Enterprise Architecture of PPDR Organisations

W. Müller

Fraunhofer IOSB Institute of Optronics, System Technologies and Image Exploitation

76131 Karlsruhe, Fraunhoferstraße 1

GERMANY

Abstract - *The growing number of events affecting public safety and security (PS&S) on a regional scale with potential to grow up to large scale cross border disasters puts an increased pressure on organization responsible for PS&S. In order to respond timely and in an adequate manner to such events Public Protection and Disaster Relief (PPDR) organizations need to cooperate, align their procedures and activities, share needed information and be interoperable.*

The paper at hands provides an approach to tackle the above mentioned aspects by defining an Enterprise Architecture (EA) of PPDR organisations and a System Architecture of next generation PPDR communication networks for a variety of applications and services on broadband networks, including the ability of inter-system, inter-agency and cross-border operations.

Keywords: *Enterprise Architecture, Public Protection & Disaster Relief, NAF, OSSAF, System Architecture*

1 Introduction

Public Protection and Disaster Relief (PPDR) organisations are confronted with a growing number of events affecting public safety and security. Some of these events expand from a local to a regional and to an international scale, while others affect from beginning multiple countries. As a consequence, the pressure on PPDR organisations to be able to cooperate in order to respond timely and adequately to such events increases. The need of cooperation demands for aligned procedures and interoperable systems which allows timely information sharing and synchronization of activities. This in turn requires that PPDR organizations come with an Enterprise Architecture on which the respective System Architectures are building. The Open Safety & Security Architecture Framework (OSSAF) provides a framework and approach to coordinate the perspectives of different types of stakeholders within a PS&S organisation. It aims at bridging the silos in the chain of commands and on leveraging interoperability between PPDR organisations. In [1] a methodology was presented, which is based on the Open Safety & Security Architecture Framework (OSSAF) framework [2] and provides the modeling vocabulary for describing a PPDR Enterprise Architecture.

In [3] the process of developing an Enterprise Architecture for PPDR organisations has been described.

The paper at hand presents the results so far of an on-going research being conducted by the research project SALUS[1] (Security And InteroperabiLity in Next Generation PPDR CommUnication InfrastructureS) regarding the PPDR Enterprise Aechitecture and the System Architecture of a next generation communication system for PPDR organisations.

2 Related work

The goal of Enterprise Architecture design is to describe the decomposition of an enterprise into manageable parts, the definition of those parts, and the orchestration of the interactions between those parts. Although standards like TOGAF [5] and Zachman [4] have developed, however, there is no common agreement which architecture layers, which artifact types and which dependencies constitute the essence of enterprise architecture.

[7] defines seven architectural layers and a model for interfacing enterprise architectures with other corporate architectures and models. They provide use cases of mappings of corporate architectures to their enterprise architecture layers for companies from the financial and mining sector.

A layered model is also proposed by [10]. The authors propose four layers to model the Enterprise Architecture: A Strategy Layer, an Organizational Layer, an Application Layer, and a Software Component Layer. For each of the layers a meta-model is provided. The modeling concepts were developed for sales and distribution processes in retail banking.

MEMO [11] is a model for enterprise modeling that is based on an extendable set of special purpose modeling languages, e.g. for describing corporate strategies, business processes, resources or information. The languages are defined in meta-models which in turn are specified through a common meta-metamodel. The focus of MEMO is on the definition of these languages and the needed meta-models for their definition.

The Four-Domain-Architecture [8] divides the enterprise into four domains and tailors an architecture model for each. The four domains are Process domain, Information /

[1] http://www.sec-salus.eu/

Knowledge domain, Infrastructure domain, Organization domain. Typical elements for each domain are also provided. The authors also provide proposals how to populate the cells of the Zachman framework with architectural elements.

The Handbook on Enterprise Architecture [9] provides methods, tools and examples of how to architect an enterprise through considering all life cycle aspects of Enterprise Entities in the light of the Generalized Enterprise Reference Architecture and Methodology (GERAM) framework.

None of the papers addressing Enterprise Architectures covers the special needs of PPDR organizations with their need on timely cooperation, alignment of procedures, and interoperability needs across different organizations.

3 SALUS EA for PPDR organisations

3.1 The SALUS Enterprise Architecture development approach

The SALUS Enterprise Architecture has been designed based on the OSSAF. The OSSAF [2] provides a framework and approaches to coordinate the perspectives of different types of stakeholders within an organisation. It aims at bridging the silos in the chain of commands and on leveraging interoperability between PPDR organisations. One can distinguish the strategic, the operational, the functional, and the technical perspective.

The methodology proposed in [1] for the development of Enterprise Architecture of PPDR organisations, in general and for SALUS specifically, uses NATO Architecture Framework (NAF) [6] as the modeling vocabulary for describing the OSSAF perspectives and views where suitable. The NAF views are modeled with the different elements of the Unified Modeling Language (UML).

The meta-model of the NAF used for the PPDR EA development, together with a description of the core concepts and their relationships has been provided in [Mueller, Reinert]. Also there the tailoring of NAF views for PPDR EA development has been described; especially the strategic and operational perspectives of the OSSAF model (see also Figure1).

Since SALUS is addressing Security and interoperability in next generation PPDR communication infrastructures and not all aspects of PPDR organisations, there is a need for tailoring the Enterprise Architecture development and its artifacts to SALUS use cases. For SALUS only those artifacts of an Enterprise Architecture are relevant which influence the technical development of communication infrastructures. Thus, a funding model of the PPDR organisation (the "PPDR as an Enterprise") or a specific organisation chart of the enterprise or a concrete product configuration used by the PPDR organisation in its daily operations were not in the scope of SALUS. The Enterprise Architecture Components addressed in SALUS are the ones highlighted in Figure 1.

Figure 1: Perspectives and views of an OSSAF-based Enterprise Architecture addressed in the SALUS EA.

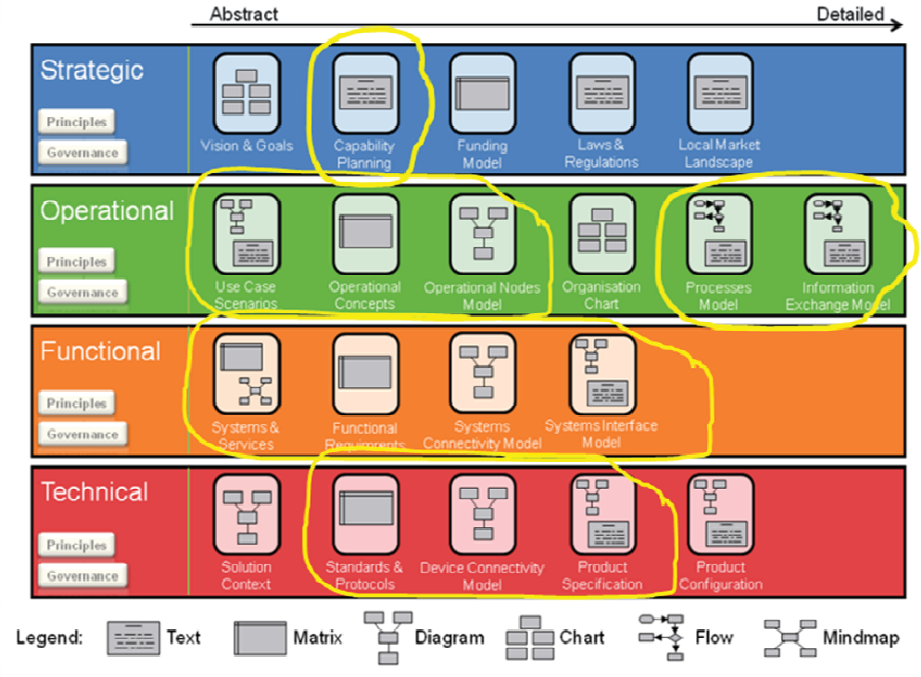
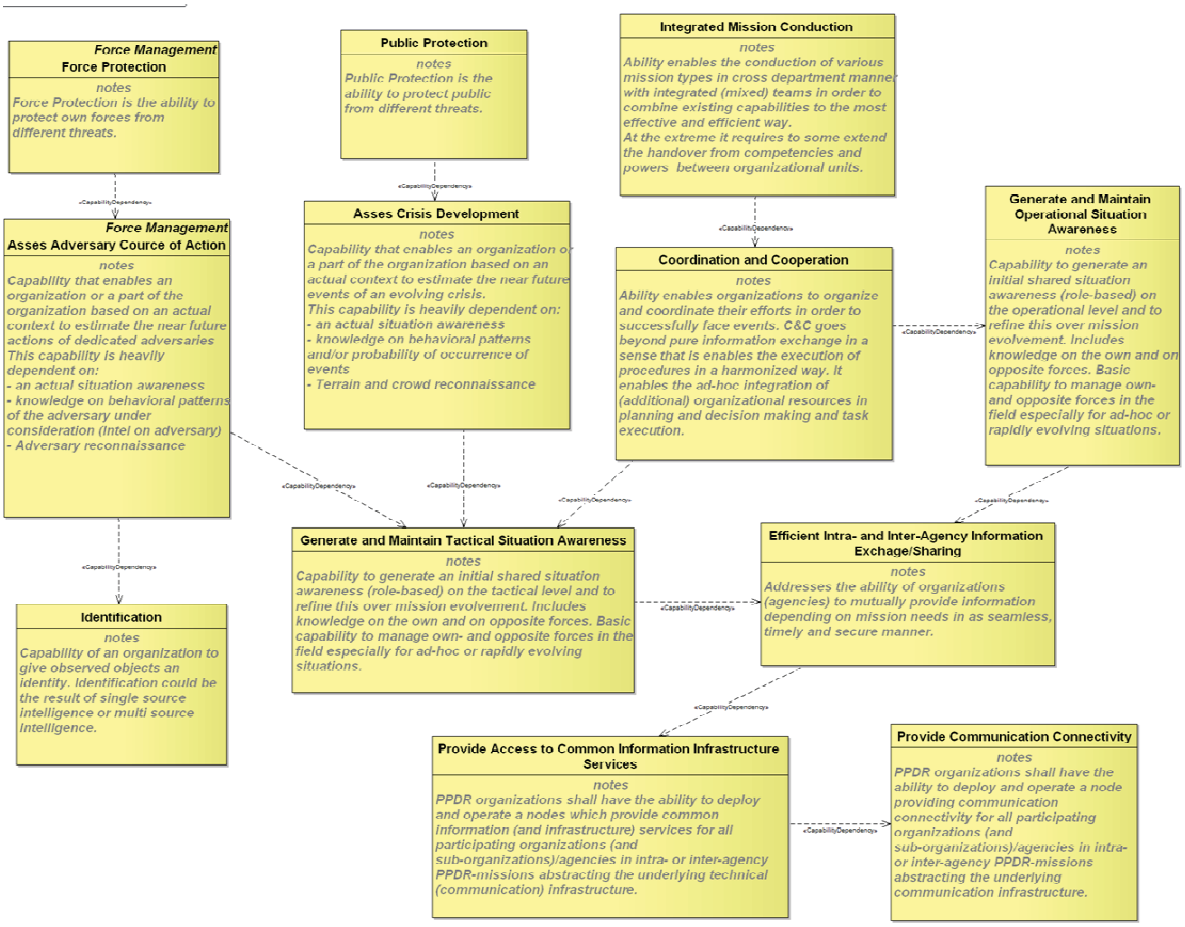


Figure 2: PPDR Capabilities relevant with respect to communication infrastructures



3.2 The SALUS Enterprise Architecture

The methodology proposed in [1] for the development of enterprise architecture of PPDR organizations is using the approach of capability based planning. One can understand a Capability according to [1] as:

”An ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology to achieve.”

Using this approach, the following SALUS Enterprise Architecture Capabilities were identified: the capability to protect the public and the citizens - Public Protection; the capability to conduct a mission in an integrated way - Integrated Mission Conduction; and the capability to protect the own forces - Force Protection (see also Figure 2).

The SALUS capabilities also rely on others, like assessing the development of a crisis or the capability to coordinate and cooperate, which in turn depend on the capabilities to generate and maintain the situation awareness. Indeed, for situation awareness capabilities to exchange and share information within an organisation or agency and between organisation and agencies. The exchanging and sharing information capabilities rely on the capability to provide communication connectivity, which is the main capability implemented by the SALUS project.

The capability providing communication connectivity enables the various PPDR operational nodes, like the command and control centers of the different command levels, such as strategic, tactical, and operational on the field; to communicate with each other, exchange information and thus cooperate in order to handle a crisis and to protect the citizens (see Figure 3).

From a functional perspective, SALUS provides a series of services needed for the capabilities to generate and to maintain situation awareness, to provide access to common information infrastructure services and to provide

communication connectivity. These services can be clustered and grouped into the following service taxonomy, as presented in the Table 1.

Table 1. Enterprise Architecture service taxonomy

Service	Taxonomy
Situation Awareness Service	Location and Monitoring Service: – Indoor Location Service – Status Monitoring Service
	Sensor and Tracking Service: – Sensor Data Acquisition Service – Sensor Control Service – Force Tracking Service
Information Assurance Service	Security Service: – Intrusion Detection Service – Resource Authentication Service – Policy Enforcement Service – Forensics Service
Management Service	Management Service: – User Management Service – Group Communication Management Service – Mobility Management Service – Policy Management Service
Network & Information Infrastructure Service	Information and Integration Service: – Message Brokering Service
	Communication Service: – Voice Communication Service, including - Push To Talk (PTT) - Group Call - 1to1 Call - Emergency Call - Ambience Listening – Data Communication Service - Streaming Service - Text Messaging Service
	Interaction Service: – Video Conferencing Service – Chat Service
	Network/Transport Service: – Mobility service - WiFi2LTE Mobility Service - Traffic Management Service – QoS Monitoring Service - Network QoS Monitoring Service – Communication Interworking Service - TETRA2TETRAPOL IW Service - TETRA2LTE IW Service - TETRAPOL2LTE IW Service

Based on the developed Enterprise Architecture, a technical oriented System Architecture was developed.

4 The SALUS system architecture

Nowadays, PPDR organisations are using Private Mobile Radio (PMR) technologies such as TETRA, TETRAPOL or P25 for their communication systems. These technologies do not provide broadband capabilities nor is expected that these technologies will be upgraded in the future. This presents a major limitation in supporting new services and information flows, like those designed in the previous sections. On the other hand, these technologies will continue to exist for at least the next 15 – 20 years due to legal commitments and the huge investments made.

In order to cope with the increasing challenges in day-to-day, planned or unplanned events, PPDR organisations need communication systems and technologies capable of supporting additional capabilities like video and data sharing, within and between PPDR organisations. New technologies, such as Long Term Evolution (LTE) for the long range and Wi-Fi or LTE-U[2] in the short range enable broadband applications and services.

Since narrowband and broadband PPDR systems will coexist, according to the migration roadmap presented in [12], interworking of PMR services between the different wireless access technologies is a major requirement. The PMR services to be supported on all access networks can be split into four main categories: Basic services, PMR supplementary services, telephony supplementary services, and security features. The basic services include the minimum feature set for a conventional PMR network. They consist of registration/de-registration, group affiliation, group calls, one-to-many communications with PTT user request to talk; individual calls, PTT or hook button based; telephony calls to/from an external telephony network, broadcast call, call from a dispatcher to all PPDR users in a group; status, such as predefined set of text messages; and generic text messaging, binary messaging, as transmit sensor information.

The PMR supplementary services are the more advanced services that are essential to PPDR users to operate safely and efficiently. They include priority calls, pre-emptive priority calls, emergency calls, late entry, dynamic regrouping, discreet and ambiance listening from the dispatcher position and location reporting. The telephony supplementary services are services related to public access telephony such as call forwarding features, when busy, or without reply; call hold, call transfer, call barring, incoming and outgoing; and call authorized by dispatcher. The security services are features that are related to the critical use of the wireless communications for PPDR users. They include mutual authentication, the ciphering on the air interface, the end-to-end encryption, the temporary and permanent disabling of a terminal.

The design of the SALUS system architecture takes into account the above mentioned coexistence of narrowband PMR technologies and emerging broadband technologies. It designs interfaces and hand-over mechanisms from Wi-Fi to LTE, TETRA and TETRAPOL to LTE, as well as LTE and Wi-Fi coverage extensions via Mobile Ad hoc NETworks (MANETs) (see Figure 4).

[2] LTE-U (LTE-Unlicensed), operates in unlicensed spectrum, typically in the 5GHz band, to provide additional radio spectrum

Figure 3: PPDR operational nodes and their information exchange need-lines

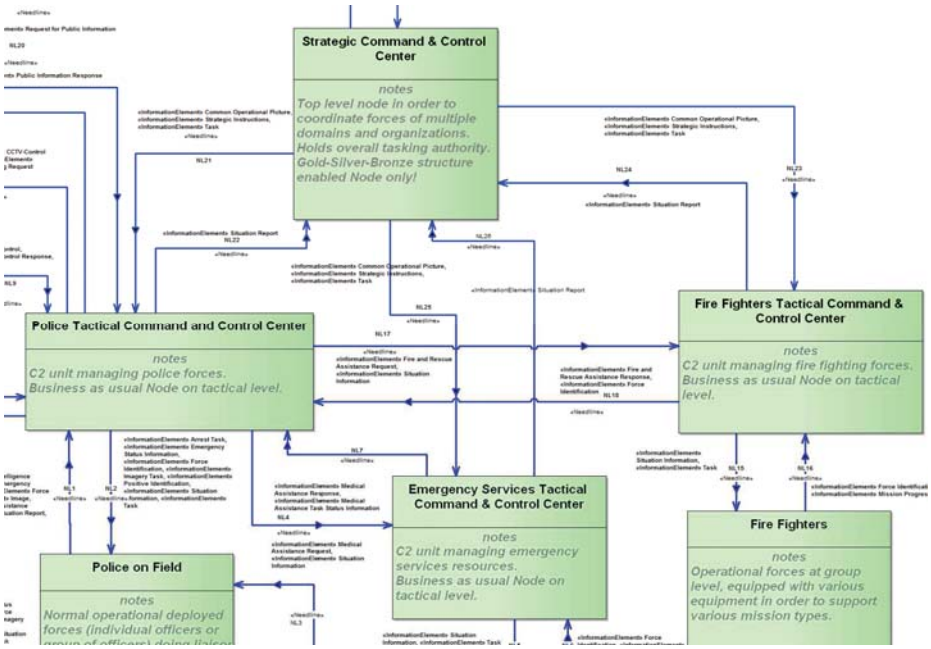
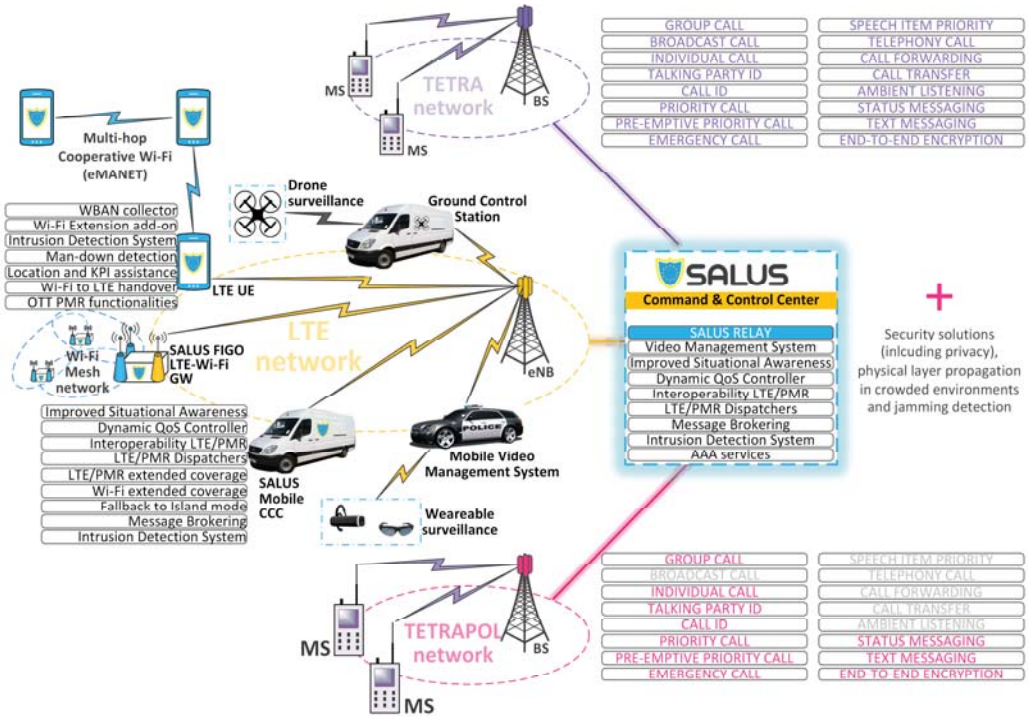


Figure 4: High-level system architecture of the SALUS platform



In accordance with the PPDR Enterprise Architecture, the Command and Control Centre (CCC) is a central piece in the system architecture. It is here where meaningful data is collected, processed and relayed to proper recipients. Besides voice and video support (including group calls), data-driven applications are running in the CCC and the PPDR network. Applications that stream, in real-time, location of PPDR operatives from their hand-held terminals to applications in the CCC, applications that provide terrain characteristics and report measurements to remote geographical information systems (GIS) applications, or applications that by some clever means of processing determine whether a PPDR operative is incapacitated, e.g. is fallen to the ground or report his location are just a few examples. Such applications are by their nature distributed: some run on hand-held terminals of PPDR operatives and some run on computers located at various locations ranging from the CCC to vehicles (like the mobile CCC). For these applications an effective and secure communication means for message exchange is needed. Furthermore, since such applications will often process personal data, the communication means should also respect the privacy of its users.

A key component to respond to these issues is the usage of a Message Broker. It establishes connections between and facilitates the exchange of messages amongst a dynamic number of distributed applications. It achieves these tasks by acting as an application level message router. The Message Broker operates on a well-known network address and accepts connections from various clients. These can be applications running on terminals of PPDR operatives connected to the network via some wireless technology, they can be process-intensive applications running on super-computers in data centres connected to the Internet backbone, or plain situation awareness applications in command and control centres. Once an application connects, the Message Broker enacts the role of an intermediary that facilitates the exchange of messages. The broker provides its own addressing mechanism by which applications address each other, that is, applications do not address each other by their network address but rather by their identities: an identity is an identifier that uniquely determines a single application. Identities allow applications to address each other independently of their network addresses and the translation (or mapping) between identities and the network addresses is something that is an internal matter of the broker. As identities, applications use their public keys. Since it sits between distributed applications, the broker can monitor, authenticate and authorize all message exchanges. To perform these tasks, it has an interface with the AAA services

As depicted in Figure 4, wireless sensor networks and Wireless Body Area Networks (WBAN) are an integral part of the communication system. Sensor data is usually collected by sensors attached to the bodies of in-field deployed PPDR personnel and then sent via their hand-held terminals (UEs) to backend application for processing. The first type of used sensors concern bio-signals, such as the heart rate, blood pressure, temperature and similar kinds of user information. Other kind of personnel wireless sensor information are movement and localization, obtained from accelerometer, gyroscope and GPS sensors. The body signals are used in order to interpret current user health state, location and position allowing an analysis to search for critical events, such as heart attack and falls of users. These data are aggregated and contextually shown on an Improved Situation Awareness application (also known as Common Operational Picture), running on the CCC.

In order to ensure a constant security monitoring of the communication infrastructure, a hybrid network-based intrusion detection system (NIDS) and host-based intrusion detection system (HIDS) approach is used. The approach can either take a signature-based or anomaly-based approach to detect intrusions. By using a hybrid approach, restrictions that are imposed by limited host resources can be overcome, especially when referring to mobile terminals. For example, lack of centralized connectivity may hinder a NIDS, and limited resources may make a sole HIDS approach infeasible. Lastly, the implementation of a hybrid IDS does not create additional infrastructure requirements, since the HIDS part is independent of the NIDS and does not interfere with it

5 Conclusions and further work

An Enterprise Architectures for PPDR organizations with a focus on capabilities of providing access to common information infrastructure services and communication connectivity was presented. The approach is based on the OSSAF and NAF frameworks. It depicts the main capabilities needed by PPDR organisations to perform their mission of ensuring security and safety of the citizens.

The System Architectures and the solution developed within our work and presented in the paper at hand provides the design of a next generation communication infrastructure for PPDR organisations, which fulfills their requirement of secure and seamless end-to-end communication.

The design allows interworking of currently existing narrowband PMR communication infrastructures like TETRA and TETRAPOL with the broadband LTE technology. Furthermore, extensions provided by other wireless technologies, such as Wi-Fi, Bluetooth or ZigBee for WBANs and Wi-Fi or LTE-U for extended coverage have been considered as well.

The design will be evaluated in June 2016 in a live experiment with PPDR users.

Acknowledgement: The work described in this paper was partly funded by the European Commission within the European Seventh Framework Programme under Grant Agreement 313296, SALUS - Security And InteroperabiLity in Next Generation PPDR CommUnication InfrastructureS

6 References

[1] W. Müller, F. Reinert "A Methodology for Development of Enterprise Architecture of PPDR Organisations", Proceedings of the 2014 International Conference on Software Engineering Research & Practice (SERP 2014), pp. 259 – 263.

[2] Open Safety & Security Architecture Framework (OSSAF), http://www.openssaf.org/download

[3] W. Müller, F. Reinert "Development of Enterprise Architecture of PPDR Organisations", Proceedings of the 2015 International Conference on Software Engineering Research & Practice (SERP 2015), pp. 225 – 230

[4] Website Zachman Framework, http://zachman.com/

[5] Website TOGAF, http://www.opengroup.org/togaf/

[6] NATO Architecture Framework Version 3, ANNEX 3 TO AC/322(SC/1-WG/1)N(2007)0004

[7] R. Winter, R. Fischer "Essential Layers, Artifacts, and Dependencies of Enterprise Architecture", Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06), IEEE Computer Society, 2006

[8] B. IYER, R. Gottlieb "The Four-Domain-Architecture: An approach to support enterprise architecture design", IBM Systems Journal, Vol 43, No 3, 2004, pp. 587- 597.

[9] P. Bernus, L. Nemes, G. Schmidt (Editors) „Handbook on Enterprise Architecture", Springer, 2003.

[10] Ch. Braun, R. Winter "A Comprehensive Enterprise Architecture Metamodel and Its Implementation Using a Metamodeling Platform", In: Desel, J., Frank, U. (Eds.): Enterprise Modelling and Information Systems Architectures, Proc. of the Workshop in Klagenfurt, GI-Edition Lecture Notes (LNI), Klagenfurt, 24.10.2005, Gesellschaft für Informatik, Bonn, P-75, 2005, pp. 64-79.

[11] U. Frank, "Multi-Perspective Enterprise Modeling (MEMO) - Conceptual Framework and Modeling Languages", Proceedings of the Hawaii International Conference on System Sciences (HICSS-35), 2002, p. 3021ff.

[12] H. Marques et al., "Next-Generation Communication Systems for PPDR: the SALUS Perspective" In: Camara, D., Nikaein, N. (Eds.): "Wireless Public Safety Networks", Volume 1, Elsevier / ISTE Press – Elsevier, London & Oxford, 2015, pp. 49 – 94.