How to empower policemen and their vehicles: A multiple case study analysis of seven public safety related ICT projects

Jyri Rajamäki, Juha Knuuttila, Outi Suni, Henna-Riitta Silanen, Antti Tuomola and Päivi Meros

***Abstract*—**The economic pressure decreases the budgets of the first responders (FR) which in turn increases the pressure for developing novel innovations to ensure adequate computational capabilities and resources in every operative scenario. FRs' most important tool in the field is the emergency response vehicle (ERV). The Finnish approach to provide digital services to the field for FRs is via ERVs. This multiple case study analysis collects together the research data and results with respect to ERVs from seven public safety related ICT projects. It is vital that different safety authorities develop the common ERV concept together. This enables new mobile digital services for FRs to their field operations. For example, people being first at the scene of the accident should be able to communicate with FRs who should be able to receive social media and multimedia messages into their operative systems.

***Keywords*—**Case study, Emergency response vehicle, Law enforcement, Police car, Public safety.

I. Introduction

DUE to the economic situation, the budgets of the public protection and disaster relief (PPDR) are cut down which in turn increases the pressure for developing novel innovations to ensure adequate computational capabilities and resources in every operative scenario [1]. In field operations, first responders' (FRs) most important tool is their vehicle. The Finnish approach to provide digital services to field for FRs is via their Vehicles [2]. In Finland, Border Patrol, Custom and Police Cars are already quite similar - except their color, because these all are equipped by The Police Technical Center [3]. Also other emergency response vehicles (ERVs) such as fire trucks and ambulances have similar needs for navigation system, patrol tracking, target maps, activity logs, alarms and remote access to central databases as well as the control of blue lights and sirens, power supply systems and communications equipment [4]. Also, the inventory of ERVs' equipment means a weekly basis the number of hours used in the examination of goods, all of which are out of from field work [5].

This work was inspired and partly supported by the Mobile Object Bus Interaction (MOBI) project at Laurea University of Applied Sciences, Finland. The MOBI project is partly funded by Tekes—the Finnish Funding Agency for Technology.

J. Rajamäki is with SID Lab, Laurea University of Applied Sciences, FI-02650 Espoo, Finland; phone: +358 40 764 2750 e-mail: Jyri.Rajamaki@laurea.fi.

J. Knuuttila is with SID Lab, Laurea University of Applied Sciences, FI-02650 Espoo, Finland; e-mail: Juha.Knuuttila@laurea.fi.

O. Suni, H.-R. Silanen, A. Tuomola and P. Meros are master students of Laurea University of Applied Sciences, FI-02650 Espoo, Finland.

A. Objectives and Scope

The scope of this study is to collect together the research results with regard to law enforcement authorities (LEAs) patrol cars from seven different research and development projects (=cases), to understand the phenomena, and to make suggestions how to improve the development of future patrol cars.

Law enforcement and other PPDR operations are critical functions of society. The first case, RIESCA (Rescuing of Intelligence and Electronic Security Core Applications) project, studies the procurement and maintenance procedures of different critical information systems that support society. Patrol cars have such critical information systems. The second case, TUVE – Information Security Network project, provides the communications infrastructure for Finnish patrol cars. The third case, KEJO – field command system, develops a common field command systems for all Finnish PPRD actors. The fourth case, VITJA – the reforming project of the Finnish polices information systems, replaces almost all major operational information systems used by the Finnish police. The fifth case, MOBI (Mobile Object Bus Interaction), researches into the integration of patrol cars' electric, electronic and ICT systems. It also equips a demo vehicle. The sixth case, SATERISK – risks of satellite-based tracking, researches all kind of technical, operational and legislative risks with regard to satellite-based tracking and navigations. These are vital services for patrol cars. The seventh case, MACICO (Multi-Agency Cooperation In Cross-border Operations) develops a concept for interworking of different security organizations in their daily activity.

B. Research Questions

This multiple case study analysis is carried out according to Yin's model [6]. It includes one main research question, which is additionally focused by seven expanded and iterative research questions in seven studies in which the research questions of each study produced more detailed insight into the main research question. In this study, the main research question is:

RQ: How can empowering of policemen and their vehicles be understood?

The seven expanded and iterative research questions are:

RQ1: How can optimal procurement and maintenance of police patrol cars' ICT systems be understood?

RQ2: How can TUVE Network and its security requirements be understood in the perspective of police patrol cars?

RQ3: How can KEJO be understood in the perspective of police patrol cars?

RQ4: How can VITJA be understood in the perspective of police patrol cars?

RQ5: How can the integration of police patrol cars' electric, electronic and ICT systems be understood in the perspective of police patrol cars?

RQ6: How can the risks of satellite-based tracking and navigation be understood in the perspective of police patrol cars?

RQ7: How can multi-agency cooperation in cross-border operations be understood in the perspective of police patrol cars?

II. Theoretical Framework

A. Public Procurement of Innovative Solutions, Pre-Commercial Procurement and Pre-Operational Validation

Public procurement of innovative solutions (PPI) means procurement where contracting authorities act as a launch customer for innovative goods or services which are not yet available on a large-scale commercial basis, and may also include conformance testing [7].

In Pre-Operational Validation (POV) the main focus is in assessing and validating existing systems whereas Pre-Commercial Procurement (PCP) the main focus is in creating new innovations. According to the ECORYS study the concept of POV was introduced in July 2011 when the 5th FP7 call for security was released [8]. The ECORYS report thus mentions the POV but does not go much deeper as the concept was fairly new at the time of writing of the study. Therefore, the concept of POV should be further defined and differentiated from the PCP.

In principle, PPI, PCP and POV gives better possibilities for Small and Medium Enterprises (SMEs) to participate in procurement projects due to lower entry barrier but procurement procedures are seen as too complex for SMEs due to limited resources and experience in procurement procedures. Therefore, the bottlenecks limiting or hindering the possibilities of SMEs to actively participate in public procurement projects in general and in the field of security especially should be further identified and investigated. In this respect, a two-layer approach is proposed enabling firstly an overall description of the challenges faced by SMEs in public procurement and secondly a more deep analysis on the most relevant topics that the investigation will highlight. Special focus should be targeted to small businesses with limited knowledge and experience in public procurement procedures and requirements related thereto.

The European Network of Law Enforcement Technology Services (ENLETS) was set up in 2008 under the French Presidency of the Council with the aim of gathering user

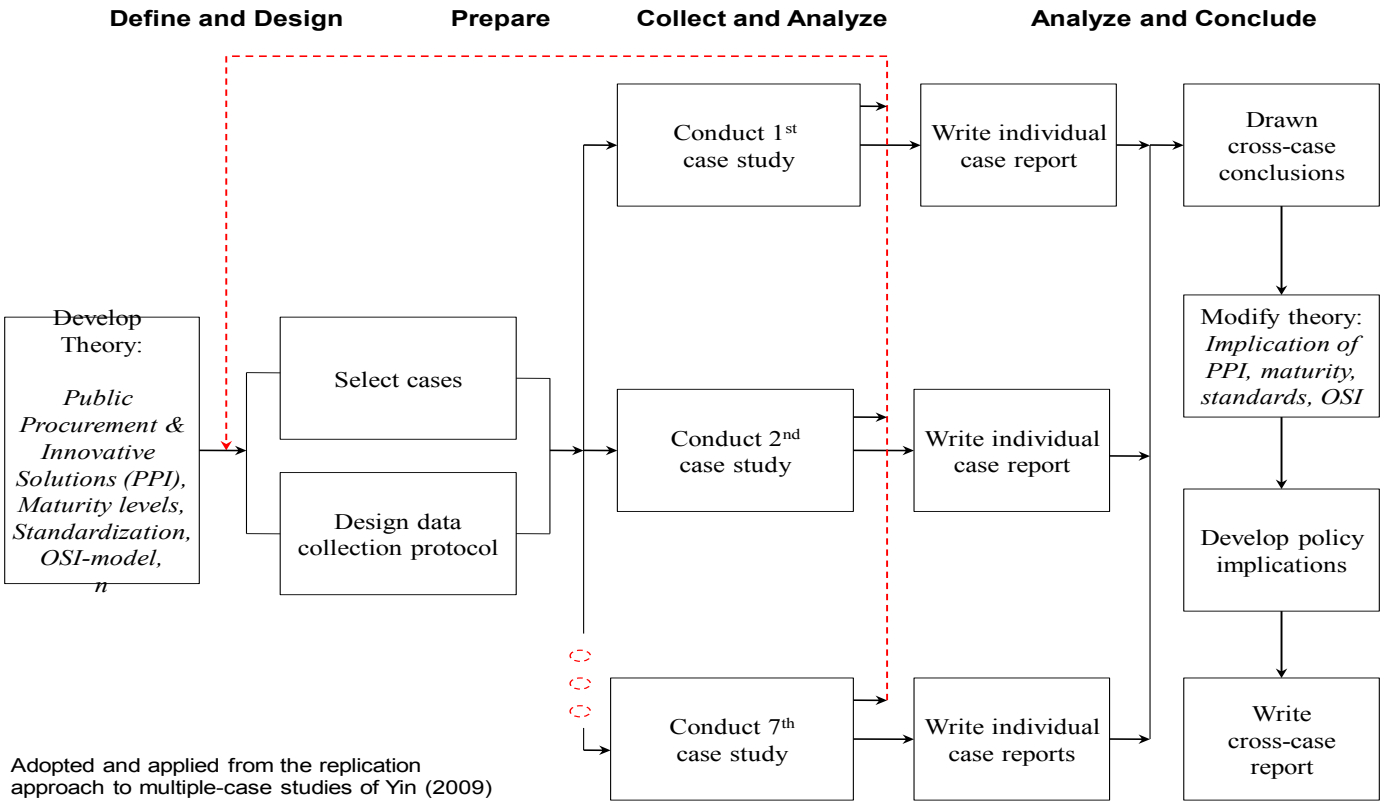

Fig.1 Multiple-case study method of this research

requirements, scanning and raising awareness of new technology and best practices, benchmarking and giving advice. As stated in the Council's conclusion, ENLETS could further enhance proper coordination between Member States for public procurement and become a leading European platform for strengthening the internal security authorities' involvement in security-related research and industrial policy and thus bridging the gap between the end users and providers of law enforcement technologies [9].

B. Maturity levels

The role of business continuity and IT continuity management is to identify business requirements and provide solutions that ensure the continuity of information services and capability to recover in case of disruptions or interruptions. Especially large organizations have considerably high number of information services, and thy have a need to implement target oriented and commonly accepted management models. This applies to IT continuity management processes and maturity models, too.

Syrjänen [10] studied a large Finnish technology company that invests strongly in information technology due to high dependency on information systems availability. This company developed and started to implement an IT continuity maturity model in the year 2007. Their maturity model is a combination of business continuity, IT governance and information risk management standards and best practices built on top of commonly used process maturity models. Syrjänen's study introduced the background and initial triggers for maturity model development. In addition, maturity model principles and usage cases were reviewed. The purpose of the study was to find out how much the IT continuity management maturity model had improved overall planning and the level of business continuity in the target organization. The core of Syrjänen's study [10] was the evaluation, the purpose of which was to evaluate the concrete benefits that the use of maturity model had brought. The benefits were analyzed from five viewpoints: information service management, IT line units, IT governance, corporate governance including risk management, and the point of view of the individual. The evaluation was based on service quality reports, incident analyses and continuity reports. In addition to the extensive report base, open discussions and feedback from the IT continuity community had a significant role while assessing the maturity model value. The theoretical framework was mostly based on industry standards and best practices and the methods of canonical action research. Although the source material provided a solid base for the study, the confidentiality of information limited what and how much information could be shared in this study.

C. Standardization

The European Commission, EUROPOL and FRONTEX have recognized that lack of interoperability limits the effectiveness of public safety practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, gaps in procurement or research [11]. A scientific proven fact is that standardization strongly affects businesses that develop and sell technologies and technology-based products and services; standards are one main enabler for fast growth [12]. For improving interoperability, standardization development with like-minded countries should be started.

Regulations and standardization play an important role in applying the results of research to the market and to the public safety end-users. The on-going planning of European external border surveillance system (EUROSUR) [13] and EU´s enhanced powers in the field of internal security by the Treaty of Lisbon pace the way for further standardization efforts.

D. "OSI-model" for ERVs

The layered model for ERVs is developed by the MOBI project [14]. The benefits of this approach to the development of ERVs are similar to those that the Open Systems Interconnection (OSI) reference model brought to the field of data communications. The layered approach breaks ERVs' electrical, electronic, information and communication technologies into smaller and simpler parts, as well as smaller and simpler components, thus aiding component development, design and troubleshooting. The standardized interfaces allow modular engineering, meaning that different types of hardware and software components communicate with each other. Interoperability between vendors allows multiple-vendor development through the standardization of ERV components. It defines the process for connecting two layers together, promoting interoperability between vendors. It allows vendors to compartmentalize their design efforts in order to fit a modular design that eases implementation and simplifies troubleshooting. The layered approach ensures the interoperability of technologies, preventing the changes in one layer affecting other layers, allowing quicker development and accelerating evolution. It provides effective updates and improvements to individual components without affecting other components. All these aspects have already been found to be very valuable in the field of data communications after the OSI model has been applied.

E. Vehicle Infrastructure and Power Management

With regard to the vehicle infrastructure and power management layer, there are two main areas to standardize: 1) what services will be adapted from a standard vehicle system and 2) how to make the car body modifications and new installation in a standardized way. The services adopted from standard vehicle include, for example, power generation when the engine is on and information applied from the vehicle's controller area network (CAN). The standardized ERV installations include vehicle body modifications, emergency lights and alarms, intelligent power management (power generation, storage and distribution systems) as well as cable and antenna installations (electromagnetic compatibility issues).

A modern ERV carries a lot of equipment and it is extremely important to be sure that all needed tools are available in field operations. All ERVs should be ready to

service on 24/7 basis. Preventive maintenance acts vital role to guarantee ERV operation preparedness but maintenance procedures during and after working sift are important too. The inventory of an ERV means a weekly basis the number of hours used in the examination of goods, all of which are out of from normal work. By applying, for example, RFID technology the inventory of tools could be automatized [5].

F. Communications

ERVs' communication layer is a part of the nation-wide public safety communications (PSC) system. The enhanced performances of the technologies in the private sector grow faster than in PSC as shown in Fig.2. Current communication standards, such as 802.11n and Long Term Evolution (LTE)-Advanced are providing data rates up to 100 Mbit/s with a roadmap up to 1 Gbit/s [15]. This enables users to rely on mobile data services and mobile Internet access in many situations. The overall performance of TETRA is on the degree in which commercial mobile networks were two decades ago. This situation prevents the use of high-data services such as live video broadcasting. Although some enhancements are planned to the TETRA standard – e.g. TETRA Enhanced Data Services (TEDS) – the gap between the technologies applied in PSC and private sector is getting wider over the time [15].

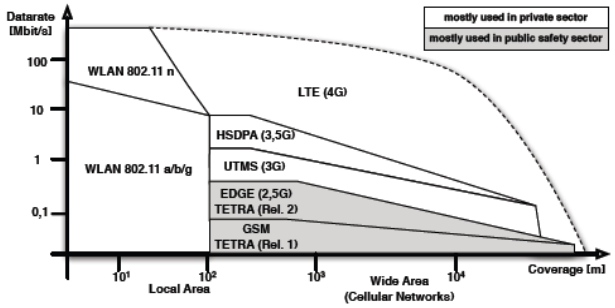

Fig.2 Coverage and data rates of wireless network technologies [15]

The main challenges in public safety communications are (1) lack of broadband connectivity and (2) lack of interoperability. In the field, wireless communications' role is to support the mobility of first responders by providing continuous connectivity among responders and with the headquarters [11]. The support includes: maintenance of voice communication to coordinate the relief efforts for the resolution of the crisis; creation and distribution of a common operational picture among all the responsible parties; collect and distribute data in the operational context or the environment from sensors; retrieve data from central repositories (e.g. building plans, inventory data) to support their activity; support the tracking and tracing of the supply chain of goods and materials needed for the response and recovery phases of a crisis. The lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, and gaps in procurement or research [11].

Table I Classification of data communication needs [17]

Class	Information carried	Service used	Rata needed
Narrow band	Alarm, status, location info	Status message, SDS[a], LIP[b]	< 100 kbit/s
Wide band	Still picture, query, announcement, low-resolution video, Internet access	File transfer, email, IP data	100-1000 kbit/s
Broad band	High-resolution video	Multi-media, streaming	> 1 Mbit/s

[a] TETRA Short Data Services
[b] ETSI Location Information Protocol

All PPDR actors have the same basic needs for the system and data communication. However, they also have own distinct requirements. Data communication needs can be classified according to the data rates required as shown in Table I.

For finding common solutions and operation models, system integration is needed. This also enables coherent system design including improved activities, cost savings and improved multi-authority co-operation at the scene. The roles of complementary wireless PSC technologies in the future are as follow [16]:

- 2G/GPRS technologies are reaching the end of their life cycle.
- 3G technology has good coverage with U900. However, problems exist on the availability/capacity of commercial networks during major accidents in crowded areas.
- 4G/LTE networks are at 2.6 GHz, which is not suitable for rural coverage. In future, 800MHz LTE systems are anticipated.
- Wireless local area network (WLAN) technology has at least three scenarios for data transfer: (1) from a vehicle to a station garage, (2) a local wireless AdHoc network around the vehicle at the scene, and (3) from a vehicle to a public WLAN; "WLAN fire plug".
- Satellite technology has a complementary role when a lack of coverage of available terrestrial communications network. It includes long term usage when no other systems are available and communication required for temporary sites.

G. Service Platform and Common Services

The standardized communication layer for all PPDR organizations enables cooperation between authorities, e.g., by setting up a common talk group for incident communications. The next pitch of harmonizing is the service platform and common services layer, in which the design principles of service-oriented architecture (SOA) and cloud computing could be applied [18]. All ERVs have many similar applications such as a navigation system, patrol tracking, target maps, activity logs, alarms and remote access to central databases as well as controlling of blue lights and sirens, power supply systems, communications equipment. The demand for controlling the physical data location in the cloud restricts the use of public clouds as the deployment model of

LEAs, but if the physical boundaries of the possible cloud environments in existing public clouds are determined before building the actual private cloud, this restriction can be relaxed [1]. If PPDR actors' requirements for computational capabilities and resources increase e.g. during a natural disaster or a similar crisis, the private cloud infrastructure can be extended with the existing public cloud hardware to meet the new requirements [1].

H. Actor-specific Services

By 'actor-specific services' we mean these digital services that differ substantially from other FRs' needs. For example, medical information systems and databases have developed rapidly in recent years [19]. Progress in mobile technologies has generated a demand to take these functionalities into account on mobile work in ambulances. The ambition to make the most out of the medical information systems in these mobile environments is to take advantage of the capabilities in mobile technologies to make use of the systems remotely. The primary functions for these mobile technologies and systems are to substitute the paperwork, provide interface to search for information and to enter information to the medical information systems while on mobile emergency. Benefits that will be gained from real time patient information updates are the increased quality of the care and more accurate information about the patient's condition during the mobile emergency care.

III. Empirical Context and Target

This chapter introduces the empirical context and target of this study. First, an introductory overview of the case study projects is provided. One of the projects (MACICO) is European level project; all the others are/were national projects. Laurea University of Applied Sciences has been the leader/coordinator of RIESCA, MOBI, SATERISC and MACICO's Finnish consortium. One of the authors has acted as the scientific manager and supervisor of these four projects. TUVE, KEJO and VITJA were led by Ministry of the Interior, its ICT Agency HALTIK or the National Police Board.

Fig.3 shows what kings of research and development activities in this filed are ongoing in Finland. When looking technology push side, the MOBI coalition includes two enterprise projects. An enterprise project, led by Insta DefSec Ltd., developed secured software services. The project utilized the results of the related research project and aimed to develop product concepts which have potentials in both domestic and export markets. Additionally, Insta DefSec Ltd. will further develop its business model in order to be able to utilize growth potential of the product concepts. The project started June 2010 and ended December 2012 [4].

Another enterprise project, led by Cassidian Finland Ltd., implements a vehicle-installed professional mobile radio (PMR) concept for law enforcement, and fire and rescue operations. The project started January 2010 and will end May 2013 [20].

When looking market pull, end-user and customer side, the Police Technical Center / National Police Board will be leading a pre-commercial procurement project (the PARVI project) for a new type of a law enforcement patrol car [21]. Ministry of the Interior's ICT Agency HALTIK and the National Police Board are developing a common Field Command System for all public safety actors [22].

The Mobile Object Bus Interaction (MOBI) research project generates research data for enterprise and governmental projects by researching and documenting the needs and requirements of the users, power generation and supply and

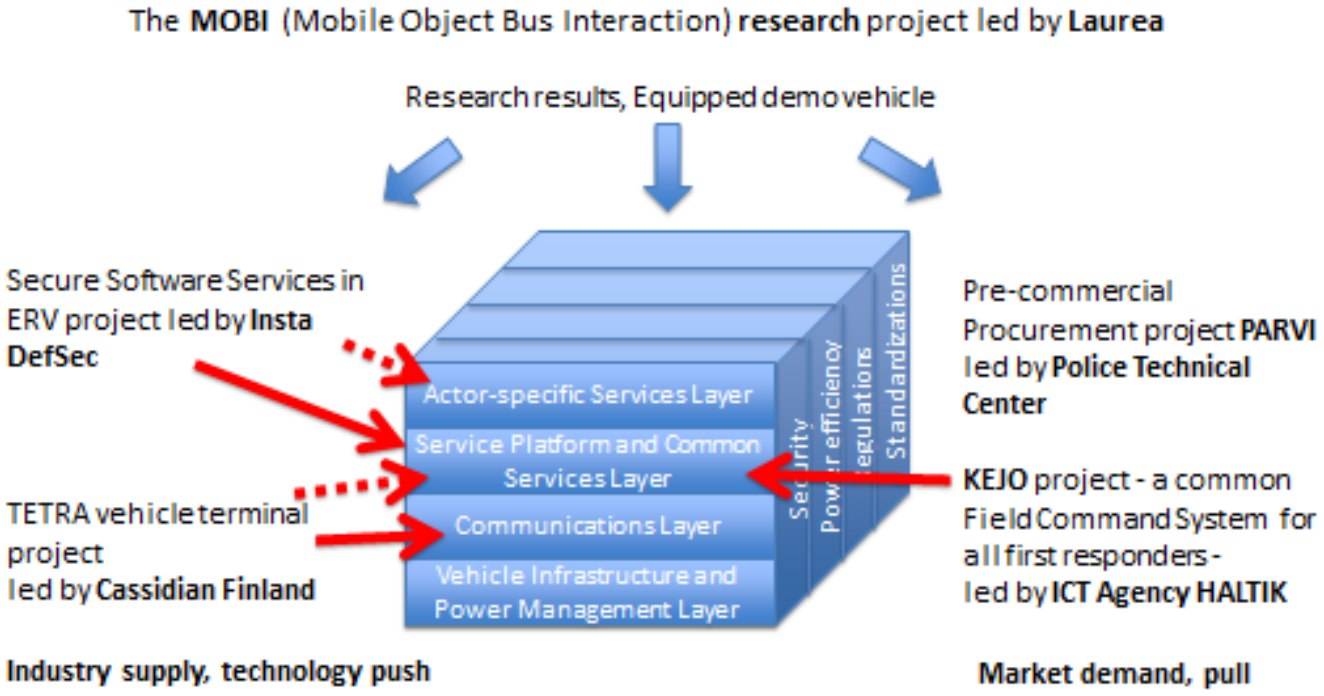

Fig.3 Finnish ERV projects

specifying the existing solutions. We are also equipping a demo vehicle. The project started September 2010 and will end March 2014 [4].

A. RIESCA

Rescuing of Intelligence and Electronic Security Core Applications (October, 2007 to March, 2010) was the first of Laurea University of Applied Sciences' externally funded R&D projects [23]. The research of RIESCA addresses a number of systems, such as transport and logistics, power and telecommunication, hydropower and nuclear power stations, which are critical to the day-to-day functioning of any technologically advanced society, such as Finland. When assessing possible risks, it is only seldom taken into account that power, hydropower and nuclear power plants are critically dependent on the reliability and security of information systems. The aim of RIESCA was to offer contributive and constructive solutions, such as DR-based solutions, to this problem [24]. The student-centered R&D viewpoint was integrated in RIESCA: an individual student or larger student groups were assigned to defined parts of the project. There are two notable advantages conferred by the use of students on the project, namely: 1) confidential information management can be used and developed in actualizations; and 2) the students acquire more new professional expertise that fits with the principles of LbD framework. In view of collaboration, the trust-based networked expertise relationships were achieved in RIESCA. The student-centered R&D activities in RIESCA are accessible in [23]; this first volume of our Sample of Evidence Series includes the description of RIESCA, see also [10, 24].

B. TUVE

The communications concept of the Finnish Government consists of many different networks that can be roughly divided into four different levels of preparedness, as shown in Fig.4. The Defence Forces' strategic communications have the highest level of preparedness. The second level is the secure data network for state officials (TUVE network) having about 30.000 users [25, 26]. The third level consists of the Government's common secure communications requirements. This level is realized by public-private-partnership (PPP); together with the State IT Service Centre and commercial telecommunication operators [27]. The fourth level has normal business requirements and it is realized by commercial networks.

The State Security Networks Ltd provides secure, undisturbed and reliable network services to Finland also in special conditions, and this is why its networks and their management have been highly secured even physically. The company has safety classification and the staffs it employs fulfil strict safety requirements. The company uses efficient and safe communications networks, as well as network control systems that ensure data security. Finnish TETRA-based PPDR network Virve is the largest of the company's networks both in size and in the number of users. Virve has been operative since 2002 with full domestic interoperability. Every week, Virve transmits 800,000 group calls and 32 million short data service (SDS) messages [28]. The Finnish experience shows that GSM networks were overloaded during emergency situations (e.g. high school massacres in 2007 and 2008 and summer storms in 2010) whereas the Virve network was operating normally.

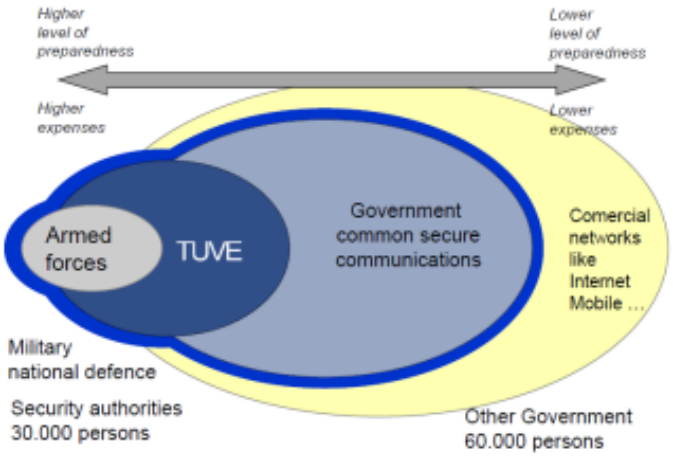

Fig.4 Communication concept of Finnish Government [25]

Finland´s Government has pursued an Information Security Network project (TUVE). Projects mission is to design and implement an Information Security network that supports high level readiness of Security Authorities, integrates existing data and communication systems and develops services and intensifies their shared use. The main goal is to significantly raise the protection level and usability of the Information Security Network. The basis for this network is the highly protected data and communication network of the Finnish Defense Forces [29].

The Information Security Network project includes all authors in Public Protection and Disaster Relief (PPDR) area. The network will be used by state management and for over 30000 users of Security Authorities. The security authority users will have common basic-, network- and infrastructure services and also common communication-, quality measurement-, terminal- and information management services, solid terminals and software. In the future the authority users will also have solid information systems and new applications [30]. The TUVE project will not include developing a whole new network but integrating security authorities as users of the communication network of Finnish Defense Forces and developing common services of authorities. This way it is possible to create costeffectively a common and interoperable, whole country comprehensive system for the authorities.

The TUVE network is connected to the public Internet. Furthermore the network will be operated independently by private name- and time servers. Links to commercial communication networks, as 3G and GSM, have been developed in a separate project. Parts of the TUVE have already been taken in use, as the renewed GMDSS-maritime emergency and safety radio system. Fig. 5 shows the interfaces TUVE has to other existing service networks [30].

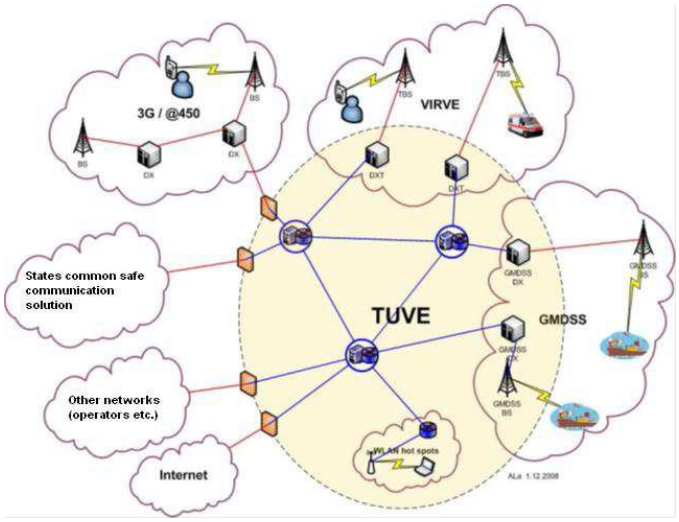

Fig. 5. TUVE´s interfaces to other networks [30]

C. KEJO

Ministry of the Interior's ICT Agency HALTIK and the National Police Board are developing a common field command system for all public safety actors. This KEJO project has started January 2013 and will end December 2016 [22]. Currently, the system is under a tender. The KEJO project includes all authors in Public Protection and Disaster Relief area. The goal in this project is to implement field management system that fulfill the requirements authors have set to the future operational models and take into account of each actors' special needs. KEJO field command system is a common system for safety authors' mobile ICT services and base for wireless mobile devices.

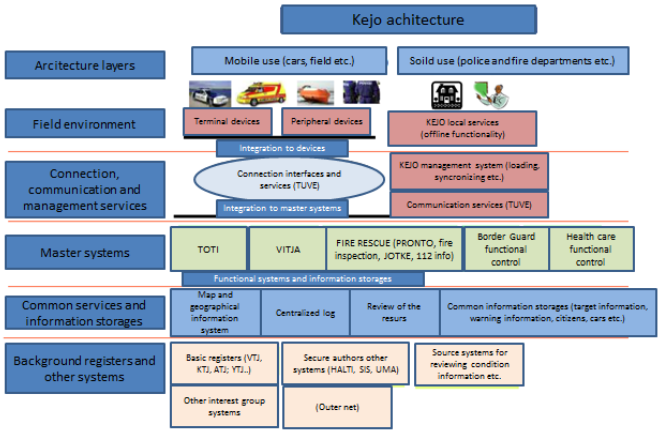

Fig. 6. KEJO architecture (adapted from [32])

The functionalities of the master system PRONTO were observed when KEJO requirements was defined to take care of that field management system can transfer information to and from PRONTO master system [31]. From KEJO is possible to send information by applications to PRONTO master system and get information by inquiries. KEJO system does not include its own information pools but gets the needed information from master systems. In first phase there are only authors in PPDR using KEJO system, but interfaces are defined so that it is easy to integrate other interfaces too [31]. KEJO field management system enables field management to safety authors, maintenance, entering information to master systems and changing information in real time with other PPDR actors. Fig. 6 presents the layers of KEJO architecture.

D. VITJA

In practice, the VITJA project, which is the reforming project of the Finnish polices information systems, replaces almost all major operational information systems used by the Finnish police [33]. The VITJA project does not only concern polices information systems, because VITJA becomes part of crime process chain that is connected with information systems of department of justice, The Finnish Border Guard, the Finnish custom and The Finnish Defence Force [34].

It is estimated that up to 80 percent of the cost of the Finnish police force comes from personnel costs. Because the Finnish governments have decided cut the funding, it has forced the law enforcement organizations to start projects to profit from technical advancement and its solutions to for example mobile working environments [33].

The VITJA project is essential for streamlining the analysis work of the police, because the current information systems were developed to store data and the usability doesn't meet today's demands of analyzing capabilities. The functional and technical capability of many of the current systems are also poor and police officers have to do much manual work to operate with the different current systems, because the lack of integration of the systems. For example, when investigating serious crimes, it can take about 2.5 hours for a police to make a basic check of personal details of the suspect. In the future policeman only has to give the persons social security number and name to the system and the policeman is able to get information from the new police information systems and from many public authorities such as the population register, and the public-safety answering point systems [34].

The major difference between VITJA and the old police information system projects was that the VITJA project started by analyzing polices processes with over 300 policemen when the old systems were built by information systems terms. The VITJA project also analyzed thoroughly the usability needs for the information systems and usability also has a great role in testing perspectives [34].

Major advancement for the police work comes from the new communications networks that enable the same information systems features on the field as in the office. This will for instance give the policemen to collect personal information from suspect right on the field when they earlier had to go to the police station [34]. This will make the police car polices office even more than it is today and the policemen have much better possibilities to offer different services on the field.

E. MOBI

The target of a Finnish national research, development and innovation program, 'Mobile Object Bus Interaction' (September, 2010 to March 2014) aims to create a common ICT hardware and software infrastructure for all emergency

vehicles [35]. This infrastructure includes devices for voice and data communications, computers, screens, printers, antennas and cablings. Additionally, the interlinking with factory-equipped vehicles' ICT systems is researched. The project utilizes the results of the related research project and aims to develop product concepts, which have potential in both domestic and export markets. The R&D scopes of MOBI have been integrated to the actualizations of study units since 2010. MOBI is a spin-off of the RIESCA project.

F. SATERISK

The idea to study risks related to satellites was created by students of Laurea in 2008 [36, 37]. Funding from TEKES was secured on 14.11.2008 and allocated for the period 1.9.2008 to 31.8.2011. The goal of SATERISK was to study the risks connected to satellite tracking and to ascertain if the use of satellite tracking ca generate further risks. The project analyses risks using different approaches: legal, technical and mode of use; it will also study potential future requirements and risks [38]. SATERISK has expanded into an academic multi-disciplinary collaboration with the University of Lapland, ITMO in St. Petersburg, Russia and the BORDERS network, coordinated by the University of Arizona, USA. In addition, the collaboration was extended with four companies in the field of satellite tracking and government officials such as customs and police in Finland. As towards future continuums and activities, there are two main spin-offs of SATERISK: the AIRBEAM FP7, and PERSEUS FP7. Here it is noteworthy that SATERISK inspired students' thinking and gave the possibility for something else to emerge; SATERISK temporarily moved students' minds far away from daily official routines and responsibilities. This clearly advanced the aspects of motivation. SATERISK also demonstrated that a student's expertise itself and student-workplace relations can trigger externally funded R&D projects. SATERISK is analyzed in [39].

G. MACICO

Multi-Agency Cooperation In Cross-border Operations (MACICO) is the Celtic-Plus project with nine partners from Finland, France and Spain [40]. The duration of the project is Dec 2011 – May 2014. It develops a concept for interworking for security organizations in their daily activity. It deals with cooperation of security organizations that do not use (in their day-to-day job) the same radio network, but in some missions could take benefit from a sharing of their respective infrastructure. Use cases such as pursuit of criminals across a border, close support of vehicles going through a border, and disaster relief operations require security organizations from both countries to communicate together and to continue to communicate with their control room [41].

IV. Research Findings

This Chapter includes the answers to the expanded and iterative research questions.

A. RQ1: How can optimal procurement and maintenance of police patrol cars' ICT systems be understood?

The five level maturity model, tested and validated within the RIESCA project, acts as a catalyst for IT continuity management implementation [42]. The maturity status of each ICT system should be validated according to the method presented in Fig. 7. Also, testing the readiness of extendibility of the selected systems needs to be studies as a part of POV.

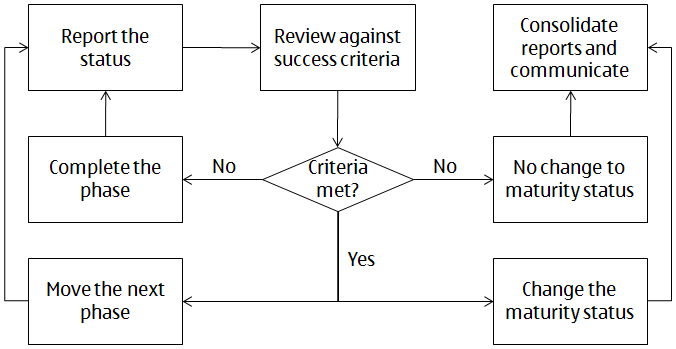

Fig. 7. Maturity status validation process [10]

B. RQ2: How can TUVE Network and its security requirements be understood in the perspective of police patrol cars?

In Finland, communications of police patrol cars are based on solutions provided by Virve (voice communications) and TUVE (data communications), meaning that the high security requirements for authorities' communications are fulfilled. This ensures secure integration of public networks and the Virve network. From technical point of view, the mobile use of TUVE is carried out utilizing multichannel routers, whose suppliers are invited to tender by The State Security Networks Ltd. New equipment should be operational by the end of 2014.

One of the main benefits that appeared within the TUVE project is that requirements for high security networks are specified at the ministry level. With better control of the ICT related costs brings synergy advantages. The government operated network removes dependence of single telecommunication operators. The common TUVE network facilitates the users interworking and communicating between and inside of different administrations.

Building a high security communications infrastructure and support for service model layers is time-consuming and requires a great number of decisions and contracts with hardware and software suppliers. These important data and communication systems for state safety must be available and usable in every security conditions. This concerns also natural phenomena, outages and cyber-attacks. Computational infrastructure must be scaled so that the relatively infrequent peak loads can be processed [1]. The communication system must be independent of single telecommunications operators. Information security must be ensured by efficient control and encrypting communications, but different authorities' services should be usable by other authorities as required. In practice, too strict data security regulations may rule out the mobile

utilizing of digital services in the field. However, most often the biggest cyber threat is so-called "insider threat" like Snowden and Manning cases indicate.

C. RQ3: How can KEJO be understood in the perspective of police patrol cars?

KEJO could be seen as a common mobile service platform for all PPDR actors. Roughly the common needs of the service platform and common services layer could be divided into two main areas: decrease in the number of physical Human-Machine Interfaces (HMIs), and a common field command system for all PPDR actors that also improves interoperability between different FR actors. However, several physical HMIs are needed for different modes of operation. For example, the HMIs when driving at full speed should be totally different than those in mobile office mode where ergonomics act an important role. Applying design principles of service oriented architecture, from end-users point of view, different existing systems seem as a one part of the field command system [3]. KEJO gives the opportunity to implement operational models for PPDR actors that support future plans and pay attention to special needs for different actors. KEJO should enable field management to all PPDR actors as well as maintenance, entering information from/to master systems and changing information in real time with different PPDR actors. KEJO should not include its own information pools but gets the needed information from master systems by inquiries and gives possibility to enter information to different master systems by applications. The principles of high secure private cloud environments could be applied. Zaerens and Mannonen [1] present an approach that enables to develop tools for producing dynamic or temporary high security private clouds according to specific needs and demands.

When looking at new actor-specific services for LEAs, unmanned border patrol systems, such as unmanned aerial vehicles (UAV), employ high-tech devices. A new ERV should be able to act as a mobile field command and control station. Future field command system standards should to take account of the control of UAVs.

D. RQ4: How can VITJA be understood in the perspective of police patrol cars?

The VITJA system will be taken into operations during 2014. The basic usage of VITJA will be possible within these LEA vehicles that have Win7/64-bit work stations. The VITJA project produces basic functionalities for reporting and register enquiries according to its own prioritization schedule. Usability of the VITJA systems can be optimized and it is estimated that with the more effective processes the annual impact will be entirely consistent with the work contribution of 300 man-years [34]. Also, police can offer better service for citizens, because the policemen have better systems on the field.

The fundamental consideration is that VITJA needs continuous on-line communication. This means that the functionality and reliability of mobile communications are highly important. The implementation schedule of other mobile functionalities of VITJA should be defined and carried out by the MOBI follow-up project PARVI.

E. RQ5: How can the integration of police patrol cars' electric, electronic and ICT systems be understood in the perspective of police patrol cars?

It is vital that different PPDR organizations will develop the common ERV concept together. There is a need for common services but there are also special needs for each actor. To fulfill both, common and special needs, we see that there is a need to apply private secure cloud environment. By secure multichannel data communications, it is possible to have information between public safety entering point and field management system in real time. This gives possibility to create common review and possibility to manage needed resources in field. Current systems can stay as master systems in the cloud and will fulfill the special needs for each author in Public Protection and Disaster Relief (PPDR).

The common service layer and the KEJO system will be the interface to the master systems in the secure private cloud. From master systems users will get needed information and through it they are able to enter new information. Master systems will be secured and controlled as required by Finnish law, but also the common system will have its own information security control as well as identification protocol of users.

The common service layer will help the interoperability with different PPDR actors; it enables for example better risk management, personnel management, business management, purchases, development and research work and agreements with different authors. It will strengthen ability to work together and gives possibility to have information in real time and management can manage resources better.

Common service layer can also provide comparable statistic of operation, economy, personnel and administration. Not to forget the savings in ICT investments due to synergy benefits.

F. RQ6: How can the risks of satellite-based tracking and navigation be understood in the perspective of police patrol cars?

Satellite-based tracking sensors and systems are very useful for law enforcement when tracking non-cooperative targets. The technical architecture of tracking systems is comprised of different segments, and each of these segments has its own set of risks and threats. Nowadays, law enforcement relies on and finds new uses for Global Navigation Satellite System (GNSS) technology to assist in investigating crime and gathering evidence. LEAs ought to have forensics technology for investigations and field work. These kinds of technologies include advanced tracking systems that apply GNSS technology to track criminals and vehicles that have been tagged. This allows LEAs to keep track of suspicious activity that can help solve cases.

In many field operations, also mobile monitoring systems are needed. A field command system is a complete solution and platform that integrates different applications into one easy-to-use interface. Most forensic services needed in the field should run on top of the field command system via a

standardized interface. Future field command system standards should take account of the control of forensic technologies, such as GNSS-based tracking systems.

G. RQ7: How can multi-agency cooperation in cross-border operations be understood in the perspective of police patrol cars?

MACICO project has studied a situation, in which a heist takes place in Finland. The Finnish police begin the chase to catch the criminals who move across the border to Sweden. It is obvious that the criminals are going move across the border several times during the chase. Finnish police operation center contacts the Swedish police operation center and explain the situation. It is agreed that the Swedish patrol continues chase in the Sweden and the Finnish patrol is allowed to go across the border if needed. Swedish command center activates needed features in the network and police patrols are able to communicate with each other fluently.

The communication flow for police in this kind of cross border operation consists of [41]:

1. Finnish police patrol detects a criminal car and starts chasing. It seems obvious that the suspect's car tries to escape to Sweden over the border.
2. Finnish police operations center contacts Sweden police operations center, asking for coordination for the chasing.
3. Swedish operations center activates two TETRA voice groups over TETRA Inter-System-Interface (ISI) in Swedish network: one for FI-SWE co-operation, one for Finnish police force to continue to communicate in their home voice group.
4. Finnish and Swedish operations centers command field units in the chasing to use those two voice groups as their purpose is.
5. Police patrols are able to communicate with each other during the mission.

Cross-border communication setup for the police:

1. Chasing started in Finland using national police home group: use Finland normal operational group.
2. Dispatcher of the operational group in Finland contacts Sweden police operations center via 1:1 call over ISI.
3. Both control centers activate the international co-op groups, which are interconnected via ISI.
4. Both control centers instruct the operative users of the chase to start using the interconnected groups (in addition to national group).
5. Finnish control center instructs Sweden center to activate home group for Finnish visitor (pre-provisioned to be connected to the corresponding police home group in Finland).
6. Finnish operative unit crosses border and authenticates to the Swedish network (home authentication over ISI). The user is pre-provisioned to Sweden network with pre-defined (limited) user rights.
7. Interconnected groups are used in co-operation (agreed to use English language).
8. Finnish police national home group is used by migrated Finnish unit, when communication entirely with Finland colleagues (in Finnish).
9. The chasing terminates in Sweden and the Finnish visiting operative unit returns to Finland making re-authentication in home network in Finland.
10. Finnish and Swedish operative centers agree to de-activate the groups over ISI.

V. Conclusion

This chapter includes the cross-case conclusions and evaluates the research process and the findings of this study from the viewpoint of the main research question of the study. Finally, suggestions for future research avenues are made.

A. RQ: How can empowering of policemen and their vehicles be understood?

It is vital that different public protection and disaster relief organizations will develop the common emergency response vehicle concept together. This enables new mobile digital services for first responders to their field operations. The MOBI research project has been an essential feasibility study finding out the requirements of all PPDR organizations and first responders in the field. However, more multidisciplinary research is needed.

Due to the significance and latest development of public procurement of innovative solutions, the ERV projects would benefit from further reviews and analysis of Pre-Commercial Procurement (PCP) and Pre-Operational Validation (POV), especially. Analyzing and reviewing the most advanced PCP and POV schemes would benefit the overall understanding of procurement issues. Moreover, the new projects should look for ways to develop the customer savvy in designing and carrying out PPI projects. Benchmarking with leading R&D intensive industries regarding purchasing of R&D services would give a broader view and better understanding of the business environment and best practices followed by leading private companies to complement the best practices followed by public procurers. Risk avoidance typical for many procuring organizations and "faster horse syndrome" are limiting the transfer to new and more advanced technologies. Finally, the projects should duly note the Council's conclusion on strengthening the internal security authorities' involvement in security-related research and industrial policy and thereby recognize the importance of the European Network of Law Enforcement Technology Services (ENLETS).

Within the duration of the MOBI project, the society has changed radically; applying of social media has exploded, and the authorities from the advanced countries have taken these matters into account when developing their digital services for public safety. For example with these advanced systems, people being first at the scene of the accident (involved and/or eyewitness) can communicate with PPDR authorities who are able to receive social media and multimedia messages into their operative systems. Unfortunately, many PPDR organizations see the Internet and social media only as an extra resource in which they can collect and transpose "material" to analyze it in their own systems. In practice, too strict data security regulations may rule out the mobile utilizing of digital services in the field. However, most often the biggest cyber threat is so-called "insider threat" like

Snowden and Manning cases indicate. When taken into account the Finnish cultural-ethnic environment, it could be invested in towards this security originated from end-users, rather than the strict technical data security by which the last 0.02% of confidence can be achieved.

B. Suggestions for Further Research

More research and development across two kinds of borders is needed.

Firstly, typical borderlines between public customers and private vendors, where tendering process is the main starting point of transaction, have to be modified towards pre-commercial procurement a tend prevailing R&D projects with front line experience.

Secondly, national borderlines have to be crossed as well in order to form coalitions with enough niche oriented purchasing volume to get tailored solutions for LEA´s vehicles from industries´ assembly lines. Even the richest small nations do not get the solutions wanted from automotive industry due to their limited volumes. Continued tailoring will not be sustainable in the long run.

Therefore true standardization on the European level is needed. International warehouses of crime are truly international in developing their technics, when will the LEAs be?

REFERENCES

[1] K. Zaerens and J. Mannonen, "Concept for the construction of high security environment in public authority cloud," in Embedded and Multimedia Computing Technology and ServiceAnonymous Springer, 2012, pp. 401-408.

[2] J. Rajamäki and T. Villemson, "Creating a service oriented architectural model for emergency vehicles," International Journal of Communications, pp. 44-53, 2010.

[3] J. Rajamaki, "Mobile digital services for border protection: Standardization of emergency response vehicles," in Intelligence and Security Informatics Conference (EISIC), 2013 European, 2013, pp. 256-261.

[4] (2013, Dec. 3). Mobile Object Bus Interaction. [Online] . Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10199203.

[5] T. Timonen and J. Rajamäki, "RFID technology as an inventory tool for future emergency service vehicles," in Recent Advances in Computer Science and Networking: Proceedings of the 2nd International Conference on Information Technology and Computer Networks (ITCN'13), 2013, pp. 142-145.

[6] R. K. Yin, Case Study Research Design and Methods. Thousand Oaks: Sage Publications, 2009.

[7] J. Edler and L. Georghiou, "Public procurement and innovation—Resurrecting the demand side," Research Policy, vol. 36, pp. 949-963, 9, 2007.

[8] ECORYS, "Study on pre-commercial procurement in the field of security within the framework contract of security studies – ENTR/09/050," ECORYS Nederland BV, Rotterdam, The Netherlands, 2011.

[9] P. Padding, "Sewcurity and safety. ENLETS," in Conference on Innovation Procurement, 2013, .

[10] K. Syrjänen, "Information technology (IT) perspective on maturity modelling and continuity management: An action and design research," in Integrative Student-Centred Research and Development Work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA), R. Pirinen and J. Rajamäki, Eds. Vantaa: Laurea Publications, 2010, pp. 68-111.

[11] G. Baldini, "Report of the workshop on "Interoperable communications for Safety and Security"," Publications Office of the European Union, 2010.

[12] A. Kivimäki, Wireless Telecommunication Standardization Processes : Actors' Viewpoint. Oulu: Oulun yliopiston kirjasto, 2007.

[13] G. Ameyugo, M. Art, A. S. Esteves and J. Piskorski, "Creation of an EU-level information exchange network in the domain of border security," in Intelligence and Security Informatics Conference (EISIC), 2012 European, 2012, pp. 356-358.

[14] J. Rajamaki, "The MOBI Project: Designing the Future Emergency Service Vehicle," Vehicular Technology Magazine, IEEE, vol. 8, pp. 92-99, 2013.

[15] S. Subik and C. Wietfeld, "Integrated PMR-broadband-IP network for secure realtime multimedia information sharing," in Technologies for Homeland Security (HST), 2011 IEEE International Conference On, 2011, pp. 20-25.

[16] M. Rantama and K. Junttila, "Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa," Tutkimusraportti.Pelastusopiston Julkaisu. vol. 16, pp. 2012, 2011.

[17] M. Rantama, "Mapping the future for Finland's rescue services," TetraToday, vol. Issue 3, pp. 32-35, 2011.

[18] J. Lehto, J. Rajamäki and P. Rathod, "Cloud computing with SOA approach as part of the disaster recovery and response in Finland," International Journal of Computers and Communications, vol. 6, pp. 175-182, 2012.

[19] P. Ofem and J. RAJAMÄKI, "Service Oriented Architecture: An Enabler of ICT Integration and Optimization in Public Protection and Disaster Relief Services," in Proceedings of the 8th WSEAS International Conference on Communications and Information Technology (CiT '14), 2014, pp. 346-359.

[20] (2013, Dec. 3). Vehicle installed professional mobile radio concept for law enforcement and fire & rescue operations. [Online] . Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10201742.

[21] H. Riippa, "Procurement at the finnish police," in Tekes Safety and Security Programme's Annu. Seminar, 2012, .

[22] (2013, Dec. 3). Projektipäällikkö – Kejo-hanke (Project Manager – Kejo Project). [Online]. Available: http://www.poliisi.fi/poliisi/bulletin.nsf/PFC/6FA46AF5EF825F98C2257AF3002E83A8.

[23] R. Pirinen and J. Rajamäki, Eds., Integrative Student-Centred Research and Development Work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA). Vantaa: Laurea publications, 2010.

[24] R. Pirinen, J. Rajamäki and L. Aunimo, "Rescuing of Intelligence and Electronic Security Core Applications (RIESCA)," WSEAS Transactions on Systems, vol. 7, pp. 1080-1091, 2008.

[25] Y. Benson, "Authority IT serving national security, " in VIRVE Day - Seminar, Helsinki, 2011, .

[26] K. Manni, "Security communications – possibilities and challenges," in VIRVE Day -Seminar, Helsinki, 2011.

[27] M. Lehti, H. Pursiainen, R. Volanen, R. Luoma, P. Timonen, R. Hagman and I. Kanane, "Promoting the availability of secure telecommunications networks," The Ministry of Transport and Communications Publication, Helsinki, 2009.

[28] H. Riippa, "The future of PPDR networks in Finland – Requirements and options," Presentation in the EU Workshop on the Future of PPDR Services in Europe, March 30, 2011.

[29] (2013, Dec. 3). Hallinnon turvallisuusverkkohanke TUVE. DOI: http://www.vm.fi/vm/fi/05_hankkeet/024_tuve/index.jsp.

[30] (2013, Dec. 3). TUVE-verkko ja sen liittymä muihin verkkoihin. VAHTI-teemapäivän 9.12.2010 esitykset. . DOI: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20101111VAHTIp/09_tuve_eskovainio_vahtipaeivae_09122010_www.pdf.

[31] P. Kortelainen and J. Ketola, "Pelastustoimen rekisteri- ja tilastointijärejstelmien tarpeet ja toteutusmalli. pronto X –hankkeen loppuraportti," Pelastusopiston julkaisu, Kuopio, Finland, Tech. Rep. B-sarja: Tutkimusraportit. 2/2012, 2012.

[32] HALTIK, "Tietopyyntö koskien viranomaisten yhteisen kenttäjärjestelmän (KEJO) toimitusta ja ylläpitoa," 2011.

[33] S. Haukka-Konu, "VITJA – rikostiedon varastoinnista tiedon hyödyntämiseen," Poliisi & Oikeus, pp. 14-15, 2012.

[34] K. Aaltomaa and M. Syrjänen, " Poliisin tulosohjauksen ja voimavarojen kohdentamisen kehittäminen " Sisäasiainministeriön julkaisut, Tech. Rep. 4/2012, 2012.

[35] J. Rajamaki, "The MOBI Project: Designing the Future Emergency Service Vehicle," Vehicular Technology Magazine, IEEE, vol. 8, pp. 92-99, 2013.
[36] J. Viitanen, SATERISK-Projektin Suunnittelu Ja Vaatimusmäärittely. Vantaa: Laurea-ammattikorkeakoulu, 2009.
[37] J. Ojala, Technical Tracking as Covert Coercive Measure for Police to Collect Information. Vantaa: Laurea University of Applied Sciences, 2010.
[38] P. Kämppi and R. Guinness, "Technical risk analysis for satellite based tracking systems," in Integrated Communications, Navigation and Surveillance Conference, Herndon, 2010, pp. M3-1-M3-16.
[39] J. Rajamäki, R. Pirinen and J. Knuuttila, Eds., SATERISK - Risks of Satellite-Based Tracking: Sample of Evidence Series. Vantaa: Laurea-University of Applied Sciences, Leppävaara Unit, 2012.
[40] L. Drouglazet, J. Rajamäki, J. Tyni and M. Aro, "Multi-agency cooperation in cross-border operations (MACICO) project," in Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14), 2014, pp. 129.
[41] P. Kämppi, J. Tyni and J. Rajamäki, "Use cases of the multi-agency cooperation in cross-border operations (MACICO) project," in Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14), Tenerife, Spain, 2014, pp. 209-212.
[42] K. Syrjänen, "Maturity-based continuity management," in Integrative Student-Centred Research and Development Work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA), R. Pirinen and J. Rajamäki, Eds. Vantaa: Laurea publications, 2010, pp. 68-111.