Luis Pereira	IT	luis.pereira@av.it.pt

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Bruno Sousa	ONE	bmsousa@onesource.pt
Nuwan Weerasinghe	KU	nuwan.weerasinghe@kingston.ac.uk
Peter Wickson	AW	peter.wickson@airwavesolutions.co.uk
Hugo Marques	IT	hugo.marques@av.it.pt

EXECUTIVE SUMMARY

The main objective of this document is to describe the validation methodology of the three SALUS Use Cases developed in WP2 (see D2.3 [9]):

- Scenario 1 – City Security, based around a developing riot
- Scenario 2 – Temporary Protection, based on an Olympic-style sporting event
- Scenario 3 – Disaster Recovery, based around heavy flooding involving two countries

Considering the SALUS Use Cases make use of the applications, features and services of the SALUS platform (first prototype described in D7.1), this document will also be used to feed D7.3 (SALUS PPDR platform – Final) and D7.4 (SALUS use cases validation – Final). The relation between this document and its final version (D7.4) is depicted in Figure 1, whilst Figure 2 highlights the governing intention from this document focusing on the "Use Case validation".

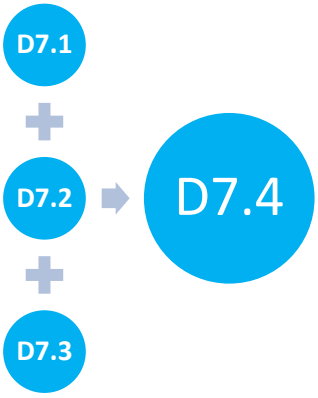

Figure 1 – Relation between WP7 documents and the SALUS Use Cases Validation

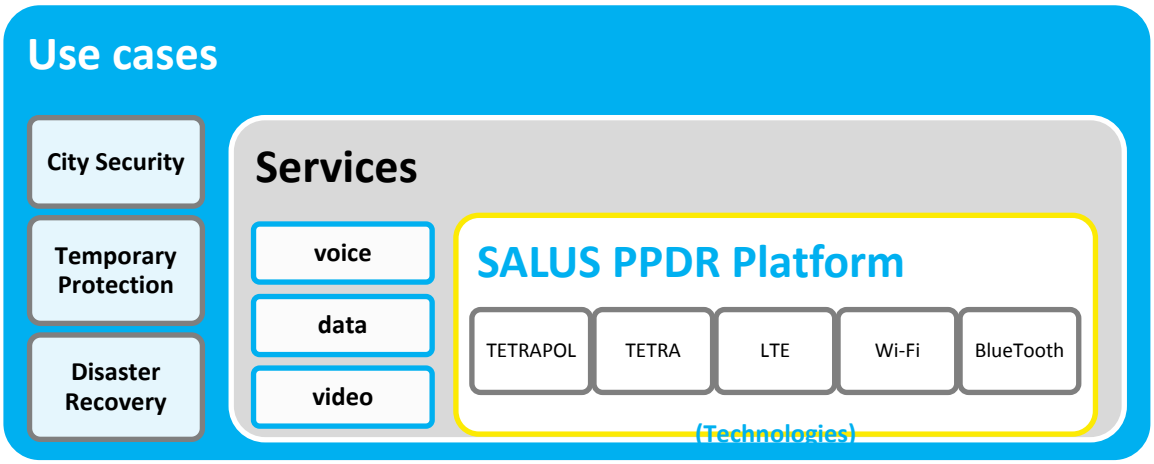

Figure 2 – Relation between the SALUS Use Cases and the SALUS PPDR platform

TABLE OF CONTENTS

TABLE OF FIGURES

1 INTRODUCTION

Public Protection and Disaster Relief (PPDR) agencies in EU member states are relying on digital Private Mobile Radio (PMR) networks for mission-critical voice and data communication. These networks are highly resilient and dimensioned to cope with crisis and emergency situations, and are well protected against monitoring and intrusion by means of encryption, authentication and integrity. The two main standards for digital PMR networks in Europe are TETRA (TErrestrial Trunked RAdio) and TETRAPOL.

These networks provide a secure and resilient mobile voice and data infrastructure, with features matched to the special requirements of PPDR, including broadcast, dynamic secure groups, push to talk, call priority and secure roaming. However, here are significant interoperability technological difficulties when using both technologies. Additionally, these networks provide limited inter-technology coverage (i.e. interoperability between different technologies) providing very ineffective management of emergency events, both at the national level and in cross-border regions.

The main goal of SALUS is to design, implement and evaluate a next generation communication network for Public Protection and Disaster Relief (PPDR) agencies, supported by network operators and industry [11]. To achieve this goal, this network needs to fully support the operational activities of the end user communities. The SALUS platform design is considered as achieved (see D7.1) and is not in the scope of this document. This document aims to describe the approach and methodologies used to validate the three SALUS Use Cases, based on operational scenarios and the storyboards detailing these Use Cases.

The use cases themselves were already developed and specified in WP2 (D2.3 [9]). The functionalities on which those use cases rely are described in D2.3 and D7.1 documents. Following this introduction, Section 2 describes the methodology used for completing the final use cases. Section 3 then describes each use case, providing information on pre-conditions, flow of events and involved actors. Section 4 provides a table that summarises all the required functionality for the successful response to the event, and Section 5 ends this report with final remarks.

2 METHODOLOGY FOR COMPLETING USE CASES VALIDATION

The aim of this document and thus of this methodology is not to technically validate the SALUS Platform and its sub systems. It is assumed here each sub system is technically unitary validated, and that the SALUS platform, as a “system of systems” has been preliminary integrated and validated.

The SALUS platform provides a set of products, technologies, hardware, software and protocols enabling many features and actions. The SALUS platform is described further in chapter 3.

The SALUS project has prepared (in WP2), three Use Cases to represent a range of situations where the SALUS platform may show its efficiency, compared to legacy systems. These Use Cases are described in chapter 4.

2.1 Methodology

The three SALUS Use Cases were preliminary validated through feedback received from multiple PPDR organizations to SALUS questionnaires (see Deliverables D2.1, D2.2, D2.3 and D2.4). Feedback from multiple PPDR organizations and key experts on this area was also collected during the 1-Day-Seminar on the Future of Communications organised by PSCE & TCCA and during the 1st SALUS Conference. From this feedback it was possible to validate how real the Use Cases were and the proposed sequence of events. From this assumption three final storyboards were defined. These storyboards were established with:

- A timeline;
- Initial and evolving situation;
- Stakeholders (number, competences, localisation, …);
- Actions performed;
- Result (situation) expected;
- Result (situation) achieved.

The aim of the storyboards is to simulate some customer field tests, and to ensure that the expected features are available. The step-by-step description of each action is the way to validate them. The detailed storyboards describe who, how, when will manage and front the disaster events planned in each of the 3 use cases.

Thus, the validation methodology relies on:

- 3 detailed storyboards reflecting the 3 Use Cases;
- 3 operational tests, based on those storyboards and on the final platform;
- At each step of a played storyboard, an operational result is obtained and compared to the expected result.

The methodology plans for Use Case validation results. These results are the 3 validation results reflecting the 3 operationally tested Use Cases. In these results, it may be noticed if the SALUS platform provides or not the expected service which is a qualitative result. We may get some quantitative or subjective results such as (e.g.):

- Clear voice or not;
- Smooth or delayed video;
- Fast or slow mobility/roaming/handover.

3 THE SALUS PPDR PLATFORM PROTOTYPE REMINDER

3.1 Abstract

This section presents the summary description of the SALUS PPDR platform prototype. The following subsections summaries describe the equipment used, as well as the list of the functionalities that the platform will offer. Regarding the functionalities presented, they are separated by first prototype and final prototype.

3.2 Summary of Equipment

This subsection presents the equipment's that were used during the first prototype of the SALUS PPDR platform. Table 1 summarizes the equipment used in the demonstration.

Table 1 – Mapping of the equipment of the first prototype.

Partners	Equipment	Description
ALU-I	Mobile Video	Mobile wearable camera
ALU-I	SCP Server	Server for the secure storage of files
ALU-I	Video Management System	Application that allows the management of the video assets
ALU-I	eNB, PDN GW	Components of the LTE Infrastructure
ADS	CCAPI Client/Server	n/a
ADS	TETRAPOL AG-R	Sub part from the IDR
ADS	TETRAPOL IDR	Independent digital repeater
ADS	TETRAPOL Terminal	Tetrapol hand portable terminal
FhG	CC App#1 and App#2	n/a
FhG	Drone	Multi-Copter
FhG	Mobile Ground Station	n/a
FIGO	Back Office Node (BON)	Virtual machine running in the ALU-I network
FIGO	Central Management System (CMS)	Network management software running on the FIGO BON
FIGO	Mobile Node (MN)	Each capable of simultaneously maintaining the following connections: 2xLTE + 2xWLAN mesh (802.11n) + WLAN AP (802.11g)
IT	AAuC Server	Virtual machine running in the ALU-I network. It is responsible for mobile node (MN) authentication and authorization on the Wi-Fi networks
IT	PKI Server	Virtual machine running in the ALU-I network. It is responsible for certifying the public keys of SALUS users, services or devices.
IT	SALUS IP Communication Server	Virtual machine running in the ALU-I network. It provides voice over IP (VoIP) services, specifically for PPDR communications. It allows push-to-talk and group call communications over IP networks.
KU	Rugged Device / Tablet	CML protocol running on 3 Android devices. Multi-hop functionality in Mobile ad hoc Network.
ONE	HUCare Backpack	Backpack with the body kit sensors, with support for LTE networks, HD video camera, audio and panic button.
ONE	HUCare Control	Command Control Centre component that displays information of multiple sensors sources, which are present in the

Partners	Equipment	Description
		elements of the PPDR entities.
ONE	HUCare Server	Server to support the exchange information between the HUCare Backpack and the HUCare Control. Also supporting processing and gathering of sensor information.
ROH	Gateway Server	n/a
ROH	LDS Chameleon Dispatcher	n/a
ROH	Mobile Dispatcher	n/a
ROH	TETRA Base Station	n/a
ROH	TETRA LTE TeTRA Node GW	relay for LTE
ROH	TETRA Terminal	Tetra hand portable terminal
ROH	TetraLink	n/a
ROH	TETRANODE NMS	n/a
UB	Man Down Sensor	Android smart-phone
UB	Man Down Server	Windows smart-phone
UB	Sensor data server	Web server installed on a notebook that forwards sensor data to CCC
UBITEL	Mobile Terminal (Android Smartphone)	Android app that captures the SSID frames from the access points nearby and forwards this lit to the localisation server
UBITEL	SmartPlug (Wi-Fi micro-access point)	Device in a pre-defined location that sends SSID frames and, thus, it is possible to triangulate the mobile node in the indoor environment based on the signal quality to all of the nodes
UBITEL	Localisation Server (PC)	The web-oriented app that captures the packets from the mobile terminal and post process them in order to estimate the terminal location on a map
UBITEL	Localisation Client (PC/Laptop)	Client with open browser to show the mobile terminal location on a map (can be any computer with web-browser and access to Localisation Server)
UL	Message Broker	MB service that runs inside a docker container.
UL	Mobile sensor app	Android app that streamed location data and heartrate signal to a sensor CCC application. It also displayed the position of units on the map.
UL	CCC sensor app	Meteor application that showed the location of forces on the map and their heart rate signals.
UL	CCC control app	Java application that remotely manipulated the mobile sensor apps: it switched on and off location and heart rate sensors and it sent key points of interest to mobile sensor apps.
UPAT	Client	Linux Netbook running myMONSTER Telco Communicator Suite (TCS).
UPAT	OpenEPC + MIH	Desktop running multiple virtual machines to simulate the components of the Evolved Packet Core (EPC), enodeb, epdg, pgw,sgw and epc-enablers.
UTWENTE	Flow exporter	Virtual machine running a flow exporter for transforming a SPAN session (i.e., traffic mirrored by a switch) into flow data using NetFlow/IPFIX.

Partners	Equipment	Description
UTWENTE	Flow collector + IDS	Virtual machine acting as a flow collector and running the flow-based IDS (SSHCure).
UTWENTE	LMA/MAG	Laptop running several VMs that run the Corresponding Node, LMA and MAGs respectively.
UTWENTE	MN	Laptop that acts as Mobile Node

3.3 Summary of offered Functionalities

The first prototype did not implement all the proposed functionalities to be supported by the diverse SALUS components. Table 2, below, summarizes the mapping of functionalities demonstrated in the first prototype and the ones to be demonstrated in the final prototype.

Table 2 – Mapping of functionalities between first and final prototypes.

Partners	Functionality	First Prototype	Final Prototype
UL and all with sensors	Integration of sensor information in the SALUS CCC application	Each partner with sensors provides its own CCC application to view sensor information	Sensor information will be integrated in the CCC application for complete situation awareness. TBC if a single or many applications are needed
UL	Security in the MB.	The message exchange with the MB is not secured.	MB will implement security mechanisms defined in the SALUS security architecture.
UTWENTE, UPAT	Mobility Management Components	The Mobility Management Components support Vertical and Horizontal Handovers between Wi-Fi and LTE with IPv4	The Mobility Management components are integrated through MIH to allow Vertical Handovers between Wi-Fi and LTE with IPv6
UPAT	Mobility Management Component with secure MIH		Integration of 802.21A in the MIH module, in order to provide the required security between the exchange messages.
KU	Secured ChaMeLeon routing protocol running on android devices for MANETs	ChaMeLeon routing protocol is deployed in a Wi-Fi Rugged device but not integrated with SALUS System	Integration of Secured ChaMeLeon driven ad-hoc network with SALUS System
FIGO	Ad-hoc network as range extension for mobile network	LTE + 802.11n based solution creating a basic range extension.	Enhanced range extension system including 5 GHz-based mesh solution and enhanced performance management.
UL, FhG and all with sensors	Sensor Message format	Partners using the Message Broker or other mechanism can specify their own message format for sensors. For instance, can be based on JSON, on XML, or other.	A common message format will be defined to be supported by the diverse sensor applications
IT	Certification services	Certificate services for authentication of SALUS users and secure servers	Additional certificate services for authentication of SALUS clients (fixed and mobile devices) and IPSec
IT	Authentication service for SALUS PPDR devices	Limited authentication capabilities of MN (Wi-Fi) devices	Full capability for authenticating MN devices in any SALUS Wi-Fi network
IT	Voice over IP support	Voice over IP support within all SALUS IP networks	Additional support for voice calls with external networks (PSTN or ISDN)
ROH and ADS	TETRA TETRAPOL interoperability	Human operator	Voice in / voice out
ROH and ALU-I	PMR-over-LTE support of multicast in CVDP relay	CVDP relay only support unicast signalling	CVDP relay supports multicast signalling
ROH and ALU-I	Integration of Mission-Critical Push to Talk over LTE in CVDP architecture	Available provided update by Rohill on pre-integrated equipment in ALU-I premises	Integration of Mission-Critical Push to Talk over LTE in CVDP architecture
UTWENTE, ONE, KU	Intrusion Detection Systems	The flow-based IDS (UTWENTE) will be demonstrated.	IDSes by UTWENTE and ONE, featuring inter-IDS communications, based on the local/global Security Manager.

Partners	Functionality	First Prototype	Final Prototype
ONE	Mobile Forensics	N/A	Integration of Mobile Forensics functionalities in the Intrusion Detection System of SALUS.
UBITEL	Indoor localisation service for end-user mobile devices	Proof-a-concept prototype with the localisation server, capable of estimating mobile devices localisation in real-time	Localisation service Is integrated with Message Broker and other necessary SALUS security Mechanisms as well as with common operators' visual interfaces
UB	Sensor data: man-down application, detection of man-down situation using motion sensors in smart-phones.	The possibility to detect man-down situation will be demonstrated with additional basic info and plot on the map.	The application will use the common message format for communication with SALUS CCC.
UB	Wi-Fi physical layer jamming		Demonstration of Wi-Fi jamming on physical layer using strong electromagnetic field. Detection and estimation of jamming area using smartphones.
FhG	Command Control Centre Applications	Situation display, UAV tracking and Video Display	Situation awareness (i.e. integration of status from sensors); PPDR Force Tracking
ADS	TETRAPOL Network connection	Tactical bubble with Control Room interface	Projectable TETRAPOL network, similar to an actual network, with its Control Room interface
ALU-I / IT	SALUS Dynamic QoS Controller	Not ready	Enables to create and/or modify service data flow policies and charging rules for each network user (UE) or group of UEs in real-time and for each type of service
ALU-I	1x 9773 LMC	ePC micro-core LTE available	ePC micro-core LTE available
ALU-I	1x enodeB	ePC micro-core LTE available	No change
ALU-I	1x Band 20 RRH	ePC micro-core LTE available	No change
ALU-I	1x Usb 4G dongle	Available	No change
ALU-I	3x galaxy S3 4G band 20	Available	No change
ALU-I	3x GalaxyTab 4G band 20	Available	No change
ALU-I	VMS solution	Based on Milestone Available	No change
ALU-I	PTT solution	Based on Rohill Available	No change
ONE	HUCare	Integrated with MB	Supporting security mechanisms defined in SALUS

4 THE FINAL SALUS USE CASES REMINDER

In this chapter we reuse some words from the D2.3 deliverable [9]- Use Case Final. It is indeed necessary to remind the results from WP2, to allow easier readability and comprehension.

This section describes the three SALUS use cases based on the three SALUS scenarios (City Security, Temporary Protection and Disaster Recovery). Starting from the use case description provided in the D.3 document, to ensure readability and comprehension,

These three types of operational scenarios were considered in SALUS as they were the basis of the study the German Ministry of Interior has produced (2010/11) to evaluate the amount of data to be transmitted and therefore the spectrum requirements for PPDR's future wireless broadband networks.

Each use case will have its own sequence of events; however similar events may occur during the first days of the crisis:

- Surveillance for security purposes (limitation of criminality);
- Investigation actions to evaluate the current status on the crisis;
- Broadcast information to the public (through television, radio and other means);
- Reparation attempts for some parts of the communication network infrastructure;
- Deployment of ad-hoc communication and possibly broadcast infrastructures after an engineering phase (i.e. performed by the military or the operators).
- Reorganization of the cohabitation between the deployed and existing communication networks in the neighbourhood of the crisis zone.

The following subsections will provide the details for each particular SALUS use case.

4.1 Use Case - City Security

4.1.1 Abstract

The City Security use case is based on the City Security scenario, which considers the management of a public disorder event (a peaceful protest which escalates into a full-scale riot) 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 other data applications-services capabilities used predominantly 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 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 capabilities such as remote controlled closed-circuit television (CCTV), aerial surveillance from a helicopter or fixed wing aircraft, 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 enhancement 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.

4.1.2 Precondition

- The protest starts off very peacefully. [1]
- The very small group of protesters (< 20 people) 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. However police public order trained support units are on patrol and to the locality. [7]
- The scenario takes place in a country where public CCTV is accepted and used by public organisations such as the police and local councils.
- Strategic command / Emergency Operations Centre not required for initial protest [12]
- 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 in “business as usual” mode.
    - Commercial 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 (“standard” BAU). However the room is initially staffed for BAU and therefore not staffed by strategic commanders of police, fire brigade, ambulances.
    - PPDR data communication facilities that allow role based access to information.

4.1.3 Flow of events

CS1 A 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.

CS2 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. The control room continuously tracks the location of the officers deployed via their GPS enabled handsets. Location updates are sent every 30s [person location].

CS3 50 protesters attend

CS4 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.
- The leading officer report about the (minor) incident to the Control Room. [Individual voice call].

CS5 Out of sight of the police and the protesters, one of the angry youths texts and tweets message to his friends. [1]

- 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’.

CS6 Within 10 minutes some 40 youths have gathered and start heckling the protesters.

CS7 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 for additional resources and transport for [priority group voice calling] the youth restrained who has now been arrested.

CS8 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 Emergency Button function automatically enables Video from the officers integrated helmet camera to be transmitted back to control as well as a short data message with the officers GPS (GALILEO) position information. 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, GPS and video plus pre-empt and network prioritisation].

- CCTV in the area are automatically activated, triggered by the officer pressing his emergency button and based on his location [Automatic CCTV activation].

CS9 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.

CS10 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.
- These additional officers switch to the talk group being used to manage the incident. A call is in already in progress and their radios quickly attach and start receiving the communication [late entry into group call].

CS11 The presence of additional officers arriving angers the youths further.

CS12 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 and performing real-time upload to Facebook, Twitter and YouTube.
- Some of them throw bottles at the police and the protesters causing some injuries.
- More youths appear from other pubs and surrounding buildings. They had received Facebook and Twitter messages and also seen footage on YouTube.
- The control room is informed about the injuries and calls for ambulance to be dispatched (telephone or radio interconnect of police and ambulance control room).

CS13 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.

CS14 The police leadership at the control room consider the situation to be more serious now, as there are now more than 150 youths and protesters on the street. Full strategic command in the Emergency Operations Centre (co-located with police Control Room) is installed. [7]

- 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 (controlled remotely from the control room) [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 stream are sent (downloaded) 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 calls the control room to request an ambulance. The officer is requested by ambulance control to carry out some basic assessment checks/treatment to help sustain life.
- The police (in Emergency Operation Centre) use criminal intelligence databases [database access] to establish details of the offenders. They discover that they are known trouble makers.

CS15 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. They receive KML files (Keyhole Mark-up Language) from dispatch and use Google Street Maps to familiarise themselves with the area and the

position of their colleagues. [Internet access].

CS16 A full scale riot is declared, as youths start looting local shops and start setting fires to cars and other property. [1] [23]

- Police officers are chasing youths into a building and lose their LTE coverage but their devices pick up a Wi-Fi hotspot provided within the building [seamless handover from LTE to Wi-Fi].
- The fire services are called in, as are more police and ambulance resources.

CS17 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 control room 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 strategic, tactical, operational 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].

CS18 A small group of police officers in attendance at the scene are dispatched to protect ambulance and fire officers [interoperability between different PPDR organisations] 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.

CS19 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]. [27]
- A gang of youths burned down a local post office. They then run into a nearby underground car park. There is no PPDR coverage in the car park.
- Use of firearms suspected. SWAT teams 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 busses and local businesses and homes.
- Police 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.

CS20 The incidents last for 4 days and spread in over 15 towns and cities across the country. [17] [22]

- In total, additional police resources required increased to several thousands.
- 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]. [27]

4.1.4 Expected Users (Use case actors)

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

Table 3 - List of users for the City Security use case

▪ Police (Gendarmerie)
  ○ Overt
  ○ Covert
  ○ Mutual aide/out of area forces
▪ Ambulance services, incl. volunteer organizations as red cross
▪ Fire Brigades
	▪ Security Services (covert)
	▪ Transport
	▪ Military
	▪ CCTV operators
	▪ Traffic management
	▪ Mayor's office in the City Hall,
	▪ Defence, civil defence

4.2 Use Case - Temporary Protection

4.2.1 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.

4.2.2 Precondition

- A large scale multi-day sports event (e.g. Olympic Games) is taking place, spread over a number of venues.
- The total number of daily visitors to the complete event is around 50,000.
- The storyboard event occurs at a single venue, which can hold 50,000 spectators. The venue is filled before the event commences. [6]
- Evacuation plans that have been pre-tested are predefined, and stored in a data base.[7]
- The venue is secured with a large number of CCTV cameras, which can be monitored from a venue specific control room.
- An enhanced command and control structure (Emergency Operations Centre) is in place for the duration of the event at every city involved.
- 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 (compared to BAU), to be used by operational forces of police, ambulance services, and fire brigades.
    - Commercial 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.
    - Ad-hoc network equipment is available in first responder vehicles.
    - EOC facilities. The room is staffed by commanders of police, fire brigade, ambulances, and the venue security organisation.
    - PPDR data communication facilities that allow role-based access to information.

4.2.3 Flow of events

TP1 The sports arena is filled to the last seat, i.e. 50,000 spectators are in the venue. The match is progressing and the crowd is joyful though a bit anxious as it is a tight match.

TP2 Using 112, an unknown person calls the local dispatch room, indicating that multiple bombs are placed at this specific venue. According to the message each bomb is said to explode after 30 minutes.[5]

- All 112-calls are recorded. [Distant Voice recording] Call analysis [Distant speech recognition] 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. [Database access]
- All information is stored in the CCC. The various organisational levels have their own access to the CCC, roles, and rules based.

TP3 The call-taker informs his superior (tactical level) of the threat, by calling and

referring to the recorded data. [Multimedia call] [7]

TP4 The tactical level officer informs the strategic team of the national coordination centre, including reference to the recorded data. [Multimedia call]

TP5 The strategic team searches for other relevant information and evaluates the situation. [Database access] The national coordination centre takes the decision to start the evacuation of the venue, and commands the local control centre to start evacuation. [Multimedia call]

TP6 The local command and control centre coordinates the evacuation procedure. The overall operation is under the management of the national coordination centre.

TP7 In parallel, the bombers have communicated their bomb threat through social media.

- Social media analysis tools find this stream of messages. [Social media analysis tool]
- The evacuation has not yet started. The first spectators receive information on the threat, get nervous and start to go to the exit. This abnormal behaviour is detected by video cameras, using video content analysis to trigger and human expertise to validate. [CCTV]

TP8 The predefined evacuation plan is started, including the following actions: [25]

- All PPDR personnel locations are tracked. [Location service, 30 s updates]
- Inform all tactical units that evacuation will take place, according to plan X. This plan is pre-defined. User specific information of this plan is sent to the involved tactical units. [Multimedia group call] 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. [Multimedia group call]
- Telecom facilities are switched over to ‘priority mode’. [Priority mode] (Public access is limited, bandwidth consuming applications are limited.)
- Non-PPDR frequency bands are jammed to avoid explosives to be remotely controlled. [Jamming device]
- Media partners are briefed, including a set of instructions on what is expected. [Multimedia multicast – this involves non PPDR telecom infrastructure]

TP9 Operation units are instructed.

- Operational staffs at the outer checkpoints are instructed to stop people coming in. The instructions are provided on a head-up display (e.g. google-glasses) [Multimedia multicast]. The instruction includes the message they have to give to the visitors, saying that “the next match is postponed for security reasons”, redirection information, gathering points to be used, etc.
- Gathering points are staffed.
- Buses with visitors are directed to leave the area immediately.

[multicast – this involves non PPDR telecom infrastructure]

- Additional ambulances and fire trucks are directed to the venue. [Location services & database access]
- Special (covert) forces are instructed to watch out for suspects. [multimedia multicast] They have received the briefing, including descriptions of possible suspects based on the analysis of the strategic team.
- Some additional drones are airborne [remote control, video streaming], to have a better view over the terrain.

TP10 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. [Multimedia broadcast, multiple technology]

TP11 The first (small) bomb explodes creating limited damage. Some LTE-PPDR infrastructure has been destroyed, creating some dead spots. [15]

TP12 Panic breaks out. People start to rush to the exits, with continuous very loud shouting.

- The panic is mapped using intelligent sound analysis [sound analysis], video images [CCTV] plotted on a map [location services].
- Venue security guards try to streamline the crowd, but with little success. A number of security guards get trapped and trampled on by the scared crowd. They press their emergency button. [Emergency service]
- Security guards need to assist one another to streamline the crowd. They see each other's positions (autonomously) [Location services] and activities that are monitored through worn sensors [WBAN] in their head-up displays so that they can cooperate more easily. [27]
- Some people get injured. Security guards separate the injured. They apply sensors to monitor the vital signs of the injured. [WBAN] These sensors become visible in a monitoring application in the CCC. [27]
- Disabled people are tagged with location devices. [WBAN, location services] The amount of assistance for these people is monitored. Where needed, security personnel are directed to assist. [Location services & database access]

TP13 Special Forces have identified suspects based on their behaviour. CCTV footage has been analysed to detect suspicious behaviour to identify possible bomb-setters. [CCTV] A combination of drones and fixed cameras start following these persons [video streaming], and plot their position on maps at the CCC [Location services]. The Special Forces are continuously updated to the current status of suspects [database access]. Intervention by special forces is directed to the most likely suspects, while other possible suspects remain tracked. [multimedia multicast]

TP14 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. This footage is added to the common operational picture. [Internet access]

- The control room instructs a team to go the specific location to video the conditions. [video streaming]
- The evacuation plan is rearranged to take care of the new situation. [database access]
- The new plans for the evacuation are distributed to all operational teams, and partner organisations. [Multimedia multicast]
- Due to the rearrangements, ad-hoc network capacity is needed at unforeseen locations. [Ad-hoc networking and WLAN handover]

TP15 The identified suspects are tracked down using various methods including fingerprints [database access] and taken into custody by the special forces. During this operation the Special Forces communicate among each other on their action and finings. [multimedia group call]

TP16 The complete venue is being search systematically for explosives. The search is executed by a group of security personnel, making geo-tagged pictures or videos of possibly suspicious objects. [Location services, streaming video, augmented reality] A small team of bomb disposal experts examines in detail these objects using remote controlled robots, with video and sensors. [Remote control, multimedia call, augmented reality] A third bomb is found and disarmed.

- During this search the location of all personnel involved is plotted. [Location services]
- Not yet evaluated persons are estimated and plotted on the map, combined with cleaned areas. [Database access]
- Progress on the operation is briefed to the strategic team, partner organisations, and media partners. [Multimedia multicast]

4.2.4 Expected Users (Use case actors)

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

Table 4 - List of users for the Temporary Protection use case

▪ Police
  ○ Overt
  ○ Covert
  ○ Mutual aide/out of area forces
▪ Ambulance
▪ Fire Brigades
▪ Security Services (covert)
▪ Transport
▪ Civilian/event security
▪ City Councils
	▪ Transport
	▪ Military
	▪ CCTV operators
	▪ Traffic management
	▪ Hospitals
	▪ Road operators
	▪ Weather institutes
	▪ Nature conservation institutes
	▪ Utilities companies (power, gas, water)
	▪ Telecom operators

Note: Fire brigades and Ambulance involvement is low until Day2 scenario occurs	

4.3 Use case - Disaster Recovery

4.3.1 Abstract

The Disaster Recovery use case is based on the analysis of the Disaster Recovery scenario, which considers PPDR communications requirements for both the short and medium terms where all existing infrastructure has been rendered unserviceable by a man made or natural disaster. Additionally the disaster scenario crosses geographical boundaries.

This use case focus on the secure communications needs for voice, video and data applications-services capabilities used by Rescue Workers, Military, Police, Fire, Ambulance and other rescue workers during a significant disaster where all or a major part of the existing PPDR communications infrastructure has been destroyed. The use case defines the capabilities and the services that are often established today using deployable communications networks that include PMR and cellular 2G/3G/LTE. The use identifies the applications and services that can be introduced using local deployable data networks, such as video from aircraft, and location based asset management and mapping. This will include how these can be securely integrated into existing deployable solutions, providing the PPDR with a holistic communications capability that addresses their voice, video and data needs both locally at the incident, as well as for remote situational awareness and management. Deployed communications would need to be able to deal with adverse environmental conditions and could include extreme wind speeds, large areas without energy/drinkable water etc., where integration with satellite as a primary communications mechanism or a transmission backhaul could be deployed. Biggest problem will be the maintaining of PPDR communications on 24/7 basis, despite all upcoming problems.

In defining the Disaster Recovery services, the use case also identifies 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 7.4.

4.3.2 Precondition

- Country A has rolled out a permanent TETRAPOL-based radio network completed with dedicated overlay (LTE-based) to offer mission critical high speed broadband data services (including video) to end users. The PPDR users also rely on commercial mobile communication networks for non-mission critical high speed data services.
- Country B has rolled out a permanent TETRA-based radio network. Country B security forces rely on commercial mobile communication networks for high speed data services.
- Both dedicated networks are designed to be “state-of-the art” and power resilient (e.g. fuel for power generators). Within the area affect due to risk assessments and financial considerations PPDR site power resilience is less than in other areas at 6 hours.[3]
- Both countries A and B are equipped with state-of-the-art mobile communications networks designed to meet the needs of the general public. Power resilience is designed to meet standard commercial requirements at half an hour
- It is assumed that both countries A and B speak a common language and have agreed provisional plans for dealing with certain major cross border events.
- This is the first natural disaster for many years requiring cross-border co-operation.

4.3.3 Flow of events

DR1 Following a prolonged period of heavy rain, a large river bursts its banks

causing major flooding that extends over the border of Country A and Country B. Several houses, shops, light industrial factories and buildings become flooded, some roads are flooded also. A number of car and van drivers become trapped, either in their cars, or have managed to climb up onto the roofs. [16]

- As a result a high volume of 112 emergency calls [thru fixed lines or mobile phone networks] are received at the different control rooms of country A and country B.
- Given that the information from the meteorological office had forecast this heavy rain and risk of flooding, a strategic, tactical and operational command structure had already been established across A and country B. The Gold strategic command group (SCG) is led by the police and consists of senior representatives from police, fire and ambulance as well as civil authorities. There are also a number of Silver tactical command groups (TCGs) in place in a number of control rooms. These are also police-led.
- Immediately several police, fire and ambulance resources are deployed to the area in response to the 112 calls that have been received, under instruction from the silver commands [group calls & interoperability between TETRA and TETRAPOL]

DR2 On arrival into the area the first responders realise that the number of stranded public and risk to life is greater than what has been reported. This is due to the fact that many people have been unable to make a 112 call because public mobile have become over loaded compounded by flooding affecting the fixed telephone network infrastructure.

- This information is relayed to the TCG control rooms that immediately deploy additional resources [group calls & interoperability between TETRA and TETRAPOL]. The additional resources which include military arrive within 2 hours and join in the rescue operation. Prior to arrival their radios are automatically switched to the appropriate talk group [DGNA]

DR3 Local schools, community and sports centres are identified as designated rest areas. They are closed for normal business and rescued people are transported there in ambulances. Make-shift medical facilities are also established as hospitals are too far away due to the poor road conditions. PPDR staff locations are tracked by the control rooms using GPS based location services [Location Services]

DR4 The rainfall continues and an electricity sub-station becomes flooded causing a wide spread electricity outage affecting both public and PPDR base stations. After half an hour, the mobile phone networks fail preventing any more emergency 112 calls being made over the commercial mobile network. The PPDR sites are now reliant on their autonomous but limited power backup capability. The remoteness of the sites, weather conditions and health and safety concerns do not allow the sites to be refuelled and after 6 hours the PPDR systems covering the affected area also fail.

- Field forces are trying to work using DMO capabilities but due to limited coverage, operation management begins to be really

challenging [DMO].

- Transportable solutions equipped with TETRA, TETRAPOL, LTE, autonomous power and satellite backhaul capabilities are deployed to provide maximum PPDR coverage and capacity in strategic locations. [Transportable solutions]
- Deployable PPDR systems operate on discrete narrow band channels and therefore use reserved channels to enable them to be deployed anywhere for either coverage or capacity enhancements. Given the permanent PPDR system is no longer available the deployable capacity will be less than the one offered by the permanent infrastructure. [12]
- Access to the deployable LTE system is reserved for high priority sub-operations and to limit some first responders using DMO [reserved access or mobile telecoms privilege access scheme (MTPAS)].

DR5 Air support is deployed by way of helicopters equipped with camera providing aerial video images to the local control room (s) [Video streaming]

- Air to ground communications is used between the control, air support and the resources on the ground [Air to ground voice and video]

DR6 The rain continues, resulting in building collapses, more casualties and stranded people in their cars and buildings. The rescue continues:

- Some emergency personnel are wearing sensors and their vital signs are monitored by the local control rooms as they enter into dangerous locations such as partially collapsed industrial buildings that might contain hazardous chemicals [BWAN]

DR7 Several hours later, a high speed train is derailed due to railway line damage caused by land slide. More than 200 citizens are severely injured.[18]

- Some resources are re-directed to the scene of the derailment and their radios are switch to a new talk group [group call][DGNA][interoperability]. Compared to the other operations in progress, this one becomes the one having the highest priority
- When weather conditions permit, CCTV cameras connected to small drones are also deployed to provide aerial video images to the local control rooms and field commanders [Group video]
- Paramedics on the scene transmit patient data and video back to the make-shift medical centres where instructions by voice are given on what treatment to apply at the scene [mobile data – sensor, video, voice]

DR8 Charities' and volunteers are now also involved in the rescue operation and transporting of casualties to the rest areas

- Police in the local control rooms use social networking to provide additional information [Internet access] to the public

DR9 Although the rain has stopped, flooding and infrastructure remains widespread. The rescue and search for casualties continues for several days with temporary PPDR infrastructure in place for the duration of the incident.

DR10 Only after a couple of weeks the PPDR mobile phone networks return to a normal mode of operation.

4.3.4 Expected Users (Use case actors)

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

Table 5 - List of users for the Disaster Recovery use case

▪ Police (High involvement)
  ○ Overt
  ○ Mutual aide/out of area forces
▪ Ambulance (High involvement) including charity based services (e.g. Red Cross or RNLI in the UK)
▪ Fire Brigades (High involvement)
▪ Transport
▪ Military
▪ Environment agency,
▪ Volunteer mountain rescue type units
▪ Highways agency,
	▪ CCTV operators
	▪ Traffic management
	▪ NGO/Volunteers
	▪ Critical Infrastructure Operators
	▪ Public Transport
	▪ All sorts of Utility (Power, Gas, Water, …)
	▪ Telecom Operators
	▪ Defence
	▪ Civil defence
	▪ Hospitals
	▪ Temporary medical and evacuation centres
	▪ City councils

5 FUNCTIONALITIES USED BY USE CASE

This section describes the SALUS platform functionalities that will be used and validated, for each use case. The driving idea to identify the features/functionalities and go through all of them is to stick to the storyboard relative to each of the three use cases. The storyboards were presented above, and a link to these storyboards is accessible through the “reference” number ‘column #2 from the table).

Then, the table is divided in 3 parts:

- City Security for scenario 1 and CSi references (described in previous chapter)
- Temporary Protection for scenario 2 and TPi references (described in previous chapter)
- Disaster Recovery for scenario 1 and RCi references (described in previous chapter)

- Table 6 – Functionalities per use case.

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
Scenario 1 – City Security							
1	CS2	APLS	Data applications	Location services	Police officers Police control	Location data	Yes
2	CS7	Individual voice call	Point-2-point voice	Individual call	Police officers Police control	2-way voice traffic	yes
3	CS8	Pre-emptive priority	Emergency voice	Pre-emptive priority	Police officers Police control	Priority indicator 2-way voice traffic	No
4	CS8	Open microphone	Emergency voice	Open microphone	Police officers Police control	Priority indicator 2-way voice traffic	No
5	CS8	Video	Group video	Group video streaming	Police officers Police control	Video data traffic	Yes
6	CS8	Prioritisation for video	Group video	Prioritisation within group	Police officers Police control	Priority indicator Video data traffic	No
7	CS10	Group voice call	Group voice	Group call	Police officers Police control	2-way voice traffic	Yes
8	CS10	Late entry	Group voice	Group call	Police officers Police control	2-way voice traffic	Yes
9	CS10	APLS	Data applications	Location services	Police officers Police control	Location data	Yes
10	CS10	AVLS	Data applications	Location services	Police officers in	Location data	YEs

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
					vehicles Police control		
11	CS10	Late entry	Group voice	Late entry	Police officers	2-way voice traffic	Yes
12	CS14	CCTV access	Data applications	Remote controlled CCTV	Police control	Live video data CCTV control data (?)	Yes
13	CS14	APLS	Data applications	Location services	Police officers Police control	Location data	Yes
14	CS14	Live video streaming	1-2-1 video	Video streaming	Police officers Police control	Live video data from officer to control room	Yes
15	CS14	Group picture	Broadcast image	Talk group related	Police officers Police control	Picture images	Yes
16	CS14	Group voice call	Group voice	Group call	Police control Police officers Ambulance control	2-way voice traffic	Yes
17	CS14	Database access	Database searching	Operational database search	Police officers	Mobile data traffic	Mobile data: Yes Database: No
18	CS15	Internet access	Data applications	Internet access	Police officers	Mobile data traffic	Yes
19	CS16	Handover from LTE to trusted Wi-Fi	Technology handover	Technology handover between different networks	Police officers	Voice/data	Data: Yes Voice: No
20	CS17	Internet access	Data applications	Internet access	Police control	Mobile data traffic	Yes
21	CS17	Augmented reality	Data applications	Augmented reality	Police officers	Mobile data traffic	No
22	CS17	DGNA	Group voice	Dynamic reassignment	Police officers Police control	Configuration data	No
23	CS18	Interoperability	Interoperability	Interoperability	Police, fire and ambulance teams	Voice traffic between tetra and LTE	Between LTE and TETRA: Yes
24	CS18	Database access	Database searching	Operational database search	Fire fighters	Mobile data	No
25	CS19	WBAN	Data applications	Monitor personnel vital signs	Police officers Police control	Mobile data	Yes

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
					Fire fighters Fire control		
26	CS19	DMO gateway	Mobile adhoc network	DMO gateway	Police firearms officers Police control	Voice traffic	Yes
27	CS20	APLS	Data applications	Location services	Police officers Police control	Location data	Yes
28	CS20	Video broadcast	Group video	Group video streaming	Police officers Police control	Video data	No
29	CS20	WBAN	Data applications	Location services	Police officers Police control Fire fighters Fire control	Mobile data	Yes (indoor and outdoor)
Scenario 2 – Temporary Protection							
30	TP2	Voice Recording	Individual voice	Telephony call	Police control	2-way voice traffic	2-way voice: yes Voice recording: no
31	TP2	Speech recognition	Data applications	Operational database search	Police control	Voice/data	no
32	TP2	Database access	Database searching	Operational database search	Police control	Mobile data	Mobile data: yes Database: no
33	TP3	Multimedia call	Voice	Multimedia call	Police control	Voice/data	yes
34	TP4	Multimedia call	Voice	Multimedia call	NOCC Police control	Voice/data	yes
35	TP5	Database access	Database searching	Operational database search	NOCC Police control	Data	No
36	TP5	Multimedia call	Voice	Multimedia call	NOCC Police control	Voice/data	yes
37	TP7	Social media analysis	Social media	Internet access	NOCC Police control	Internet Data	Internet data: yes Social media: no
38	TP8	APLS	Data applications	Location services	NOCC All PPDR personnel	Location data	yes

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
					Police control		
39	TP8	Multimedia group call	Group voice/data	Group call	NOCC Police officers Fire fighters Ambulance crews Event security Transport Road operators	2-way Voice/Data	Voice: yes Data: no
40	TP8	Multimedia group call	Group voice/data	Group call	NOCC City council	2-way Voice/Data	Voice: yes Data: no
41	TP8	Priority Mode (MTPAS)	Mobile network prioritisation	MTPAS	NOCC PPDR Personnel	Voice/data	no
42	TP8	Frequency Jamming			Radio Technical Support	Radio Frequencies	No
43	TP8	Multimedia multicast	Group voice/data	Multicast call	NOCC Media	2-way Voice/Data	Yes
44	TP9	Multimedia multicast	Group voice/data	Multicast call	NOCC Event security Transport	2-way Voice/Data	Yes
45	TP9	AVLS	Data applications	Location services	NOCC Fire Ambulance	Location data	Location: yes Vehicle system: no
46	TP9	Database access	Database searching	Operational database search	NOCC Fire Ambulance	Data	No
47	TP9	Multimedia multicast	Group voice/data	Multicast call	NOCC Covert personnel Transport	2-way Voice/Data	Yes
48	TP9	Remote control video streaming	Group video	Group video streaming	NOCC	Video data traffic	Yes

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
49	TP10	Multimedia broadcast	Group voice/data	Multicast call	NOCC General public	Video data	No
50	TP12	Sound analysis	Data applications	Sound analysis	NOCC General public	Data	No
51	TP12	Location services	Data applications	Location services	NOCC General public	Data	Yes
52	TP12	Pre-emptive priority	Emergency voice	Pre-emptive priority	NOCC Event security	Priority indicator 2-way voice traffic	No
53	TP12	Open microphone	Emergency voice	Open microphone	NOCC Event security	Priority indicator 2-way voice traffic	No
54	TP12	APLS	Data applications	Location services	NOCC Event security	Location data	Yes
55	TP12	Augmented reality	Data applications	Augmented reality	Event security	Mobile data traffic	Mobile data: yes Aug. reality: No
56	TP12	WBAN	Data applications	Location services	Event security	Mobile data	Yes
57	TP12	APLS (wheelchair)	Data applications	Location services	NOCC Disabled public	Location data	Yes
58	TP13	Live video streaming	1-2-1 video	Video streaming	NOCC Covert personnel	Live video data from officer to control room	Yes
59	TP13	APLS	Data applications	Location services	NOCC Covert personnel	Location data	Yes
60	TP13	Multimedia multicast	Group voice/data	Multicast call	NOCC Covert personnel SWAT team	2-way Voice/Data	Voice: yes Data: no
61	TP14	Internet access	Data applications	Internet access	NOCC	Mobile data traffic	Yes
62	TP14	Live video streaming	1-2-1 video	Video streaming	NOCC Event security	Live video data	Yes
63	TP14	Database access	Database searching	Operational database search	NOCC Event security	Data	Mobile data: yes Database: no
64	TP14	Multimedia multicast	Group voice/data	Multicast call	NOCC All PPDR personnel	2-way Voice/Data	No
65	TP14	Adhoc network and WAN handover			NOCC		Yes

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
66	TP15	Fingerprint scanners	Data applications	Operational database search	SWAT team	Operational data	Mobile data: yes Fingerprint: no
67	TP15	Multimedia group call	Group voice/data	Group call	SWAT team	2-way Voice/Data	Voice: yes Data: no
68	TP16	Geo-tagging	Location services	Location services	Bomb squad	Location data	Yes
69	TP16	Live video streaming	1-2-1 video	Video streaming	Bomb squad	Live video data	Yes
70	TP16	Augmented reality	Data applications	Augmented reality	Bomb squad	Mobile data traffic	Mobile data: yes Aug. reality: No
71	TP16	Remote control			Bomb squad		No
72	TP16	Multimedia group call	Group voice/data	Group call	Bomb squad	2-way Voice/Data	Voice: yes Data: no
73	TP16	APLS	Data applications	Location services	NOCC All PPDR personnel	Location data	Yes
74	TP16	Database access	Database searching	Operational database search	NOCC Event security	Data	Mobile data: yes Database: no
75	TP16	Multimedia multicast	Group voice/data	Multicast call	NOCC Media partners	2-way Voice/Data	Voice: yes Data: no
Scenario 3 – Disaster Recovery							
76	DR1	Group voice call	Group voice	Group call	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	Yes
77	DR1	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	No
78	DR2	Group voice call	Group voice	Group call	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	Yes
79	DR2	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	No

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
80	DR2	DGNA	Group voice	Dynamic reassignment	Tactical command Police officers Fire fighters Ambulance crew Military	Configuration data	No
81	DR3	APLS	Data applications	Location services	Tactical command Police officers Fire fighters Ambulance crew Military	Location data	Yes
82	DR4	DMO	Group voice	Direct mode operating	Police officers Fire fighters Ambulance crew Military	2-way voice traffic	No
83	DR4	Transportable solutions			Tactical command Police officers Fire fighters Ambulance crew Military		TETRAPOL: Yes TETRA: Yes LTE: No
84	DR4	Priority Mode (MTPAS)	Mobile network prioritisation	MTPAS	Tactical command Police officers Fire fighters Ambulance crew Military	Voice/data	No
85	DR5	Live video streaming	1-2-1 video	Video streaming	Air support	Live video data	Yes
86	DR5	Air to ground	Air to ground		Air support Tactical Command	2 way voice and video	No
87	DR6	Live video streaming	1-2-1 video	Video streaming	Tactical command Police officers Fire fighters Ambulance crew Military	Live video data	Yes
88	DR6	WBAN	Data applications	Location services	Police officers Police control Fire fighters	Mobile data	Yes

No.	Ref.	Functionality	Category	Item	Actors	Information types	Validated (first prototype)
					Fire control		
89	DR7	Group voice call	Group voice	Group call	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	Yes
90	DR7	DGNA	Group voice	Dynamic reassignment	Tactical command Police officers Fire fighters Ambulance crew Military	Configuration data	Yes
91	DR7	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic	No
92	DR7	Group video call	Group video	Group video streaming	Tactical command Police officers Fire fighters Ambulance crew	Video data traffic	No
93	DR7	Data group call	Group voice/data	Group call	Paramedics Medical centre personnel	Patient mobile data	No
94	DR8	Internet access	Data applications	Internet access	Police control room	Mobile data traffic	Yes

6 A SUMMARY OF THE HARDWARE AND SOFTWARE FOR THE VALIDATION OF THE USE CASES

The use case validation requires all the components in terms of software and hardware to be integrated in the SALUS platform, initially described in D7.1.

Deliverable D7.1 “SALUS PPDR platform – Intermediate”, in chapter 2 “The SALUS PPDR Platform” [28] gives, first, an overview of the SALUS PPDR platform and, then, describes the platform components. The table below reminds briefly the list of those components. Much more details are available in the document mentioned above (D7.1).

Table 7 – Platform description.

what	Functionalities
TETRA	The Terrestrial Trunked Radio (TETRA) is employed in all the SALUS use cases for mission critical services, such as group calls, late entry and emergency calls
TETRAPOL	TETRAPOL is employed in all the SALUS use cases for mission critical services, as some countries use TETRAPOL instead of employing TETRA.
LTE	To enable LTE as a future PPDR network, SALUS considers two main components the LTE Evolved Node (eNodeB) to provide a working network infrastructure and the Open Evolved Packet Core (EPC) with Media Independent Handover (MIH) support for mobility management between heterogeneous technologies.
Wi-Fi	The Wi-Fi network is an important part of the various communication technologies expected to interoperate in the SALUS PPDR platform.
Wireless sensor Networks	Wireless sensor networks are an integral part of SALUS. They allow collection of information from the environment that improves situation awareness of PPDR forces.
Location Devices	The indoor location service comprises a set of smart electricity plugs with built-in low-power Wi- Fi access points deployed in the building.
Video System	Video is the key application driving the need for wireless broadband public safety networks. It brings additional tools and information for better and faster decision making while enhancing operational effectiveness.
Air Surveillance	The Air Surveillance System consists of the following three main parts: ▪ Mobile Ground Control Station (MGCS); ▪ Sensors; ▪ Assets carrying the sensors.
Command and Control Centre	Operational Decision-making node at the tactical level. It consists of various applications collocated in one location (for example dedicated control room), connected via an IP-based LAN.
Mobility Management	Mobility management plays an essential role in the routers in the backbone of the SALUS PPDR platform. Proxy Fast Mobile IPv6 (PFMIPv6) will be used to support mobility of devices between IPv6-based networks.
Security Services	Public Key Infrastructure KPI, Intrusion Detection Systems (IDSes) are deployed in all networks of the SALUS Security Architecture and are responsible for detecting intrusions in critical infrastructure components, Mobile Device Forensics
SALUS IP communications Server	The SALUS IP Communications server enables voice and video communication over IP networks.

7 CONSIDERATIONS AND REMARKS

The first step for the validation of the three SALUS Use Cases was achieved through the feedback directly received from PPDR organizations to specific questionnaires sent by SALUS. These questionnaires and their answers can be found on Deliverables D2.1, D2.2, D2.3 and D2.4. Feedback from multiple PPDR organizations and key experts on this area was also collected during the 1-Day-Seminar on the Future of Communications organised by PSCE & TCCA and during the 1st SALUS Conference.

The second step in the validation was the production of three different storyboards (one per each Use Case) that were partially validated (in terms of technical feasibility) by the SALUS PPDR platform – first system prototype, during the first Project Review.

As such it is assumed the three SALUS Use Cases to be validated in terms of reality and coherency in the sequence of events, being only missing the full validation in terms of technical feasibility, which can only be achieved when the final prototype would be ready. In this sense it is important to note the SALUS platform is an aggregation of complex systems. These systems were designed and are currently being developed in different countries by different industries/organizations in Europe. Sub-systems of these systems are sometimes taken as commercial off-the-shelf (COTS) and used “as they are”, whilst others are being adapted and some other are designed and created specifically for the purpose of the SALUS platform. The SALUS Platform is considered as a “system” and, as end-users expect from this system, services, features and functionalities are dependent from each Use Case. The end-user uses the SALUS platform and expects form it an adequate and predictable behaviour compliant with his mission. Then, while using the SALUS platform, the end-users will decide if the system was compliant or not. The validation results rely on the experimented end-user feedback about the SALUS Prototype. This may be a bit fuzzy or subjective, because linked to the end-user perception. As an example, the SALUS prototype will allow some roaming features, but we do not have quantitative requirement about the admitted delay to recover, such convenience or inconvenience will be noted by the end-user, as long he goes to the flow chart corresponding to each of the 3 use cases.

BIBLIOGRAPHY

[1] BBC. (2011, October 24). *London riots: Metropolitan Police response report*. Retrieved December 21, 2013, from BBC News: http://www.bbc.co.uk/news/uk-england-london-15433404

[2] CEPT/ECC. (2013). *User requirements and spectrum needs for future European broadband PPDR systems (Wide Area Networks).*

[3] Dragland, Å. (2013, May 9). *Improving Communications During Disasters*. Retrieved October 2013, from Science Nordic: http://sciencenordic.com/improving-communication-during-disasters

[4] European Council's Law Enforcement Working Party. (2013). LEWP Matrix.

[5] *List of Terrorist Incidents*. (2013). Retrieved October 2013, from Wikipaedia: http://en.wikipedia.org/wiki/List_of_terrorist_incidents

[6] Municipality of Rotterdam. (2009). *COT Rapport: Strand rellen in Hoek van Holland.* Municipality of Rotterdam.

[7] National Policing Improvement Agency. (2009). *Guidance on Command and Control.* London: Association of Chief Police Officers.

[8] *Recent Natural Disasters*. (2013). Retrieved from http://www.disaster-report.com/

[9] SALUS. (2013). *SALUS Deliverable D2.3.* London: SALUS.

[10] SALUS. (December 2013). *Deliverable 2.1, SALUS PPDR use cases – Intermediate.*

[11] SALUS. (December 2013). SALUS Description of Work (DoW).

[12] UK Home Office. (2013). *Public Safety Group Call Use Metrics.*

[13] Wikipedia. (n.d.). Retrieved October 2013, from Wikipedia: http://nl.wikipedia.org/wiki/Troonswisseling_in_Nederland_(2013)

[14] Wikipedia. (2004). *Boscastle Flood of 2004*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/Boscastle_flood_of_2004

[15] Wikipedia. (2009). *Grayrigg Derailment*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/Grayrigg_derailment

[16] Wikipedia. (2009). *Riots beach of Hoek van Holland* . Retrieved October 2013, from Wikipedia: http://nl.wikipedia.org/wiki/Strandrellen_in_Hoek_van_Holland

[17] Wikipedia. (2010). *2010 Slovenia Floods*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/2010_Slovenia_floods

[18] Wikipedia. (2011). *England Riots 2011*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/2011_England_riots

[19] Wikipedia. (2011). *Royal Wedding of Prince William and Kate Middleton*. Retrieved November 2013, from Wikipedia: http://en.wikipedia.org/wiki/Wedding_of_Prince_William_and_Catherine_Middleton

[20] Wikipedia. (2011). *Security for the 2012 Summer Olympics*. Retrieved November 2013, from Wikipedia: http://en.wikipedia.org/wiki/Security_for_the_2012_Summer_Olympics

[21] Wikipedia. (2012). *London 2012 Olympic and Paralympic Games*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/London_2012_Olympics

[22] Wikipedia. (2012). *Project-X Haren*. Retrieved October 2013, from Wikipedia: http://nl.wikipedia.org/wiki/Project_X_Haren

[23] Wikipedia. (2013). *7 July London Bombings*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/7_July_2005_London_bombings

[24] Wikipedia. (2013, November). *Kings Cross Fire*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/King%27s_Cross_fire

[25] Wikipedia. (2013). *Protests in Slovenia*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/2012%E2%80%9313_Slovenian_protests
[26] Wikipedia. (2013). *Ski-World Championship 2013, Schladming, AUSTRIA*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/FIS_Alpine_World_Ski_Championships_2013
[27] Working Group for Wireless Personal Area Networks (WPANs). (2010). Channel Model for Body Area Network (BAN). *IEEE P802.15*.

ACRONYMS

3G	Third Generation
3GPP	Third Generation Partnership Project
AAuC	Authentication Authorization Centre
AIRBUS	Airbus (Formerly Cassidian)
AP	Access Point
ASFPG	Association Security and Fraud Prevention Group
ATHO	ATHENS Olympic Games
ATIS	Alliance for Telecommunications Industry Solutions
AUTOCON	Ad-Hoc Network Auto configuration
AW	Airwave Solutions
BAN	Body Area Networks
BON	Back Office Node
BS	Base Station
CA	Certification Authority
CCAPI	Control Centre Application Programmable Interface
CCC	Command Control Communication
CCSR	Centre for Communication Systems Research
CEPT	The European Conference of Postal and Telecommunications Administrations
CISM	Computing, Information Systems and Mathematics
CML	Chameleon
CMS	Central Management System
COSI	Standing Committee on Internal Security
CVDP	TBD
DGNA	Dynamic Group Number Assign
DMO	Direct Mode Operation
e2e	End-to-End
EAP	Extensible Authentication Protocol
EC	European Commission
EC/EU	European Commission / European Union
ECRIT	Emergency Context Resolution with Internet Technologies
ECS	Emergency College Services (Finland)
EPC	Evolved Packet Core
EOS	European Organization for Security
ERIC	Emergency Response Interoperability Centre
ESA	European Space Agency
ESRIF	European Security Research and Innovation Forum
ETSI	European Telecommunications Standards Institute

FP5/6/7	Framework Programme 5th/6th/7th
FRONTEX	European External Borders Agency
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
IAP	Integrated Applications Promotion
ICT	Information and Communication Technologies
IDABC	Interoperable Delivery of European eGovernment Services to public Admin., Businesses, Citizens
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISI	Inter System Interface
ISO	International Organisation for Standardisation
iSOF	interoperable Secure Operation Framework
IST	Information Society Technologies
IT	Instituto de Telecomunicações
ITU	International Telecommunication Union
KU	Kingston University
LTE	Long Term Evolution
LEWP	Law Enforcement Working Party
LMA/MAG	TBD
MAC	Medium Access Layer
MANET	Mobile Ad-hoc Network
MCR	Multi-Channel Routing
MIMO	Multiple Input Multiple Output
MSK	Master Session Key
NATO	North Atlantic Treaty Organisation
OLSR	Optimized Link State Routing
OTAK	Over The Air Keying
P2P	Peer-to-Peer
PAS	Tetrapol Publicly Available Specification
PC	Project Coordinator
PCC	Project Coordination Committee
PHY	Physical layer
PKI	Public Key Infrastructure
PM	Project Manager
PMs	Person Months

PMC	Project Management Committee
PMR	Professional Mobile Radio
PSTN	Public Switched Telephone Network
QMR	Quarterly Management Report
QoS	Quality of Service
R&D	Research and Development
RFC	Request For Comment
RNLI	Royal National Lifeboat Institute
ROH	Rohill Technologies B.V.
SAE	1: Simultaneous Authentication of Equals
SAE	2: System Architecture Evolution (3GPP)
SDS	Short Data Services
SIP	Session Initiation Protocol
SME	Small Medium Enterprise
SON	Self-Organizing Networks
STREP	Specific Targeted Research Project
SwMI	Switching and Management Infrastructure
TC	Technical Committee
TEA	TETRA Encryption Algorithms
TETRA	TErrestrial Trunked RAdio
TFEU	Treaty on the Functioning of the European Union
TL	Task Leaders
TM	Terminal Manager
TMO	Trunked Mode Operation
UCIF	Unified Communications Interoperability Forum
UMTS	Universal Mobile Telecommunications System
UPAT	University of Patras
VoIP	Voice over IP
WBAN	Wireless Body Area Networks
WG	Working Group
Wi-Fi	IEEE 802.11
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WMN	Wireless Multimedia and Networking
WP	Work Package
WWRF	Wireless World Research Forum

ANNEX A - VALIDATION PLAN OF FIRST PROTOTYPE

A.1 SALUS PPDR PLATFORM – FIRST SYSTEM PROTOTYPE FUNCTIONALITIES

Figure 3 below depicts the SALUS PPDR platform – first system prototype - available functionalities for validation/demonstration during the 1st project review:

Figure 3 – First system prototype functionalities

A.2 SALUS PPDR PLATFORM – FIRST SYSTEM PROTOTYPE DEMONSTRATION SCENARIO

The validation/demonstration of the SALUS PPDR platform – first system prototype, will be mainly based on the **Disaster Recovery Use Case**, as described in SALUS deliverable 2.3.

A.2.1 Precondition

- Country A has rolled out a permanent TETRAPOL-based radio network completed with dedicated overlay (LTE-based) to offer mission critical high speed broadband data services (including video) to end users. The PPDR users also rely on commercial mobile communication networks for non-mission critical high speed data services.
- Country B has rolled out a permanent TETRA-based radio network. Country B security forces rely on commercial mobile communication networks for high speed data services.
- Both dedicated networks are designed to be "state-of-the art" and power resilient (e.g. fuel for power generators). Within the area affect due to risk assessments and financial considerations PPDR site power resilience is less than in other areas at 6 hours.[3]
- Both countries A and B are equipped with state-of-the-art mobile communications networks designed to meet the needs of the general public. Power resilience is designed to meet standard commercial requirements at half an hour
- It is assumed that both countries A and B speak a common language and have agreed provisional plans for dealing with certain major cross border events.
- This is the first natural disaster for many years requiring cross-border co-operation.

A.2.2 Scenario summary

Following a prolonged period of heavy rain, a large river bursts its banks causing major flooding that extends over the border of Country A and Country B. Several houses, shops, light industrial factories and buildings become flooded, some roads are flooded also. A number of car and van drivers become trapped, either in their cars, or have managed to climb up onto the roofs.

A common (Country A and Country B) Command and Control Centre (CCC) has been deployed as a result from the meteorological office weather forecast.

A.2.3 Flow of events

[Bruno/One] At the beginning, the scenario is explained.

[Philippe/ALU-I] The reviewer and the PO are provided with a guided tour through the site – includes ALU-I lab plus outdoor location, where the MGS is located.

The reviewer and the PO are brought back to the Lab and the SALUS PPDR platform – first system prototype validation starts.

#1: Several police, fire and ambulance resources are deployed to the area under instruction from the CCC.

Set-up of talk-groups, group call is made from the CCC to PPDR users in **different technologies** (TETRA and TETRAPOL or TETRA and LTE or TETRAPOL and LTE)

Persons Involved: ROH – Mervin (TETRA; LTE Teamlink app) ADS DANIEL – (TETRAPOL)
1. [Mervin/ROH] One TETRA, one TETRAPOL mobile stations (MS) and one LTE user equipment (UE) with pre-configured talk groups, are shown to the reviewer; NOTE: There must exist at least one talk group that contains a TETRA user and a LTE user (i.e. belong to the same talk group); 2. [Mervin/ROH] 'TeamLink' application is explained [the device screen is been shown in a projector screen].

#2: On arrival into the area the first responders realise that the number of stranded public and risk to life is greater than what has been reported.

Group call (triggered by PPDR users) involving **different technologies** request additional resources.
Persons Involved: ROH – Mervin Teamlink App OTHER – TETRA terminal
1. [Mervin/ROH] 'TeamLink' application is used to trigger a group call that will involve two TETRA MS and one LTE UE (the one used by Mervin); 2. [Mervin/ROH] The procedure is repeated but the group call is now started by a TETRA MS

#3: Military arrive at the scene and join in the rescue operation. Prior/upon to their arrival their radios are automatically switched to the appropriate talk group.

Late entry is made by the CCC
Person Involved: ROH - Mervin Chameleon LDS OTHER - LTE UE to be attached.
1. [Mervin/ROH] Chameleon LDS is used to remotely activate/associate one LTE UE to the appropriate talk groups; Patch between military and police group. 2. Reviewer checks the LDS operation on the LDS display. It is shown that the new LTE UE can participate on an on-going group call; 3. [Mervin/ROH] Additional functionalities for the Chameleon LDS may be shown.

#4: As PPDR users arrive at the scene, their locations are tracked by the CCC

Localization/positioning of PPDR users based on GPS and/or sensors are shown on **situation awareness** application. This may include inside building/tunnel scenario (no GPS).
Persons Involved: UL – David to show location application Person next to VAN – with Android phone to be outdoor location UBITEL – Vitaly Person in the lab – with Mobile Phone for indoor location

1. [David/UL] Outdoor location is shown through the use of UL location application and sensors [outdoor location may be reported to the CCC via FIGO MESH network - the same network that supports the GCS];
2. [Vitaly/UBITEL] Indoor location is shown through the use of UBITEL location solution;
3. Reviewer checks this on a projector screen.

#5: As PPDR users arrive at the scene, their vital signs are tracked by the CCC.

Sensors monitor a subset of PPDR users' vital signs and this information is displayed on a **situation awareness** application.

Persons Involved:

UL – David demo sensors apps

1. [David/UL] Vital signs are monitored through the use of the same UL application [a single sensor may be used, just to show the concept];
2. Reviewer checks this on a projector screen.

#6: As PPDR users arrive at the scene, their LTE UEs are uploaded with the area map and key points of interest (CCC location, schools, hospitals, etc.)

High-speed (broadband) access to data – UL to update their Android app to show location map plus positioning of nearby users

Persons Involved:

UL – David – to have device with map

1. [David/UL] Using a ROH LTE device [the device screen is been shown in a projector screen], it is shown the user can get access to the area map (broadband, fast connection).

   NOTE#1: Originally, the ROH device will use a specific UL application, but it would be great to have this (somehow) integrated with the TeamLink application;

   NOTE#2: ideally the map should also show key points of interest (KPIs) for the operation, such as Hospitals and CCC location, area of coverage, etc.
2. Reviewer checks this on a projector screen.

#7: Access to the deployable LTE system is reserved for high priority sub-operations and to limit some first responders.

MTPAS (Mobile Telecommunication Privileged Access) **support on deployable LTE**

Persons Involved:

ALU-I – Jerome

1. [Jérôme/ALU-I] explanation for how LTE can safeguard QoS for public safety communications;

   NOTE: this will be demonstrated with the 2 video cameras

#8: Despite the TETRA/TETRAPOL and LTE transportable solutions are in place, in some areas there is still no PPDR network coverage and DMO begins to be really challenging. A transportable (self-sustained) Wi-Fi hotspot is brought into the scene and with a mix of infrastructure/mesh and multiple-hop wireless topology, PPDR communications are restored in that area (Wi-Fi, IP based communications only).

FIGO MN for **infrastructure and Mesh**,

Terminal authentication, AAuC PKI, IP Communications Server

Chameleon routing protocol for **multiple hop wireless network**

Vertical handover from LTE to Wi-Fi and vice-versa

Persons Involved:

- FIGO – Frank – deploy WiFi Infrastructure
- IT – Hugo – to explain PKI Server and IP Communication Server
- IT – Luis? – to hold mobile device to authenticate in the AAuC.
- Other – JohnDoe – to perform VoIP call using the IP Communication Server
- KU – Alexandros, Person
- Other for KU

NOTE#1 Outside: There is a FIGO access point providing a Wi-Fi (hotspot) coverage and at least one Wi-Fi mobile node (MN);

NOTE#2: Outside–to-inside: the hotspot is connected to the CCC through a FIGO Wi-Fi mesh network

NOTE#3: On the CCC there will be the PKI, an IP communications server and a Wi-Fi MN;

1. [Frank/FIGO] Explanation on the FIGO mesh network, including its visual topology through FIGO application.
2. [Hugo/IT] The PKI is presented including explanation how users/terminals can obtain digital certificates for authentication purposes;
3. [Hugo/IT] One Wi-Fi MN is used to show how terminal authentication (access to SALUS infrastructure) is controlled by the AAuC through the use of digital certificates.
4. [Hugo/IT] Explanation on how a terminal can use a SALUS digital certificate to create an end-to-end secure IPSec tunnel to the CCC.
5. Reviewer checks previous steps on a projector screen;
6. [Hugo/IT] The IP communications server is presented and its functionalities are explained;
7. Reviewer checks this on a projector screen.
8. [JohnDoe] A user on the hotpsot uses VoIP to communicate with the MN on the CCC (through FIGO mesh);
9. [Alexandros/KU] A VoIP call between three (or more) devices in a stand-alone multiple hop wireless network is shown (call occurs with no access to the infra-structure).

   Note#7: The reviewer keeps and uses one of the terminals – he is an intervenient of the voice call.
10. [Georgios/UPAT] A video streaming scenario is shown during the handover from LTE to Wi-Fi due to lost of coverage from one of the networks. It is shown that despite loosing coverage it is possible to handover to another network and maintain communication (resiliency).
11. [Bernd/UTWENTE] Seamless horizontal mobility in Wi-Fi, based on IPv6. To demo with Video application.

12. Reviewer checks this on a projector screen.

#9: To improve the situation awareness, an air drone equipped with camera is deployed to provide aerial video images to the CCC

Air drone, **remote control, video streaming**, **Ground Control Station**

Use TETRAPOL terminal to communicate between CCC and GCS

Persons Involved:

- ADS – Daniel
- FHG – Frank
- FHG – Operator of drone

1. [Daniel/ADS] The CCC uses a TETRAPOL MS to request drone assistance to the GCS outside (which also uses a TETRAPOL MS);
2. [Frank/FhG] GPS coordinates are sent through FhG application;
3. [FhG] Drone flies to waypoint 1 and video streaming from the drone is shown on the CCC. The video streaming is relayed by the GCS through the FIGO mesh network to the CCC;

   NOTE: ALU-I video management system (VMS) is able to integrate the drone video;
4. Reviewer checks this on a projector screen.

#10: Several hours later, a high speed train is derailed due to railway line damage caused by land slide. More than 200 citizens are severely injured. Some PPDR users are re-directed to the scene of the derailment and their radios are switched to a new talk group

Deployable LTE and TETRAPOL (island mode)

Persons Involved:

- ALU-I – demonstrate functionalities of LTE
- ADS – DANIEL demonstrate functionalities of TETRAPOL
- ROH - demonstrate functionalities of TETRA

1. [Jérôme/ALU-I] The reviewer is shown the LTE, TETRA and TETRAPOL deployable solutions (probably during its guided tour through the lab).
   a. [Daniel/ADS] explains more deeply the TETRAPOL repeater solution (island mode) and the *new* implemented functionalities;
   b. [Jérôme/ALU-I and Mervin/ROH] may want to also add some additional description on their own (LTE/TETRA) solutions.
2. [Mervin/ROH] Mobile Dispatcher, deployment of TETRA system

#11: Compared to the other operations in progress, the area of the railway accident becomes the one having the highest priority.

LTE with pre-emption

Persons Involved:

- ALU-I – demonstrate functionalities of LTE

1. [Jérôme/ALU-I] The pre-emption capability is shown on the LTE – there is an LTE cell overloaded (no resources available) and one less important call is disconnected so a more important call can take place;

   NOTE: There is yet the need to clarify how this should be shown to the reviewer, probably by

displaying configuration through a management interface - too technical?

#12: The air drone is redirected to the area where the railway accident has occurred, to provide improved situation awareness.

Air drone, **remote control**, **video streaming**, **Ground Control Station**
Persons Involved: • ADS - DANIEL TETRAPOL • FHG - Frank • FHG – Operator of Drone
1. [Daniel/ADS] In the CCC a TETRAPOL MS is used to request drone assistance to the GCS outside (which also uses a TETRAPOL MS); 2. [Frank/FhG] New GPS coordinates are sent through FhG application ; 3. [FhG] Drone flies to waypoint 2 and video streaming from the drone is shown on the CCC. The video streaming is relayed by the GCS through the FIGO mesh network to the CCC, within different wireless technologies; 4. Reviewer checks this on a projector screen;

#13: Paramedics (using PPDR terminals and wearable cameras wirelessly linked to a vehicle/boat) on the scene transmit patient data and video back to the make-shift medical centres where instructions by voice are given on what treatment to apply at the scene.

Wearable camera, ~~LTE Mobile video management system (car/boat),~~ video streaming, **sensors (with Bluetooth linked to PPDR terminals) for vital signs monitoring**, **voice call**, **high-speed (broadband) access** to data
Persons Involved: • ALU-I – show video camera • ALU-I – • ONE - Cordeiro • Person Volunteer - backpack
1. [ONE] Show video from backpack with sensor information 2. [ONE] The HUCare is explained in detail, how it can be used to support the activity of paramedics. 3. The reviewer checks the footage being received at the CCC and also on the one being received by the doctors (campaign hospital) LTE terminals (e.g. ROH LTE terminals)

#14: A PPDR user is caught by a landslide and his down. This is captured at the CCC through the man-down application alert. The CCC remotely triggers the emergency button on the user's PPDR terminal which enables the open microphone functionality and establishes a communication channel

Man-down sensor, **man-down application alert**, **emergency button**, **remote activation of emergency button**, **open microphone**.
Persons Involved: • UB – Branko

1. [Branko/UB] A man-down situation is triggered (e.g. using one of the LTE terminals with the man-down application;
2. [Branko/UB] A man-down situation alert pops on the situation awareness application and the location is extracted (and passed to the FhG drone application – if possible);

#15: The air drone is redirected to the location of the man-down to provide improved situation awareness.

Air drone, **remote control**, **video streaming**, **Ground Control Station**
Persons Involved: • FHG - Frank • FHG – Operator of Drone
1. [FhG] Show position of man down on map of FhG CCC Application, and 2. [Frank/FhG] New GPS coordinates are sent through FhG application 3. [FhG] Drone flies to waypoint 3 and video streaming from the drone is shown on the CCC. The video streaming is relayed by the GCS through the FIGO mesh network to the CCC; 4. Reviewer checks this on a projector screen;

#16: Charities' and volunteers are now also involved in the rescue operation and transporting of casualties to the rest areas. Police in the local control rooms use social networking to provide additional information [Internet access] to the public.

PPDR infrastructure to provide (limited) **Internet access to citizens (to check with ALU-I)**
Persons Involved: • UL David
1. [David/UL] Limited data access is provided to citizens; 2. [David/UL] A MN (ROH LTE device) is used to simulate a citizen using Wi-Fi to access the Internet. Whatever the url the citizen uses, it will always resolve to the same IP address, which is the webpage for the event; NOTE: this webpage contains information for citizens: procedures, events, phone numbers, locations, etc…); 3. Reviewer checks this on a projector screen.

#17: Although the rain has stopped, flooding and infrastructure remains widespread. The rescue and search for casualties continues for several days with temporary PPDR infrastructure in place for the duration of the incident. During this period the SALUS Intrusion Detection System has detected suspicious activity in one PPDR Terminal which has tried to obtain a valid digital certificate. This action triggered an alert for terminal recovery/disconnection. Using the terminal's location coordinates, the police was able to recover the terminal and the Mobile Forensics allowed to obtain additional information on the motivation behind the theft.

SALUS PKI, **SALUS IDS**, **remote control**, **Mobile Forensics**
Persons Involved: UTWENTE – Bernd
1. [Rick/UTWENTE] An attacker tries to obtain unauthorized access to the public safety communications network;

NOTE#1: the attacker performs an enumeration/ recognition attack (e.g. nmap) ant then by discovering a 22 port open on the PKI server, it performs a SSH brute force attack;

2. [Rick/UTWENTE] The IDS is able to detect the attack (and eventually to take countermeasures – if possible). The IDS management interface is shown to the reviewer.
3. Reviewer checks this on a projector screen

#18: Only after a couple of weeks the PPDR mobile phone networks return to a normal mode of operation.