System and Architecture of an Adapted Situation Awareness Tool for First Responders

Debora Robles Perez[*]
Communications Department – Universitat Politècnica de València
derobpe@upvnet.upv.es

Manuel Esteve Domingo
Communications Department – Universitat Politècnica de València

Israel Perez Llopis
Communications Department – Universitat Politècnica de València

Federico J. Carvajal Rodrigo
Communications Department – Universitat Politècnica de València

ABSTRACT

First responders (FRs) in Europe are currently facing large natural and man-made disasters (e.g. wild fire, terrorist attacks, industrial incidents, big floods, gas leaks etc.), that put their own lives and those of thousands of others at risk. Adapted situation awareneSS tools and taIlored training curricula for increaSing capabiliTies and enhANcing the proteCtion of first respondErs (ASSISTANCE) is an ongoing European H2020 project which main objective is to increase FRs Situation Awareness (SA) for helping and protecting different kinds of FRs' organizations that work together in large scale disasters mitigation. ASSISTANCE will enhance the SA of the FRs organisations during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with a range of sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency.

Keywords

Critical Infrastructure Protection, First Responder, Command and Control, Autonomous Vehicles, Resilience.

INTRODUCTION

ASSISTANCE presents a holistic solution that will adapt a well-tested Situational Awareness (SA) application as the core of a wider SA platform. The ASSISTANCE's platform will be capable of offering different configuration modes for providing the tailored information needed by each FR organization while they work together to mitigate the disaster (e.g. real time video and resources location for firefighters, evacuation route status for emergency health services and so on). This Work in Progress (WiP) Paper is organized into 4 main sections. The first of these sections outlines a brief review of relevant literature and related work, which will be analyzed displaying actual technical advances in SA areas. Reviewing the state of art leads ASSISTANCE to a solution that will enhance the SA of the responding organizations during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with a range of sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency. In addition, the project is extremely focused on tangible solutions, which will lead to on field testing. As a consequence, ASSISTANCE project proposes 3 demo pilots, that will be shown in the next section, for ensuring its results validation in controlled environments with all consortium end users direct involvement. The description of the pilots will be contextualized by real disaster use-cases. Following, a section explaining the ASSISTANCE system and architecture will be detailed, designed on the outcomes of several questionnaires filled in during the preparation phase by 18 FRs European organizations in terms of self-protection and capabilities enhancement. The user requirements comprise

---

[*] Corresponding author

mainly functional demands, but FRs users also specified non-functional requirements identifying physical or performance characteristics. ASSISTANCE project will use robots and drones' swarms, UAVs and smart wearable sensors, all equipped with specific sensors for covering the FRs specific data needs. The sensors mounted on unmanned platforms along with the ones mounted on the FRs' equipment will be integrated in a complete Situation Awareness Platform (SAP) that will also include innovative modules that will improve the FRs' SA and capabilities for performing their work in a more efficient and secure manner. Furthermore a description of the ASSISTANCE network architecture will be discussed presenting a high-level overview of the three main segments. Overall, WiP last section displays a conclusion comments to the current ASSISTANCE system.

RELATED WORK

In this section, we review and summarize a few research and commercial disaster management information systems used by different FRs Organizations for increasing ASSISTANCE's current capabilities enhancing their SA. It should be noted that, in order to compare our system as objectively as possible, the following projects or software pursue ASSISTANCE's similar goals. ALADDIN (2017-2020) is a European Commission (EC) H2020 call ongoing project dedicated to neutralize drones, but focused in protecting critical infrastructures. In addition, the main research of ALADDIN is regarding detection and tracking using complex formats for its neutralization. ASSISTANCE instead is focused on providing a tool for FRs in order to protect them during the mitigation of a large event in an easy way to use. ICARUS (2012-2016) was a EC FP7 call project aimed to decrease the total cost, both in human lives and in expenses terms, of a major crisis. Their approximation was based on the use of unmanned platform for rescue victims. ASSISTANCE will use a wider range of different UAVs, drones and robots adapted to the FRs information needs in different scenarios for increasing their SA and protect them against unexpected dangers. In addition, the SA capabilities proposed in ASSISTANCE goes beyond to the Command, Control, Communications, Computers, & Intelligence (C4I) system developed in ICARUS, since their C4I only acts as integration platform without offering any added value to the FRs Organizations as for example the FRs Wearable Sensors, UAV&Drones' Advanced Capabilities, Augmented Video Fusion and so on. *DragonForce DRAKONTAS* (n.d.) is a commercial mobile team collaboration platform that delivers mission-critical command and control and incident management capabilities in real time. As in ASSISTANCE it integrates real-time personnel tracking, instant text messaging among individuals and groups, plus online storage and data sharing capabilities, digital forms and situation reports, and an interesting team capability that turns any map, picture or floor-plan into a shared whiteboard. Homeland Security (2016) application is a counter explosive tool that puts key decision making data, such as safe standoff distances, damage and injury contours, nearby areas of concern, and suggested roadblocks, directly at responders' fingertips. As a disadvantage, it lacks of user and group communications. *IMPACT* (n.d.) is a Geographical Information System (GIS) tool easy to use by non-GIS professionals as first responders, designed to enhance SA, communication, preparedness and coordination for security events. FRs can use it for planning, situation awareness, and response to natural and man-made disasters for *Impact Examples* (n.d.): wildfire monitoring, plume model, evacuation plans, line-of-sight, evacuation simulation among other. ASSISTANCE will benefit and continue from IMPACT achievements. *CommandX* (n.d.) is a commercial system for emergency communications where a workplace can communicate with multiple instances locally or via a network connection. As in ASSISTANCE situation map is running on the communication server, making possible that multiple users can access it simultaneously, with an important difference, CommandX works with ArcGIS by *ESRI* (n.d.), a proprietary geodata infrastructure.

USE CASES AND PROPOSED PILOTS

Among the increasing natural or man-made disasters FRs' ASSISTANCE potential will be tested using the following use-cases: Earthquake, industrial accident and terrorist attack; although in each pilot we will be focusing in different innovative modules that will enhance and secure FRs' SA beyond the state of the art, all the system would be tested. In this section, we summarize the Use-Cases (UC) and the Pilots (P) scenarios, where each pilot will be led by a different type of FRs organization, while the others consortium FRs will cooperate with them as in a real disaster.

UC1 Earthquake. In 2015, Nepal suffered a 7.8 (in the Richter scale) magnitude earthquake, damaging the local telecommunications infrastructure, showing up difficulties within the Government's Emergency Response (Shrestha and Pathranarakul 2018). Coburn and Spence (2003) suggested that having a pre-earthquake emergency plan can be one of the best ways to ensure an effective response. Nevertheless, emergency plans should be realistic and pragmatic (Alexander 2015).

P1 Earthquake (Izmir, Turkey). The beginning situation for this pilot is that a 7.8 magnitude earthquake like in Nepal strokes urban environment during the night time. Therefore, many buildings have collapsed or are severely damaged and main commercial communication networks have been heavily affected.

Network coverage will be provided by Ad Hoc network using drones' swarm equipped with Wi-Fi access points. Victims have to be transported to the available hospitals. Information on optimal routes, which include real-time information on damaged infrastructures and CBRN Hazard module will be tested. Last one will be mounted on unmanned platforms (drones or robots) and will project on a GIS thought layers' potential hazard footprints in real time.

UC2 Industrial Accident. The largest industrial catastrophe in history took place in 1984 in Bhopal(Labaka et al. 2013), India, through a gas leak. Many FRs died and the rest of them got overwhelmed handling the situation occurred due to the lack of several technical capabilities. To mention a few: troubles identifying the gas type, lack of resources or adequate transport and routing for emergency evacuations (Bisarya and Puri 2005).

P2 Industrial accident (Rotterdam Rijnmond area, The Netherlands). A big fire is developing in a chemical warehouse destroying various chemical products, producing large amounts of potentially toxic fumes.

CBRN Hazard module will project on GIS layers gas cloud dispersion models and/or toxic footprint predictions continuously updated by measurements from sensors mounted on unmanned platforms. This way, FRs will increase their protection and it will allow them to correctly inform, alarm or even evacuate specific areas.

UC3 Terrorist attack. On 21 April 2019, Easter Sunday, in 20 minutes, eight coordinated bombs went off in popular hotels and historical churches across Colombo. Later in the day, there were smaller explosions at a housing complex and a guest house, killing mainly police officers who were investigating the situation raiding suspect locations (Amarasingham 2019). Another issue to deal with in terrorist attacks as in Manchester bombing 2017 (Mirbabaie et al. 2018) is that often disrupt communications infrastructures, through either damage or other actions of the belligerents. Such riots also affect the development and extension of telecommunications infrastructure.

P3 Terrorist attack (Seville, Spain). During the Seville Feria's week, with a 3,5 million people attending, a truck crash in the Maestranza bullring (2km distance from the feria enclosure) and a big explosion takes place; panic starts. Many calls arrive to the emergency services with breathing difficulties or troubles escaping. Two unknown drones are within the area. These facts alert the FRs on the potential presence of a toxic agent/substance and maybe malevolent drones in the area. Ten minutes later when all LEAs resources are focused in the bullring area trying to know what has happened, a suspicious tank truck is detected going very quickly to the direction of the feria main entrance, where a large crowd is being evacuated.

FRs on field will use the HMI in order to lock the drones as a target and after that a friendly drone duly modified will follow the suspicious drone automatically and will performs its interception through the use of net launched. Mission management module will allow to improve the collaboration between the FRs and the asset and payload operators at this evolving scenario, giving them a full awareness situation, preventing second attacks.

ASSISTANCE SYSTEM AND ARCHITECTURE

ASSISTANCE System

The sensors mounted on unmanned platforms along with the ones mounted on the FRs' equipment will be integrated in a complete SA platform that will also include innovative modules that will improve the FRs' SA and capabilities for performing their work in a more efficient and secure manner. Additional capabilities for using drones as active FRs' tools, instead of only as unmanned platforms for mounting sensors, will be also developed such as the mentioned from the pilots: Hostile drone neutralization, provision of network coverage through the use of swarms of drones or location and routing.

SAP core will be adapted based on the civil version of the Spanish Army Friendly Force Tracking (SIMACET-FFT) system developed by UPV partner, and currently deployed in several international missions. This system is a complete SA solution capable of integrating a wide range of sensors and offering advanced SA and Command and Control (C2) capabilities. ASSISTANCE will use some of these preexisting SA capabilities in its core platform, which will be tailored and updated during the project. In addition, innovative SA modules/capabilities will be developed for being integrated in this core platform in order to build the whole ASSISTANCE SA platform. SAP high level design schema is shown in Figure 1. The existing modules included in the core application are depicted in blue color and the new ones that will be developed during the project in red color. The information represented in the SA Platform HMI will change depending on the active function mode selected, which will be associated to the information needs of each concrete type of FRs organizations (e.g. firefighters, LEAs, medical staff) according to their expressed needs.

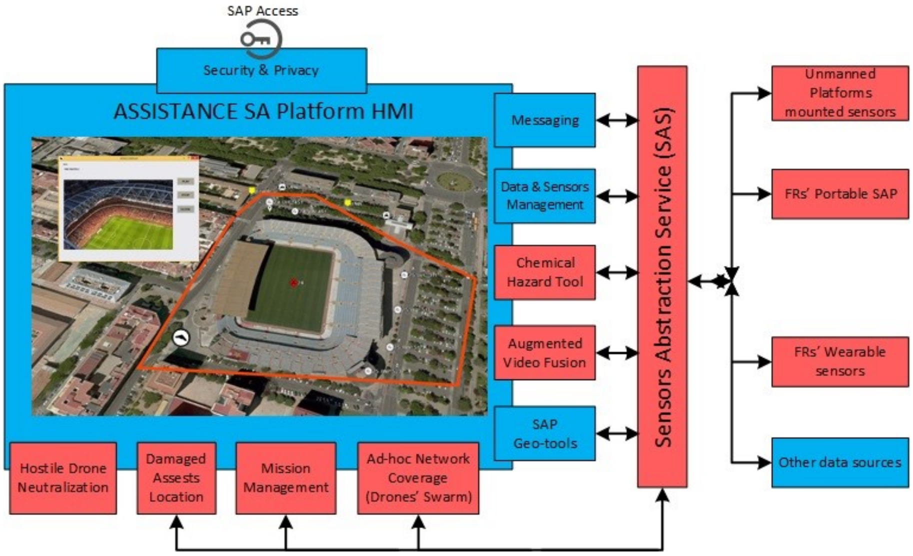

Figure 1. SAP high level design schema

System Design

In this subsection ASSISTANCE's overall system information exchanges will be described in terms of individual information exchanges between pairs of modules/sub-systems. Each individual information exchange between a pair of entities will be named as a "communication service". The overall ASSISTANCE data model has been designed describing the different objects and their corresponding attributes that will model all data exchanged among the ASSISTANCE modules.

This overall data model has been designed in an agnostic manner paying attention to the data characteristics and the needs of the different modules/sub-systems involved in each information exchange. In order to make easier the understanding of each individual information exchange, the overall data model has been divided in parts according to the data needs of the modules/sub-systems involved in each information exchange. Thus, data models described for each individual information exchange form part of the overall ASSISTANCE system data model. It is important to note that, as stated in the Architecture, all information exchanges in ASSISTANCE system will be performed through the Sensor Abstraction Service (SAS) module, which will provide a homogeneous manner of exchanging all necessary data among the different ASSISTANCE modules/sub-systems.

The communication services described will follow the schema stated in Figure 2. That means starting from the sensors part and showing how sensors and resources (e.g. UxV, vehicles, persons) information is gathered by the SAS and distributed among all systems that need this data. After that, bilateral data/information exchange between the rest of the modules will be also described.

SAS Communication Services

SAS is the overall middleware used in ASSISTANCE for all data exchange among the different ASSISTANCE system components. Therefore, in order to simplify the design of the different data exchanges, the SAS will be taken as a transparent component in all bilateral modules' information exchange between ASSISTANCE subsystems. e.g. (SAP to CHT, MMM to Drones base stations and SAP to DALR). SAS will be only shown as a module when the information exchanges involves directly the SAS and other module e.g. Sensors-SAS. The communication process between the SAS and the rest of the systems, includes different protocols depending on each case. This overall information exchange is described graphically in the Figure 3.

ASSISTANCE Architecture

The ASSISTANCE system comprises the full integration of all modules/components, which will produce a synergy driving ASSISTANCE beyond the current FRs SA perception. The overall ASSISTANCE architecture, its components, interactions and information flows are described in figure 2. The SAP will receive information from different sensors and systems and will integrate all this information, showing it in a tailored manner through its main HMI, to the different FRs that will use the platform. On the other hand, different ASSISTANCE modules and systems will receive information from sensors and different sources for performing their internal process and will send these processes results to the SAP. The information exchange paradigm that has been selected by

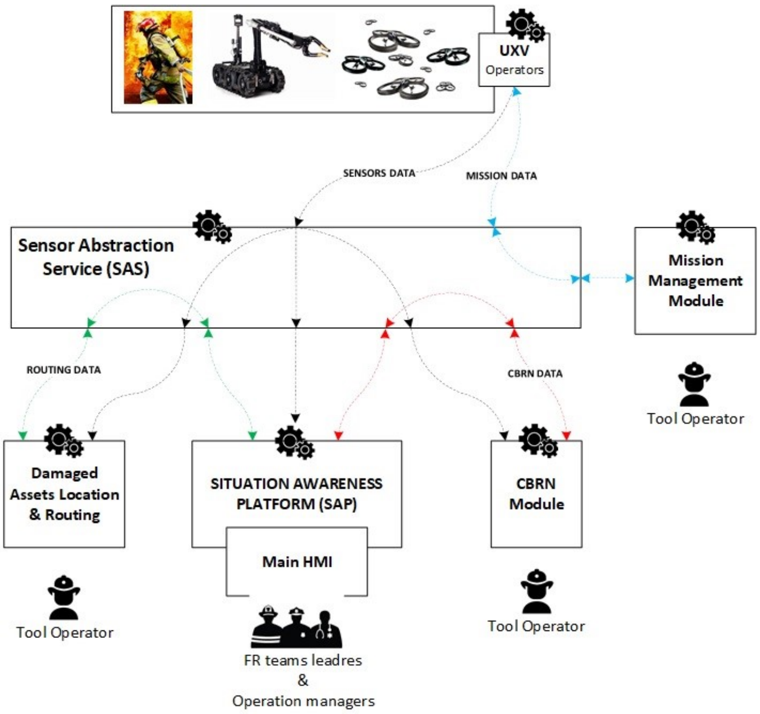

Figure 2. ASSISTANCE Architecture Schema

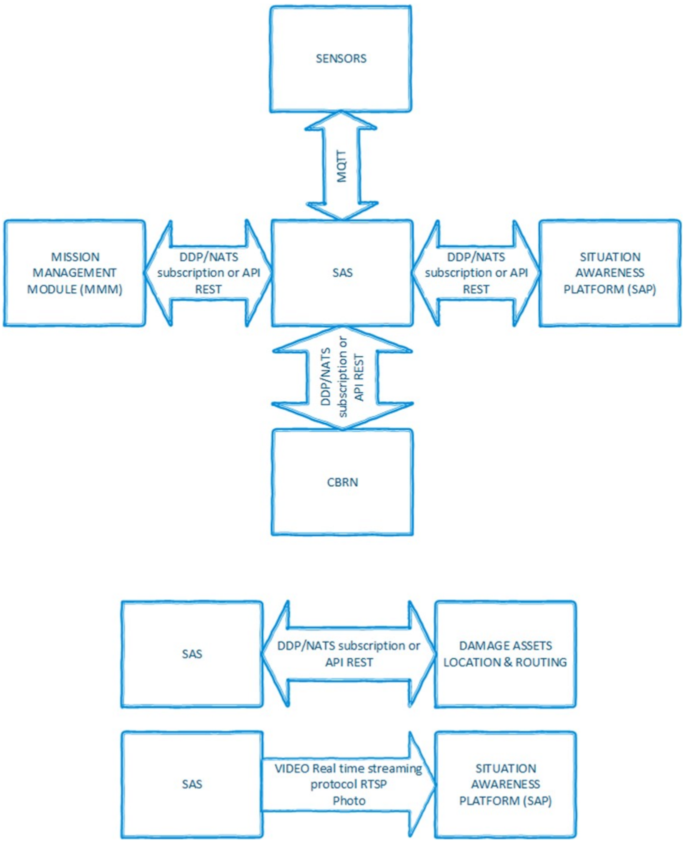

Figure 3. Modules involved in the SAS communication process

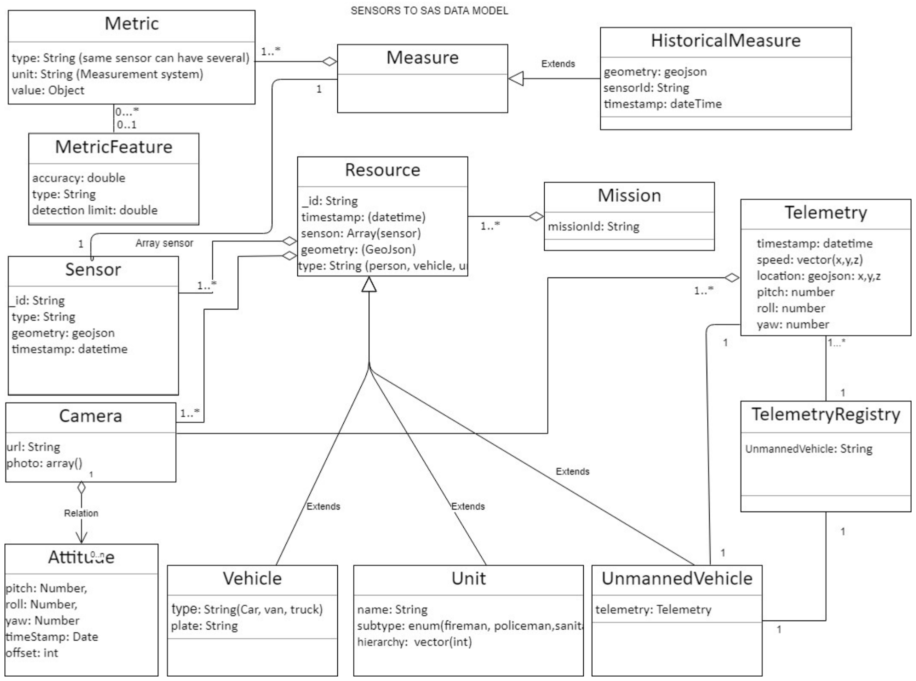

Figure 4. Data model of the information offered by SAS related to sensors, drones and units deployed

ASSISTANCE for the different modules and systems integration is a publish/subscribe approach performed through the SAS. Micro services architecture has been chosen because its simplicity, its improved productivity, and because it is also autonomous and scalable (Uckelmann et al. 2011). The data from sensors will be collected through a secure *MQTT* version protocol (Chien et al. 2019; Singh et al. 2015) directly from the sensors, then data will be published to the SAS or to any subsystem subscribed to the publish/subscribe MQTT topic protocol of the sensor. Once inside the SAS data will be shared to the different subsystems using several technologies cited as follow: Web sockets (Reddy et al. 2019), Distributional Differential Privacy (DDP) or Network Address Translation (NATS) (Frew et al. 2008) protocol, that allows publishing in real-time to a web site as it uses the publish-subscribe messaging pattern.

SAS Data Model

SAS data model, could be inferred from figure 4 Where the central element is the Mission, that can have *n* resources such as a vehicle, unit or unmanned vehicle, which will acquire field data from the sensors, acting as an abstraction layer.

SAS Data Collection

The Data Collection System (DCS) connects the available sensors using the MQTT protocol by means of a subscription to the topic of each sensor. DCS will gather the data from each sensor each time the data changes and will store the data in the SAS database and then all systems subscribed to these data will receive this updated information.

SAS Data Delivery System

The Data Delivery System (DDS) is the part of the SAS in charge of sending the information to all modules/subsystem subscribed or on demand. The subscription will be performed through real-time Web Socket using DDP or NATS real time server, these two technologies have been chosen because they are complementary.

SAS Data Inputs and Outputs

Also according to Figure 2, SAS will receive all information from the sensors stated in the system and will publish it in a standard manner for being processed by the different ASSISTANCE modules/systems subscribed to the corresponding real-time Web Socket DDP/NATS or API REST methods.

ASSISTANCE NETWORK LAYER

One of the main goals of ASSISTANCE is to establish reliable, resilient, robust and secure connectivity between sensors, UxVs, field units, advanced C2 centers and the rear C2 centers. The overall ASSISTANCE communication solution is based on a secure hybrid network approach that will provide high availability in remote areas outside of the coverage area of common communication networks and/or areas where these networks were disabled due to an emergency event. The hybrid network will provide the necessary availability and data rates within the latency constraints in order to support the large set of interactions between the field operators and the advanced and rear C2 centers in time-critical missions.

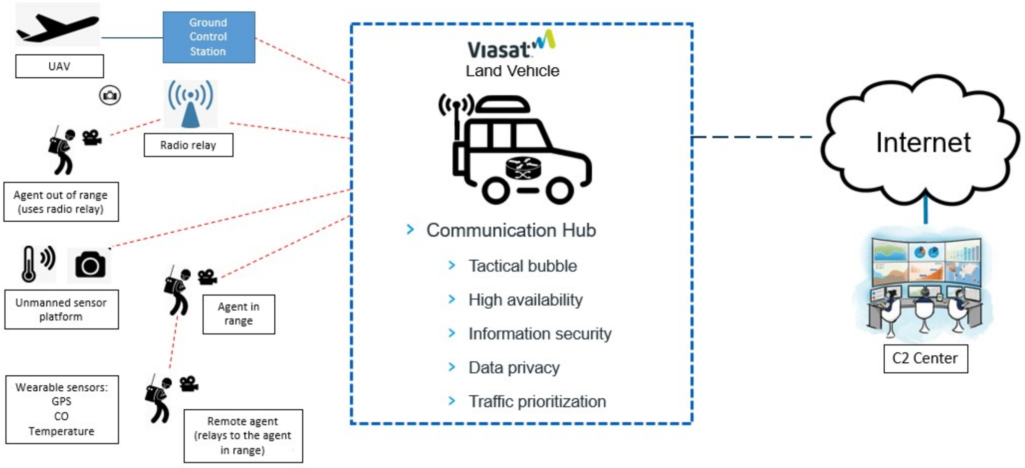

Figure 5. ASSISTANCE network architecture schema

This section details a description of the ASSISTANCE network architecture with Figure 5 presenting a high-level overview of the three main segments: *Radio network* presents the last-mile network that connects the FRs, UAVs and unmanned sensors to the communication hub. *Communication hub* is the Land Vehicle that acts as the backhaul network, i.e. the communication node which connects the radio network to the C2 center via the Internet. *Command and Control Center* is the entity that has a global view and control of all the components of the ASSISTANCE project.

1. Radio Network

The main goal of the radio network is to provide connectivity to field operators (first responders), UAVs and unmanned sensors in remote operation areas which are out of coverage of common communication networks for whatever reason, for instance due to infrastructure unavailability as a consequence of the disaster where ASSISTANCE is going to be deployed. Furthermore, this radio network has to provide high range connectivity to stationary and highly mobile units with low latency for time-critical missions. This can be accomplished by deploying a self-forming/self-healing Mobile Ad Hoc Network (MANET) (Chlamtac et al. 2003) in control applications, which provides mission critical video, voice, Situational Awareness, and data sharing without depending on an established infrastructure. The MANET is established between radios which are available in full-featured handheld (equipped on the FRs) and vehicular configurations, as well as small form factor modules for easy integration into unmanned systems (equipped on the UAVs and drones). In addition to the audio channels, each radio module is able to stream multiple High Definition videos (16 Mbps IP Throughput), as well as acting as a relay to other radios in range, thus creating a mesh radio network with a large range (20 km Line of Sight (LOS)) per network Hop). The radio modules (equipped on first responders and UAVs) will send or relay all the data streams to the communication hub, from where the traffic will be routed to the C2 center. Moreover, the communication hub provides different network interfaces for the end users to connect via an Ethernet or optical cable.

2. Communication hub

The communication hub connects the radio network to the C2 centers by using two different networks: traditional Long Term Evolution (LTE) (Deruyck et al. 2016) network and Satellite network. This allows the communication hub to use the high bandwidth LTE network when the vehicle is in LTE coverage area and switch to using a consortium partner satellite network in cases when there is no LTE coverage, which is very common for the use

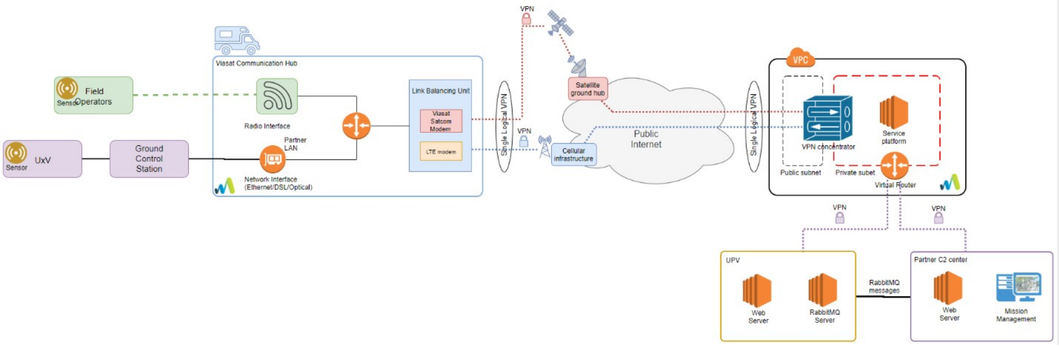

Figure 6. Detailed schema of the ASSISTANCE network architecture

cases in the ASSISTANCE project. Thus, providing high reliability and availability even in rough terrains and changing conditions. Figure 6 illustrates a detailed schema of the ASSISTANCE network architecture.

Link failover In order to ensure reliability and availability in different network scenarios, two separate VPN tunnels (one over LTE and the other over the Satellite link) will be established between the Link Balancing Unit on-board the communication hub (vehicle) and the VPN concentrator hosted in a Virtual Private Cloud (VPC) which terminates the VPN tunnels. The Link Balancing Unit and VPN concentrator manage the VPN tunnels in order to provide Active/Standby failover between the two links (LTE and Satellite). The VPN tunnels act as a single logical VPN tunnel by performing packet-based fail-over between the links. This means that the established sessions are maintained in the case of a link failure and don't need to be re-established (stateful failover).

3. C2 Centers

In the ASSISTANCE pilots' deployments there will be two different kinds of C2 centers, the advanced C2 center and the rear C2 center. The advanced C2 center will be deployed on field and it can be composed by one or several laptops that directly take information from sensors deployed on field and use this information for taking tactical decisions and also for protecting the units deployed on field. It is possible that different kinds of FRs have their own advanced C2 center on field. The rear C2 center is the entity that has a global view and control of all the components of the ASSISTANCE system which means that it is crucial that the data exchange complies with strict security and latency requirements. This can be achieved by establishing and end-to-end VPN connection between the C2 center and the communication hub. Each ASSISTANCE partner can establish a VPN to the VPC which will enable the bidirectional data exchange with the ASSISTANCE remote components (field operators, UAVs, sensors).

CONCLUSION

In this wiP paper we have reviewed how ASSISTANCE will preserve FRs as well as will enhance their SA during disaster mitigation, in a wide range of use-cases, even in remote areas or through a commercial networks failure, due to the novel architecture and mechanisms proposed. It has been stated a system architecture for ongoing disaster that facilitates with a tailored SAP which supports FRs management depending on each organization needs, reflecting the real state of the event over the integration of new paradigms, tools and technologies.

ASSISTANCE is fully oriented to validate its capabilities in real scenarios, approaching real use-case with similar pilots, testing the overall system capabilities by the FRs consortium partners. First Responders' on field feedback will allow the consortium to correct potential technical errors in order to improve the system for the final project pilot demonstration and a future paper with tangible results.

ACKNOWLEDGMENTS

ASSISTANCE is funded by the Horizon 2020 Program of the European Commission, in the topic of Critical Infrastructure Protection, grant agreement 832576.

REFERENCES

ALADDIN (2017-2020). *H2020 ALADIN, Advanced hoListic Adverse Drone Detection, Identification & Neutralization*. `https://aladdin2020.eu/`.

Alexander, D. E. (2015). “Disaster and emergency planning for preparedness, response, and recovery”. In: Oxford University Press.

Amarasingham, A. (2019). “Terrorism on the Teardrop Island: Understanding the Easter 2019 attacks in Sri Lanka”. In: *CTC Sentinel* 12.5.

Bisarya, R. and Puri, S. (2005). “The Bhopal gas tragedy—a perspective”. In: *Journal of Loss Prevention in the Process Industries* 18.4-6, pp. 209–212.

Chien, H.-Y., Kou, X.-A., Chiang, M.-L., and Su, C. (2019). “Secure and efficient MQTT group communication design”. In: *International Conference on Computational Science/Intelligence & Applied Informatics*. Springer, pp. 177–186.

Chlamtac, I., Conti, M., and Liu, J. J.-N. (2003). “Mobile ad hoc networking: imperatives and challenges”. In: *Ad hoc networks* 1.1, pp. 13–64.

Coburn, A. and Spence, R. (2003). *Earthquake protection*. John Wiley & Sons.

CommandX (n.d.). `http://www.eurocommand.com/en/comprehensive-solutions/commandx-all-inclusive.php`.

Deruyck, M., Wyckmans, J., Martens, L., and Joseph, W. (2016). “Emergency ad-hoc networks by using drone mounted base stations for a disaster scenario”. In: *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, pp. 1–7.

DragonForce DRAKONTAS (n.d.). `https://www.drakontas.com/index.php/dragonforce/`.

ESRI (n.d.). `https://www.esri.com/es-es/home`.

Frew, E. W., Dixon, C., Elston, J., Argrow, B., and Brown, T. X. (2008). “Networked communication, command, and control of an unmanned aircraft system”. In: *Journal of aerospace computing, information, and communication* 5.4, pp. 84–107.

Homeland Security, D. of (2016). *FiRST, First Responder Support Tools*. `https://www.dhs.gov/publication/first-responder-support-tools-first-application`.

ICARUS (2012-2016). *FP7 ICARUS, Integrated Components for Assisted Rescue and Unmanned Search operations*. `http://www.fp7-icarus.eu/`.

IMPACT (n.d.). `https://geo.ornl.gov/impact/index.html`.

Impact Examples (n.d.). `https://geo.ornl.gov/impact/docs/IMPACT_Examples.pdf`.

Labaka, L., Hernantes, J., Laugé, A., and Sarriegi, J. M. (2013). “Enhancing resilience: implementing resilience building policies against major industrial accidents”. In: *International Journal of Critical Infrastructures 6* 9.1-2, pp. 130–147.

Mirbabaie, M., Bunker, D., Deubel, A., and Stieglitz, S. (2018). “Examining convergence behaviour during crisis situations in social media-a case study on the manchester bombing 2017”. In: *International Working Conference on Transfer and Diffusion of IT*. Springer, pp. 60–75.

MQTT (n.d.). `http://mqtt.org/`.

Reddy, P. B., Reddy, A., Reddy, V. V., Sarath, C. S., and Manikandan, K. (2019). “Real-time monitoring system (websocket-based) for remote intelligent buildings”. In:

Shrestha, B. and Pathranarakul, P. (2018). “Nepal Government’s Emergency Response to the 2015 Earthquake: A Case Study”. In: *Social Sciences* 7.8, p. 127.

Singh, M., Rajan, M., Shivraj, V., and Balamuralidhar, P. (2015). “Secure mqtt for internet of things (iot)”. In: *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, pp. 746–751.

Uckelmann, D., Harrison, M., and Michahelles, F. (2011). “An architectural approach towards the future internet of things”. In: *Architecting the internet of things*. Springer, pp. 1–24.