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

Project Number: 313296

Deliverable 2.3

SALUS PPDR use cases – Final

Scope	Scheduled deliverable
Lead Beneficiary	Airwave
Dissemination level	Public
Document creation date	31/Oct/2014
Document release date	31/Dec/2014
Contractual Date of Delivery	31/Dec/2014
Version	1
Status	Final

***Abstract**: Deliverable 2.3 describes the final SALUS use cases as a result of multiple PPDR user inputs, and building on the interim use cases that were described in deliverable 2.1. More emphasis is placed on the actual sequence of events as they would unfold in the three operational scenarios, the emergency response to the events and the PPDR communications that would be deployed to support the emergency response. As with deliverable 2.1, this deliverable focuses on maximising the return on investment of their existing networks recognising today's market and financial realities, whilst addressing the pressing future communications needs.*

AUTHORS

Name	Organisation	Email
Andy Nyanyo (editor)	**AW**	**andy.nyanyo@airwavesolutions.co.uk**
Hugo Marques	IT	hugo.marques@av.it.pt
Peter Wickson	AW	peter.wickson@airwavesolutions.co.uk
Frank Brouwer	FIGO	frank.brouwer@figonet.com
Manfred Blaha	PSCE	manfred.blaha@gmx.net
David Jelenc	UL	david.jelenc@fri.uni-lj.si
Jérôme Brouet	ALU	jerome.brouet@alcatel-lucent.com
Kari Junttila	ESC	kari.junttila@pelastusopisto.fi
Branko Kolundzija	UB	kol@etf.rs

QUALITY ASSURANCE TEAM

Name	Organisation	Email
Bert Bouwers	ROH	bert.bouwers@rohill.nl
Wouter Klein Wolterink	UTWENTE	w.kleinwolterink@utwente.nl
Geert Heijenk	UTWENTE	geert.heijenk@utwente.nl
Hugo Marques	IT	hugo.marques@av.it.pt

EXECUTIVE SUMMARY

The main objective of this document is to present the final version of the SALUS use cases developed from the three agreed SALUS scenarios. These use cases will be used to address the needs of the Public Protection and Disaster Relief (PPDR) user community as they migrate into the next generation PPDR network with their continuing exacting voice requirements augmented with ever increasing data needs and multimedia capabilities.

The following three use cases have been developed:

- Scenario 1 – Public order demonstration or riot
- Scenario 2 – Olympic-style sporting event
- Scenario 3 – Heavy flooding due to prolonged periods of rain

The use cases have been developed go into a lower level of detail than previously since they have been updated and refined following initial end user feedback.

Following this deliverable the next steps will be to use these finalized use cases as inputs to subsequent work packages and tasks such as tasks 7.2. 7.3 and 7.4 in work package 7 which include the intermediate and final prototype demonstrations.

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

Public Protection and Disaster Relief (PPDR) agencies in EC member states are relying on digital Private Mobile Radio (PMR) networks for mission-critical voice and data communication. These networks are highly resilient and properly dimensioned to cope with crisis and emergency handling, 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, and they do have 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 community. The development and end user validation of use cases based on operational scenarios is therefore an important first step as it will drive the requirements from which the solution will be based.

This document describes the development of the final detailed use cases that have been produced and the methodology used in which to produce them. 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 the final use cases

Following on from the interim SALUS deliverable 2.1, the approach to completing the final SALUS use cases was to build on the interim use cases and further refine them based on additional end-user feedback as well as to add more detail. This was done by storyboarding the step-by-step sequence of events that are likely to occur during each scenario [9], and then validating them with the end user community to test for accuracy and credibility of the scenarios and the final requirements going into SALUS deliverable 2.4 [10].

At each step the emergency response and the method of communications that would be in use to support that emergency response were identified.

Due to the procedural variations that exist between end users from different countries the feedback received was used to describe some specific parts of the use cases in a more generic context. Alterations to the flow were changed only where they made a significant impact on the technological requirements.

The collected end user feedback can be found in Appendices 1 to 3 at the end of this document.

Figure 1 below shows at a high level, the approach that was used.

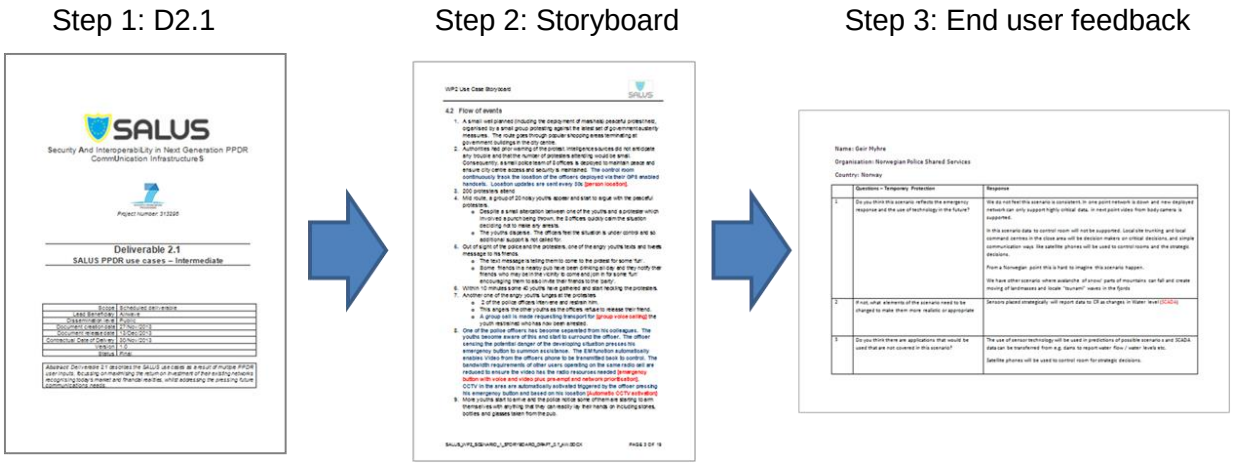

Figure 1 – High level approach for use cases and requirements capture.

2.1 High Level Delivery Plan

Figure 2 below shows the high level delivery plan that was agreed to manage the activities necessary to complete deliverable 2.3.

No.	Item	Owner	Due Date
1.	Participation in WP2 workshop to develop interim use cases	All partners	16/01/2014
2.	Production of storyboards for scenarios 1, 2 and 3	AW, FIGO, CAS	01/02/2014
3.	Review of storyboards for input to WP3	IT, ALU, ROH	15/02/2014
4.	First draft of final use cases	AW, FIGO, CAS	30/05/2014
5.	WP2 workshop - partner input and resolve interfaces	All partners	10/06/2014
6.	Update final use cases/storyboards	AW, FIGO, CAS	15/08/2014
7.	Test draft use cases with end users	All partners	26/11/2014
8.	Update final use cases/storyboards	AW, FIGO, CAS	05/12/2014
9.	Quality check by the Quality Assurance Group	UTWENTE, IT, ROH,	12/12/2014
10.	Final submission of deliverable 2.3	AW	31/12/2014

Figure 2 – High level delivery plan

3 The Final SALUS Use Cases

This section describes the three SALUS use cases based on the three SALUS scenarios (City Security, Temporary Protection and Disaster Recovery).

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.

3.1 Scenario 1 - City Security

3.1.1 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.

3.1.2 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.

3.1.3 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 talkgroup 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 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]

3.1.4 Expected Users (Use case actors)

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

Table 1 - 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

3.2 Scenario 2 - Temporary Protection

3.2.1 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.

3.2.2 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.

3.2.3 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. [Voice recording] Call analysis [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 staff 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. [Multi media 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 analyzed 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]

3.2.4 Expected Users (Use case actors)

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

Table 2 - 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	

3.3 Scenario 3 - Disaster Recovery

3.3.1 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.

3.3.2 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.

3.3.3 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]

1..1. 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.

3.3.4 Expected Users (Use case actors)

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

Table 3 - 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

4 Summary of Functionality Used

No.	Ref.	Functionality	Category	Item	Actors	Information types
Scenario 1 – City Security						
1	CS2	APLS	Data applications	Location services	Police officers Police control	Location data
2	CS7	Individual voice call	Point-2-point voice	Individual call	Police officers Police control	2-way voice traffic
3	CS8	Pre-emptive priority	Emergency voice	Pre-emptive priority	Police officers Police control	Priority indicator 2-way voice traffic
4	CS8	Open microphone	Emergency voice	Open microphone	Police officers Police control	Priority indicator 2-way voice traffic
5	CS8	Video	Group video	Group video streaming	Police officers Police control	Video data traffic
6	CS8	Prioritisation for video	Group video	Prioritisation within group	Police officers Police control	Priority indicator Video data traffic
7	CS10	Group voice call	Group voice	Group call	Police officers Police control	2-way voice traffic
8	CS10	Late entry	Group voice	Group call	Police officers Police control	2-way voice traffic
9	CS10	APLS	Data applications	Location services	Police officers Police control	Location data
10	CS10	AVLS	Data applications	Location services	Police officers in vehicles Police control	Location data
11	CS10	Late entry	Group voice	Late entry	Police officers	2-way voice traffic
12	CS14	CCTV access	Data applications	Remote controlled CCTV	Police control	Live video data CCTV control data (?)
13	CS14	APLS	Data applications	Location services	Police officers Police control	Location data
14	CS14	Live video streaming	1-2-1 video	Video streaming	Police officers Police control	Live video data from officer to control room
15	CS14	Group picture	Broadcast image	Talk group related	Police officers Police control	Picture images
16	CS14	Group voice call	Group voice	Group call	Police control Police officers	2-way voice traffic

No.	Ref.	Functionality	Category	Item	Actors	Information types
					Ambulance control	
17	CS14	Database access	Database searching	Operational database search	Police officers	Mobile data traffic
18	CS15	Internet access	Data applications	Internet access	Police officers	Mobile data traffic
19	CS16	Handover from LTE to trusted WiFi	Technology handover	Technology handover between different networks	Police officers	Voice/data
20	CS17	Internet access	Data applications	Internet access	Police control	Mobile data traffic
21	CS17	Augmented reality	Data applications	Augmented reality	Police officers	Mobile data traffic
22	CS17	DGNA	Group voice	Dynamic reassignment	Police officers Police control	Configuration data
23	CS18	Interoperability	Interoperability	Interoperability	Police, fire and ambulance teams	Voice traffic between tetra and LTE
24	CS18	Database access	Database searching	Operational database search	Fire fighters	Mobile data
25	CS19	WBAN	Data applications	Monitor personnel vital signs	Police officers Police control Fire fighters Fire control	Mobile data
26	CS19	DMO gateway	Mobile adhoc network	DMO gateway	Police firearms officers Police control	Voice traffic
27	CS20	APLS	Data applications	Location services	Police officers Police control	Location data
28	CS20	Video broadcast	Group video	Group video streaming	Police officers Police control	Video data
29	CS20	WBAN	Data applications	Location services	Police officers Police control Fire fighters Fire control	Mobile data

No.	Ref.	Functionality	Category	Item	Actors	Information types
Scenario 2 – Temporary Protection						
30	TP2	Voice Recording	Individual voice	Telephony call	Police control	2-way voice traffic
31	TP2	Speech recognition	Data applications	Operational database search	Police control	Voice/data
32	TP2	Database access	Database searching	Operational database search	Police control	Mobile data
33	TP3	Multimedia call	Voice	Multimedia call	Police control	Voice/data
34	TP4	Multimedia call	Voice	Multimedia call	NOCC Police control	Voice/data
35	TP5	Database access	Database searching	Operational database search	NOCC Police control	Data
36	TP5	Multimedia call	Voice	Multimedia call	NOCC Police control	Voice/data
37	TP7	Social media analysis	Social media	Internet access	NOCC Police control	Internet Data
38	TP8	APLS	Data applications	Location services	NOCC All PPDR personnel Police control	Location data
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
40	TP8	Multimedia group call	Group voice/data	Group call	NOCC City council	2-way Voice/Data
41	TP8	Priority Mode (MTPAS)	Mobile network prioritisation	MTPAS	NOCC PPDR Personnel	Voice/data
42	TP8	Frequency Jamming			Radio Technical Support	Radio Frequencies
43	TP8	Multimedia	Group voice/data	Multicast call	NOCC	2-way Voice/Data

No.	Ref.	Functionality	Category	Item	Actors	Information types
		multicast			Media	
44	TP9	Multimedia multicast	Group voice/data	Multicast call	NOCC Event security Transport	2-way Voice/Data
45	TP9	AVLS	Data applications	Location services	NOCC Fire Ambulance	Location data
46	TP9	Database access	Database searching	Operational database search	NOCC Fire Ambulance	Data
47	TP9	Multimedia multicast	Group voice/data	Multicast call	NOCC Covert personnel Transport	2-way Voice/Data
48	TP9	Remote control video streaming	Group video	Group video streaming	NOCC	Video data traffic
49	TP10	Multimedia broadcast	Group voice/data	Multicast call	NOCC General public	Video data
50	TP12	Sound analysis	Data applications	Sound analysis	NOCC General public	Data
51	TP12	Location services	Data applications	Location services	NOCC General public	Data
52	TP12	Pre-emptive priority	Emergency voice	Pre-emptive priority	NOCC Event security	Priority indicator 2-way voice traffic
53	TP12	Open microphone	Emergency voice	Open microphone	NOCC Event security	Priority indicator 2-way voice traffic
54	TP12	APLS	Data applications	Location services	NOCC Event security	Location data
55	TP12	Augmented reality	Data applications	Augmented reality	Event security	Mobile data traffic
56	TP12	WBAN	Data applications	Location services	Event security	Mobile data
57	TP12	APLS (wheelchair)	Data applications	Location services	NOCC Disabled public	Location data

No.	Ref.	Functionality	Category	Item	Actors	Information types
58	TP13	Live video streaming	1-2-1 video	Video streaming	NOCC Covert personnel	Live video data from officer to control room
59	TP13	APLS	Data applications	Location services	NOCC Covert personnel	Location data
60	TP13	Multimedia multicast	Group voice/data	Multicast call	NOCC Covert personnel SWAT team	2-way Voice/Data
61	TP14	Internet access	Data applications	Internet access	NOCC	Mobile data traffic
62	TP14	Live video streaming	1-2-1 video	Video streaming	NOCC Event security	Live video data
63	TP14	Database access	Database searching	Operational database search	NOCC Event security	Data
64	TP14	Multimedia multicast	Group voice/data	Multicast call	NOCC All PPDR personnel	2-way Voice/Data
65	TP14	Adhoc network and WAN handover			NOCC	
66	TP15	Fingerprint scanners	Data applications	Operational database search	SWAT team	Operational data
67	TP15	Multimedia group call	Group voice/data	Group call	SWAT team	2-way Voice/Data
68	TP16	Geo-tagging	Location services	Location services	Bomb squad	Location data
69	TP16	Live video streaming	1-2-1 video	Video streaming	Bomb squad	Live video data
70	TP16	Augmented reality	Data applications	Augmented reality	Bomb squad	Mobile data traffic
71	TP16	Remote control			Bomb squad	
72	TP16	Multimedia group call	Group voice/data	Group call	Bomb squad	2-way Voice/Data
73	TP16	APLS	Data applications	Location services	NOCC All PPDR personnel	Location data
74	TP16	Database access	Database searching	Operational database search	NOCC Event security	Data
75	TP16	Multimedia multicast	Group voice/data	Multicast call	NOCC Media partners	2-way Voice/Data

No.	Ref.	Functionality	Category	Item	Actors	Information types
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
77	DR1	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic
78	DR2	Group voice call	Group voice	Group call	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic
79	DR2	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic
80	DR2	DGNA	Group voice	Dynamic reassignment	Tactical command Police officers Fire fighters Ambulance crew Military	Configuration data
81	DR3	APLS	Data applications	Location services	Tactical command Police officers Fire fighters Ambulance crew Military	Location data
82	DR4	DMO	Group voice	Direct mode operating	Police officers Fire fighters Ambulance crew Military	2-way voice traffic
83	DR4	Transportable solutions			Tactical command Police officers Fire fighters Ambulance crew Military	

No.	Ref.	Functionality	Category	Item	Actors	Information types
84	DR4	Priority Mode (MTPAS)	Mobile network prioritisation	MTPAS	Tactical command Police officers Fire fighters Ambulance crew Military	Voice/data
85	DR5	Live video streaming	1-2-1 video	Video streaming	Air support	Live video data
86	DR5	Air to ground	Air to ground		Air support Tactical Command	2 way voice and video
87	DR6	Live video streaming	1-2-1 video	Video streaming	Tactical command Police officers Fire fighters Ambulance crew Military	Live video data
88	DR6	WBAN	Data applications	Location services	Police officers Police control Fire fighters Fire control	Mobile data
89	DR7	Group voice call	Group voice	Group call	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic
90	DR7	DGNA	Group voice	Dynamic reassignment	Tactical command Police officers Fire fighters Ambulance crew Military	Configuration data
91	DR7	Interoperability between TETRA and TETRAPOL	Group voice	Interoperability	Tactical command Police officers Fire fighters Ambulance crew	2-way voice traffic
92	DR7	Group video call	Group video	Group video streaming	Tactical command Police officers Fire fighters Ambulance crew	Video data traffic
93	DR7	Data group call	Group voice/data	Group call	Paramedics	Patient mobile data

No.	Ref.	Functionality	Category	Item	Actors	Information types
					Medical centre personnel	
94	DR8	Internet access	Data applications	Internet access	Police control room	Mobile data traffic

5 Considerations and Remarks

The interim use cases that were documented in D2.1 have through extensive PPDR user engagement across Europe been developed to a greater level of detail, incorporating the technological capabilities that are associated with each scenario. This has included monitoring and factoring-in to the requirement capture exercise and activities undertaken by CEPT and LWEP, as well as during the SALUS end user workshops [2] [4].

The feedback received in general supported the 3 use cases and the requirements captured within them for D2.4. Therefore, the use cases are deemed typical and accurately reflect the requirements of the PPDR community.

Following this deliverable the next steps will be to use these finalized use cases as inputs to subsequent work packages and tasks such as tasks 7.2. 7.3 and 7.4 in work package 7 which include the intermediate and final prototype demonstrations.

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

[10] SALUS. (2013). *SALUS Deliverable D2.4.* London: SALUS.

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

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

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

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

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

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

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

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

[22] Wikipedia. (2013). *Protests in Slovenia*. Retrieved October 2013, from Wikipedia: http://en.wikipedia.org/wiki/2012%E2%80%9313_Slovenian_protests

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

[24] 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

[25] Wikipedia. (2011). *Security for the 2012 Summer Olympics*. Retrieved November 2013, from Wikipedia: http://en.wikipedia.org/wiki/Security_for_the_2012_Summer_Olympics
[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
AIE	Air Interface Encryption
AIRBUS	Airbus (Formerly Cassidian)
AODV	Ad hoc On demand Distance Vector Protocol
AP	Access Point
ASFPG	Association Security and Fraud Prevention Group
ATHO	ATHENS Olympic Games
ATIS	Alliance for Telecommunications Industry Solutions
AUTOCON	Ad-Hoc Network Autoconfiguration
AW	Airwave Solutions
BAN	Body Area Networks
BS	Base Station
CA	Certification Authority
CCSR	Centre for Communication Systems Research
CEPT	The European Conference of Postal and Telecommunications Administrations
CISM	Computing, Information Systems and Mathematics
COSI	Standing Committee on Internal Security
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)
EOS	European Organization for Security
ERIC	Emergency Response Interoperability Center
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
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

APPENDIX 1: END USER FEEDBACK – SCENARIO 1

Question 1

Do you think the high level scenario outlined is realistic (i.e. could be real) and therefore provides a suitable base on which to develop use cases for operational deployment of functionality?

Feedback	By	Organisation
Basically „YES“ but I think “police-reality” is much more difficult and especially during demonstrations, riots,… is it very helpful to act in accordance with clear and trained patterns AND to have binding guidelines (in Austria: RFbL) [RFbL – Richtlinien für besondere Lagen – “Guidelines for special operations” (non-BAU-scenarios)] • Basic knowledge about “crowd management” • “risk analysis” • clear structures and responsibilities • (Specific organizational structure BAO [BAO is the austrian abbreviation for special operations, meaning the opposite of „business as usual“]) • prepared contingency plans in case of looting • Radio location and tracking – big problem • Austrian Police use “digital radios”, very easy to handle for all units – also for rescue and fire brigades,… • Integrated operation center (short ways) • many radios may overload the operation – or block it: could be very dangerous for the officers • offensive use of the described technology is very effective,.. • police curfew ? (Austrian law: § 49 SPG [SPG = Austrian Security Police Act])	Granig, Lt.Col.	Vienna Police
Whilst a scenario can escalate as described, the response model is overly complex and too much reliance on technology. The Control Room needs to control resources – others need to look after intelligence and operational information to ensure correct tactics discovered. Note that police public order trainesd support units are always on patrol and would be dicerted to the locality.	Tom Blair	Airwave Solutions (Previously Strathclyde Police)
This is generally what would happen in a scenario such as this	Karen Pirrie	Tactical Advisor Sussex Police
Yes. It is possible that all these technology is usable.	Raine Luukkonen	Pelastusopisto Finland (ESC)
Yes, I think this scenario could largely reflect the emergency response and the use of technology in the		Finland (ESC)

Feedback	By	Organisation
future		
Most of the technical solutions described are already used in some countries and they really help in controlling and leading the emergency troops.	Raimo Savola	Emergency Services College Finland
Yes, in my opinion, this is quite probable. The technology already exists.		Emergency Services College Finland
Document describes scenario quite good.	Geir Myhre	Norwegian Police Shared services (PSCE member)
Probably. Perhaps it´s a little to much technology.		PSCE
Yes, it's a good representation	Jim Strother	Airwave Solutions (Previously Metropolitan Police Service, UK)

Question 2

If not, what elements of the scenario need to be changed to make them more realistic or appropriate?

Feedback	By	Organisation
I think,, the elements are ok (see point 1) Finally we conclude, that for the area of the city of Vienna, but also for the rest of Austria, scenarios for occurring disasters [SKKM = national crisis and disaster prevention management] but also for incidents (up to the potential "worst-case-scenarios") in the framework of huge events, like the "Euro 2008" [Europ. Football Chamopionship] have been prepared and are also basis for actual incidents. We may also refer to the "RfbL" [Guidelines for leadership during special events => non-business-as-usual]	Granig, Lt.Col.	Vienna Police
The establishment of Command and Control. The establishment of public order tactics. The strict control of Firearms Officers and the safety of police, public and the protestors.	Tom Blair	Airwave Solutions (Previously Strathclyde Police)
The blue light services would not be the only agencies involved in this scenario, Government, military, local authorities, the voluntary sector and other key infrastructure agencies (utilities and rail etc) may also be involved, particularly in the EOC. All of these agencies will need to be communicated with and be aware of what is happening.	Karen Pirrie	Tactical Advisor Sussex Police

Feedback	By	Organisation
Social media and other public communications would be used extensively, not just to identify the ring leaders but also to send out instruction and reassurance messages, these need to be closely linked to the operation to quell rumours. Being able to quickly scan and identify key phrases to help in prioritising public communications would be important.		
The medical dispatch centre (MDC) should be notified from the beginning. The centre should be in its initial state, where it only receives updates of the situation. The video from the protest scene should also be available in the MDC where the person in charge can see it. As the situation worsens, the on-duty coordinator notifies the MDC command that raises the readiness level and dispatches several ambulances near the scene. The command structure should have been formed sooner at least by including and connecting all dispatch services. Judging from the number of wounded officers (and I assume several protestors, too), it might be sensible to initiate the “plan for massive disasters” [translation comment; I could not find a better translation for plan for massive disasters, sorry].		Medical dispatch Ljubljana
I think the scenario of enlarging riot is good	Raimo Savola	Emergency Services College Finland
Only one thing stood out, the part " 1. The fire officers consult a remote database [database access] of recommended places to cut the vehicle in order to gain access." This is currently done using a local app on a tablet and works well. Of course, it can be remote database, but the current system is not remote.		Emergency Services College Finland
14. Helicopters are set in the operation to support ground forces with video Video stream transmitted from helicopters/drones (UAV) etc to Control room and on-scene commander for oversight video and tracking (Group video) as a addition to CCTV. In many cases the on-scene commander has most use for oversight video and tracking of friendly forces.	Geir Myhre	Norwegian Police Shared services (PSCE member)
Some are wearing body armour with sensors. I think this technology will be used by the military and not the police in a long time.		PSCE
10: could add patching talkgroups which is a common requirement in these circumstances	Jim Strother	Airwave Solutions (Previously

Feedback	By	Organisation
		Metropolitan Police Service, UK)

APPENDIX 2: END USER FEEDBACK – SCENARIO 2

Question 1

Do you think the high level scenario outlined is realistic (i.e. could be real) and therefore provides a suitable base on which to develop use cases for operational deployment of functionality?

Feedback	By	Organisation
The scenario is life like. Pre Planning would cater for bomb threats. These days the venues would be secure with pre searches and strict venue control and security. Unlikely that evacuation would be ordered although not impossible. You may be evacuating into greater danger. Whilst CCTV footage is very useful, the amount of data from sensors would be significant and who would monitor? Would the sensors enhance or detract from managing the situation? Significant resource required.	Tom Blair	Airwave Solutions (Previously Strathclyde Police)
Mostly this would be the response to this type of scenario	Karen Pirrie	Tactical Advisor Sussex Police
Yes	Raine Luukkonen	Pelastusopisto Finland (ESC)
Yes, I think this scenario could largely reflect the emergency response and the use of technology in the future		Finland (ESC)
Yes it does. It's easier to preplan limited area (like stadium) security.	Raimo Savola	Emergency Services College Finland
I think this is a good scenario	Geir Myhre	Norwegian Police Shared services (PSCE member)
Probably. Perhaps it´s a little too much technology.		PSCE
Yes, comprehensive and realistic for a future scenario	Jim Strother	Airwave Solutions (Previously Metropolitan Police Service, UK)

Question 2

If not, what elements of the scenario need to be changed to make them more realistic or appropriate?

Feedback	By	Organisation
I'm not sure the NOCC would make the decision to evacuate, this is more likely to be done at a tactical level, the NOCC should be overseeing from a strategic point of view. Additional resources mentioned in point 10 are unlikely to initially go to the venue before an explosion, they would be directed to a holding point close to the venue and be directed to the venue as needed. Consideration also needs to be given to the fact that near a bomb people approaching it are advised to switch off radios/ telephones for various reasons which may impact on live streaming around suspect packages.	Karen Pirrie	Tactical Advisor Sussex Police
On the scene there should be a coordination centre with medical rescuers. However, the event is still monitored by the MDC (medical dispatch center) that also keeps monitoring the number of currently wounded and also has an overview of the capacity of nearby hospitals and the capacity of available medical transportation services. I expect that in the case of such a huge event, there should be some sort of a system of "temporary medical services" with provisional ambulances (for instance in tents). If the number of injured exceeds some threshold, the plan for massive disasters should come into effect: the establishment of sectors (red, yellow, green, black). Based on the level of threats, the teams would be divided into groups that operate in field, in various sectors, teams that take care of transport to hospitals, etc. While the sensors to monitor vital signs are appealing, I am not sure who will monitor their readings if we wire up, for instance, 20 persons: a hospital (which), the coordination centre? What kind of data can be obtained? How do hospitals (doctors) react, if it founds out that someone is losing his pulse? Who is brought in to react?		Medical dispatch Ljubljana
Is it realistic that all spectators fingerprints are scanned before entering stadium?	Raimo Savola	Emergency Services College Finland
Helicopters are set in the operation to support ground forces with video. Especially in Norway CCTV is not very commonly used Video stream transmitted from helicopters to Control room and on-scene commander for oversight video and tracking	Geir Myhre	Norwegian Police Shared services (PSCE member)

Feedback	By	Organisation
(Group video) as a addition to CCTV. In many cases the on-scene commander has most use for oversight video and tracking of friendly forces. Very often in this kind of scenario there will be flying restrictions over the stadium for drones and UAVs since those are very hard to control. It is easier to control helicopter traffic in an area. In our organization we have more on-scene responsibility, the on-scene commander takes more tactical decisions and needs information to do that. Control rooms have more responsibility for the strategic work.		
Some are wearing body armour with sensors. I think this technology will be used by the military and not the police in a long time.		PSCE

APPENDIX 3: END USER FEEDBACK – SCENARIO 3

Question 1

Do you think the high level scenario outlined is realistic (i.e. could be real) and therefore provides a suitable base on which to develop use cases for operational deployment of functionality.

Feedback	By	Organisation
This is a very large operation that will require military assistance to the civil power very quickly – including their communications capabilities. Military assistance will take hours running into day or more to deploy. You cannot command a huge area. Applying the principles of command and control, the geography would very quickly be sectorised with their own tactical commands and a joint a joint strategic command.	Tom Blair	Airwave Solutions (Previously Strathclyde Police)
This would generally be the way that this type of scenario would be dealt with and the potential consequences are likely.	Karen Pirrie	Tactical Advisor Sussex Police
The scenario accurately reflects the emergency response. Considering the vastness of the disaster, we would also put the plan for massive disasters into practice (these plans are adopted based on the size of the disaster). Additional medical forces are expected to be used, particularly the first responders, which should be equipped with devices that connect them to the central. I expect the army forces to cooperate, since they have very capable in-field medical facilities. I particularly like the idea of having several layers of leadership at common locations.		Medical dispatch Ljubljana
The scenario accurately reflects the real-life situations. Our main concern is that the police usually does not lead (or is in charge of) the intervention. In Slovenia, the civil (and other public) protection in case of such disasters is organized and executed as a single, unified entity. Such operations would be led by commanders of the Civil protection, command centres of Civil protection, commissioners of Civil protection and commanders or unit leaders of various PPDR services.		Slovenian Fire Brigade Association
Yes	Raine Luukkonen	Pelastusopisto Finland (ESC)
Yes, I think this scenario could largely reflect the emergency response and the use of technology in the		Finland (ESC)

Feedback	By	Organisation
future		
This scenario reflects how vulnerable technology can be in case of big catastrophe.	Raimo Savola	Emergency Services College Finland
Yes. I suppose the helicopter and drone video are not thought of as being real time. This would require network which is not available.		Emergency Services College Finland
We do not feel this scenario is consistent. In one point network is down and new deployed network can only support highly critical data, in next point video from body camera is supported. In this scenario data to control room will not be supported. Local site trunking and local command centres in the close area will be decision makers on critical decisions, and simple communication ways like satellite phones will be used to control rooms and the strategic decisions. From a Norwegian point this is hard to imagine this scenario happen. We have other scenario where avalanche of snow/ parts of mountains can fall and create moving of landmasses and locale “tsunami” waves in the fjords	Geir Myhre	Norwegian Police Shared services (PSCE member)
Yes	Jim Strother	Airwave Solutions (Previously Metropolitan Police Service, UK)

Question 2

If not, what elements of the scenario need to be changed to make them more realistic or appropriate?

Feedback	By	Organisation
Whilst it is possible for the rail element to take place. These days it is doubtful that rail services would still be operating after a day (certainly in the UK) and I would imagine Europe.	Tom Blair	Airwave Solutions (Previously Strathclyde Police)
I would be surprised if the military were called and arrived within two hours of this scenario occurring, depending on which country it was. The military would usually be a last resort and would be called in later if at all. The agency designated for management of rest centres and supplies (In the UK the local authority) would be much more involved. In addition a casualty bureau with different numbers would be set up to try and field calls particularly around concerned relatives trying to find family/ friends. This may receive important info which needs to be fed back into the EOC Transportable solutions using just 4x4's may not work. The area is flooded and they are unlikely to get to some areas they need to, they may also become damaged by flooding or mud slides etc The train incident would have significantly more resources involved in it from various agencies and the private sector, the train companies themselves and whoever owns the rail network. It is likely that for this event the medical side would implement their major incident plans and have triage centres and Dr's at site, calling back to the control room for medical advice may not happen, they may need to for particularly critical cases contact the hospitals they are going to keep them informed of the patient's condition and treatment.	Karen Pirrie	Tactical Advisor Sussex Police
For medical purposes, the medical response centre (MRC) monitors the need for medical assistance and assists the coordinator that is located in-field.		Medical dispatch Ljubljana
Such operation would be led by the operational command centres, which would be staffed with representatives from various PPDR services (firemen, police, ambulance workers, military, and other representatives of various PPDR services that might be needed on site, such as speleologists, mountain rescue services, red cross representatives, etc). The main person in charge of the command centre is called the "intervention lead". She/he is authorized by the law.		Slovenian Fire Brigade Association

Feedback	By	Organisation
At the level of municipalities, regions and finally the state, headquarters of public protection would be established, in order to coordinate the work of PPDR forces. These headquarters would be staffed with experts from various fields and representatives of various PPDR forces. These people would largely benefit from the described network and the applications in this scenario.		
Maybe something about possible backup systems for different technical solutions.	Raimo Savola	Emergency Services College Finland
Why CCTV cameras on drones?		Emergency Services College Finland
Sensors placed strategically will report data to CR as changes in Water level (SCADA)	Geir Myhre	Norwegian Police Shared services (PSCE member)

APPENDIX 4: MATRIX OF PUBLIC ORDER EVENTS

Item	Scenario 1	Scenario 2	Scenario 3
2010 Slovenia floods [14]			✓
Earthquakes in Slovenia (1998 and 2004)			✓
Protests in Slovenia (2013) [22]	✓		
Enschede fireworks disaster (13 May 2000)	✓		
Turkish Airlines flight 1951 crash (Schiphol, 25 February 2009)	✓		
Royal Wedding UK [24]		✓	
Ski-World Championship 2013, Schladming, AUSTRIA [26]		✓	
Floods (Germany, Czech, Hung, Aus)			✓
England Riots 2011 [17]	✓		
2012 Olympics and Paralympics (Jul, Aug, Sept 2012) [20] [25]		✓	
Boscastle floods of 2004 (Boscastle, Cornwall, England) [16]			✓
Buncefield Fire, Buncefield, Herts, England Dec 2005	✓		
Grayrigg derailment, 2009 Cumbria England [18]	✓		
7/7 bombing London, England [15]	✓		
The Coronation of Holland's King Willem-Alexander [13]		✓	
Attack on the Dutch Royal Family (Apeldoorn, 30 April 2009)	✓		
Riots beach of Hoek van Holland [23]	✓		
Nuclear reactor going out of control	✓		
Serious radiation leak	✓		
Lockerbie aircraft terrorist attack	✓		
Snow storm of 25 November 2005 [8]			✓
Nuclear Security Summit 2014		✓	
Project-X Haren (21 September 2012) [21]	✓		
International Four Days Marches Nijmegen (Mid July every year)	✓	✓	
Rotterdam Marathon (April every year)		✓	
SAIL Amsterdam (every 5 years; next time August 2015)		✓	
Pinkpop Festival (Landgraaf, every year in the Pentecost)		✓	
Life I Live festival (The Hague, every year)		✓	
Serious Request (every year in Christmas)		✓	
Kings Cross Fire [19]	✓		
Hyde Park Bombings 1982, London	✓		
Notting Hill Carnival, London, every year over the August bank holiday	✓		
New Years Eve celebrations in London	✓		