PSCE WHITE PAPER 3

Security and interoperability in next generation PPDR Communication infrastructures: Enterprise and System Architecture

Source: SALUS project

PSCE: Future of public safety communications

To solve the complex challenge of building efficient future PPDR networks that will integrate existing and new technologies and will have as major objectives to enhance operational effectiveness and improve interoperability between agencies from home and neighbouring countries, a robust methodology is required. SALUS approach is to use the Enterprise Architecture (EA) which has been successfully used in complex domain such as defence. Indeed, the guiding principle of the EA is to support the adaptation of the "business" to benefits from new technologies and to exploit the (new) technologies to better support the "business".

The document gives a first cut at the SALUS Enterprise Architecture reflecting the Use Case scenarios related to the "City Security, Temporary Protection, Disaster Recovery" and covering the most important and challenging missions of PPDR organisations and where the use of an efficient system is paramount. The SALUS EA is based on the Open Safety and Security Architecture Framework (OSSAF) and on NATO Architecture Framework (NAF). For the sake of simplicity, this document addresses a reduced number views from the four perspectives defined by OSSAF:

- Strategic perspective: focusing only a the 'capability planning'
- Operational perspective: developing operational node concepts and information exchange models,
- Functional model: developing systems and services (focusing on application services and technical services), their functional requirements and their connectivity model and their interface,
- Technical view: focusing on solution, standards and protocols, and device connectivity models.

Indeed, moving from one perspective to the next level gives more granularities on the way the system will operate. It is to be noted that from all the capabilities and services required for future PPDR system, this document (which is the Intermediate version of the SALUS Enterprise and System Architecture) is describing the complete modelling for a sub-set of the key SALUS services only.

The analysis of the scenarios leads to the identification of the SALUS capabilities (Strategic Perspective) and their dependencies. It shows that providing "Access to Common Information Infrastructure Services" and "Communication Connectivity" are essential capabilities to achieve the high level capabilities of protecting citizens, properties and PPDR own personnel as well as conducting missions in an integrated way.

 Date of publication: 15/02/2016

The next level of the EA model provided in this document (Operational Perspective) is the identification and definition of the operational nodes, the information exchanges between the operational nodes and the information items details. The operational nodes reflect the different levels of PPDR organisations (strategic, tactical and operational) and different agencies (here limited to three –police, fire-brigade, emergency medical services, but could be extended to a higher number following similar principles). This step also includes the derivation of requirements related to information exchange and identification of operational activities. It is to be noted that additional efforts will be required in the description of operational workflows).

Based on the above, functional blocks are defined (Functional Perspective). At this step, it is essential to adopt a common vocabulary and a Service Oriented Architecture (SOA) approach to ease reusability, scalability and flexibility of the different services for different deployment scenarios and use cases. A service map is proposed along five domains:

1. Operations domain: this include the real operational functions lists, activities and workflows and is not further developed in this document;
2. Community of Interest (COI) domain: functionalities that are user and applications specific,
3. Network and information infrastructure (NII) domain: services that cover information and technology aspects;
4. Service management domain: cross-domain service related to system and system element management;
5. Service assurance domain: cross domain service providing security functions.

A service taxonomy is proposed for each service category; this defines a finer grained definition of individual abstract services. Examples of such abstract services are ‘Force Tracking Service’ or ‘Indoor Localization Service’ for the COI category, ‘Message Brokering Service’ or ‘TETRA2LTE Service’ for NII category. A short description of each meaningful service for SALUS is provided.

Then, this document develops detailed specifications and system architecture for the individual services that will be core services for SALUS first and second validation platform. These specifications include service level specifications, interfaces, state machine, information model, service composition and service functionality specifications. The services that are further detailed in this document are the following: 1) Message Broker Service 2) Force Tracking Service 3) Sensor Data Acquisition Service 4) Intrusion detection Service 5) Forensic Service 6) Dynamic QoS Control Service.

Finally, this document also includes an example of an end-to-end system architecture targeting scenario 1 and 2 (City Security and Temporary protection) with the objective to put in a ‘simpler’ drawing the different functions and elements and to give an example of the mapping of the services developed above in physical entities.

DOWNLOAD THE FULL PAPER
http://www.sec-salus.eu/wp-content/uploads/2014/05/SALUS_D3.2_v1.0.pdf
FOR MORE INFORMATION, CONTACT:
Frank Reinert (frank.reinert@iosb.fraunhofer.de), Fraunhofer IOSB.
Hugo Marques (hugo.marques@av.it.pt), Instituto de Telecomunicações.

 Date of publication: 15/02/2016