Laurea Julkaisut | Laurea Publications

LAUREA
AMMATTIKORKEAKOULU

Pasi Kämppi, Jyri Rajamäki, Seija Tiainen & Riku Leppänen (eds.)

MACICO

Multi-Agency Cooperation In Cross-border Operations

Samples of Evidence Series: Volume 4

Laurea Julkaisut | Laurea Publications | 38

Pasi Kämppi, Jyri Rajamäki,
Seija Tiainen & Riku Leppänen (eds.)

MACICO

Multi-Agency Cooperation In Cross-border Operations
Samples of Evidence Series: Volume 4

Cover pictures: Tapio Mäkinen

ISSN-L 2242-5241
ISSN 2242-5241 (print)
ISSN 2242-5225 (online)

ISBN 978-951-799-386-9 (print)
ISBN 978-951-799-387-6 (online)

Grano Oy, Espoo 2014

Content

Foreword / Pirinen 6
Preface MACICO Intro / Saijonmaa 7
Preface / Holmström 8
List of Abbreviations 9

Articles

1. Introduction I Pirinen 10
2. Related Projects I Pirinen 16
3. MACICO Project I Tiainen & Kämppi 24
4. Stakeholder Analysis I Kämppi 29
5. Technological Solutions I Kämppi & Holmström 35
6. Common Services and Operational Procedures I Rajamäki 41
7. Trust Building I Rajamäki 52
8. Authentic Evaluations, Case: Viksu 2014 I Leppänen & Kämppi 66
9. Discussion I Rajamäki, Savunen, Riippa & Knuuttila 74

List of Publications 81
List of Authors 84

FOREWORD - SAMPLE OF EVIDENCE SERIES

I extend my sincere thanks to participators and welcome you to reading the samples of evidence series which is addressed for proving that students can be as central actors in focused university strategy and Research and Development (R&D) related higher education and involved to the international R&D and its knowledge creation, transferring and dissemination.

The students' participation in publications, project preparation and even project management activities confirms that they are as central actors in Laurea's R&D. The generally high level of the MACICO results makes a continuum of implications that student-centric R&D is significant for development to the field for integration of R&D and novel pedagogy at Laurea. The outcomes of the student-centric R&D related learning in MACICO project were mainly based on Information Systems Research methodology and qualitative approach. Among universities of applied sciences in Finland, Laurea produces the relative high number of European Credit Transfer and Accumulation System (ECTS) credits from integrated R&D, such as MACICO project.

The strengths of the student-centric model are understood to be in equality, trust, confidence and the role of students as central actors and holders of responsibility in international R&D scale. The used integrative model maintains and supports open interaction through the operating environment. The recognized advances in learning by MACICO were related to the uniqueness of the realizations; "this spirit and way of learning and teaching was sole and real R&D related".

Rauno Pirinen
Founder of the Sample of Evidence Series
D.Sc. (Tech) - (Industrial Engineering and Management)
Ph.D. - (Computer Science and Information Systems)
Laurea University of Applied Sciences, Finland

PREFACE MACICO INTRO – AIRBUS

Interconnection of Public Safety radio networks has been on the agenda of the industry, operator, and user community in the form of standardization in European Telecommunications Standards Institute (ETSI) for over 15 years; the first milestone being the ´Three Country Pilot´, made between Belgium, the Netherlands, and Germany in 2003. Real operative use has, however, been delayed due to undeveloped forms of international cooperation in public safety, lack of business models to finance the development, and implementation, as well as regulatory and national security rules in some countries.

Airbus Defense and Space Oy (Airbus) has been active in the Terrestrial Trunked Radio (TETRA) network intersystem interface (ISI) developments over the past 15 years, the driver company in ETSI ISI-standardization and also in the interoperability of ISI implementations in TETRA + Critical Communications Association (TCCA). The Airbus objective in this topic has been development of the capability to support its customers' needs for interconnecting different countries' public safety TETRA radio networks together, and to also provide the needed radio communication service for cross-border visiting radio users. The MACICO project has been a good industry and research framework to develop solutions for Airbus' key nationwide TETRA radio network customers and to show the benefits of cross-border communication capabilities before there is the business model in place, in order to see commercial deployments. We anticipate this to take place in Scandinavian countries in 2015-16.

In the MACICO project, Airbus has further developed the TETRA ISI standards and the improved implementation of the TETRA ISI interface in the Airbus TETRA infrastructure to comply with the mandatory user requirements for cross-border cooperation of first responders. The major technical achievements have been full cross-border functionality between Airbus TETRA networks, the implementation of the TETRA talk group linking over ISI to provide international interoperability groups between users of several TETRA networks, as well as implementation of authentication of visiting TETRA terminals from a home network (TETRA ISI interface to deliver authentication and air interface session keys to the visited network) . Focus has also been on tools for TETRA operators to support the service.

The results of the Airbus MACICO TETRA ISI development are summarized in a TETRA-TETRA laboratory demonstration for cross-border incident management (between Sweden and Finland). The demonstration used migrating Airbus TETRA terminals and a fleet-map of voice groups to manage interoperation in a joint rescue operation. All developments have been made with Airbus' own intra and terminals, but compliance with the TCCA-defined test and certification has followed. Airbus has achieved TCCA certification for its TETRA infrastructure release6.0 ISI implementation. In coming developments after MACICO, the conformance with other TETRA manufacturers, especially Motorola, is a key target to enable implementation of Europe-wide TETRA networks interconnections.

Another Airbus objective in MACICO was to demonstrate TETRA service in a commercial Android terminal, using 4G radio access. A laboratory demonstration of this concept took place in 2012. This was the first step to show Airbus TETRA customers that they have, in the Airbus product roadmap, the capability for TETRA operators to add commercial 3/4G terminals to the existing TETRA networks, provide interoperability with existing TETRA terminals, and can expand their user base to critical infrastructure users, who prefer to use commercial terminals and also commercial cellular access networks, when the reliability of those comply with their requirements.

There has been good collaboration of MACICO Finland project partners to reach those goals of the MACICO project, set by Airbus.

Jaakko Saijonmaa, Dr.
Senior Expert, Head of CTO office,
Airbus Defence and Space Oy

PREFACE - AJECO OY

Modern societies rely highly upon reliable data communication. Information is an invaluable asset.

Reliable methods for transporting information are crucial. A constantly increasing amount of critical systems in a modern society are being remotely controlled and monitored. For example, but not limited to, the increasing need for remote control in power utility and grid applications, security surveillance, secure transactions in the commercial sector, and so on. The word "reliable" must be understood by its widest interpretation –reliable does not only refer to technical reliability, it refers to general trustworthiness, information security, and non-repudiation, as in providing proof of data integrity and origin, including authentication with a high assurance of being genuine.

Ajeco is the creator and inventor of a patented communications architecture named DSiP – Distributed Systems intercommunication Protocol (R) ™, or in short DSiP. The architecture is realized as a software suite consisting of node-, virtual-router-, control- and monitoring utilities. The DSiP system solution has been developed during the past 14 years, and it is used among several critical applications with operational status.

The DSiP solution is network- and technology agnostic in the sense that it is able to route data between network peers, regardless of the used physical means of transport. TETRA-, Satellite-, Mobile data-, LAN-technologies, for example, may all be used as parallel communications methods between network peers, however in such a way that the peers will not detect, or see, the different physical transport channels, regardless of link-performance and latencies, of course.

A very important factor in critical communications systems, in addition to reliability and security, is a concept called Common Information Sharing Environment, or in short CISE. In addition to providing multichannel communication, non-reputability, encryption, and security, the DSiP architecture provides means for solving complex compatibility issues providing interface and process ontology and methods.

Ajeco has focused on developing suitable multichannel router hardware and associated software in the MACICO, project. In addition to the aforementioned work, emphasis has been on reliability and security, taking into account developments in the field.

The work within the MACICO, project has been successful, efficient, and target driven. Ajeco expresses its gratitude to Tekes, the project partners in general, and especially the Finnish MACICO steering group, whom we have shared many interesting meetings and discussions with.

In Helsinki, October 21st 2014
John Holmstrom
CEO
Ajeco Oy

LIST OF ABBREVIATIONS

Abbreviation	Meaning
2G	Second Generation Wireless Telephone Technology
3G	Third Generation Wireless Telephone Technology
3GPP	The 3rd Generation Partnership Project
AAC	Automatic Access Control
ABC	Automated Border Check
ADSL	Asymmetric Digital Subscriber Line
AIRBEAM	AIRBorne information for Emergency situation Awareness and Monitoring
BCP	Border Crossing Point
CI	Critical Infrastructure
CPS	Cyber-physical system
CSR	Case Study Research
DSiP	Distributed Systems Intercommunication Protocol
DSR	Design Science Research
EES	Entry / Exit System
EMP	Electromagnetic Pulse
ENLETS	European Network of Law Enforcement Technology Services
ERV	Emergency Response Vehicle
ETSI	European Telecommunication Standards Institute
FR	First Responder
GAP	Guidance and Alarm System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
Horizon 2020	The EU Framework Programme for Research and Innovation
ICT	Information and Communications Technology
IP	Internet Protocol
ISI	Inter System Interface
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KATAKRI	Kansallinen turvallisuus auditointikriteeristö
LEA	Law Enforcement Agancy / Authority
LTE	Long Term Evolution
MACICO	Multi-Agency Cooperation in Cross-border Operations
MOBI	Mobile Object Interaction
OSSTM	Open Source Security Testing Methodology
PDCA	Plan-do-check-act
PMR	Professional Mobile Radio
POKE	Poliisin kenttäjohtojärjestelmä
PPDR	Public Protection and Disaster Relief
PPP	Public-private-partnership
PS	Public Safety
PSC	Public Safety Communications
PSCE	Public Safety Communications Europe
PTT	Push-to-talk
QoS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
RIESCA	Rescuing of Intelligence and Electronic Security Core Applications
RPA	Remote Piloted Aircraft
RTP	Registered Traveller Program
SATERISK	Risks of Satellite-based Tracking
SCADA	Supervisory Control and Data Acquisition
SDS	Short Data Service
SMS	Short Message Service
SOA	Service Oriented Architecture
SRA	Strategic Research Agenda
TCCA	TETRA + Critical Communications Association
TEDS	TETRA Enhanced Data Service
TETRA	Terrestial Trunked Radio
TETRAPOL	Digital FDMA PMR Standard
TUVE	Turvallisuusverkko
UAS	Unmanned Aircraft System
UAV	Unmanned Aircraft Vehicle
URS	User Requirements Specification
VIKSU 2014	Young Firefighters' Camp 2014
VIRVE	Viranomaisverkko

Rauno Pirinen

1. INTRODUCTION

This study of MACICO: Multi-Agency Cooperation In Cross-border Operations was addressed to the interactions and research and development (R&D) of security organizations and cross-border processes. The shared MACICO processes, described in this book, operates usually in dedicated networks and using of own systems and services, but which in some critical missions could directly and indirectly benefit by respective sharing of external activities, distribution of mission critical information, and sharing of information systems or information intensive infrastructure.

In a short-term scenario, MACICO project was addressed to the needs for improved systems, tools and equipment for radio communication in cross-border operations and during operations which were taking place on the territory of other member states as critical over border situations. In a long-term perspective, MACICO encompassed the interoperability issues of European countries and for formulation of transition from currently deployed legacy networks into the future broad band networks. The timeframe of MACICO was between December 2011 and December 2014.

MACICO was EUREKA framework and Celtic-Plus cluster related R&D project with nine consortium partners from Finland, France and Spain. As the macro-level steering forum, the EUREKA framework focuses on long-term initiative for securing and enhancing the European telecommunications industry. Here, the EUREKA framework addresses to the emergent innovations across borders and raising the productivity and competitiveness of European businesses through technology which was established by a Conference of Ministers of 17 countries and Members of the Commission of the European Communities, meeting in Paris on 17 July 1985. This was at a time when the European telecommunications arena and framework underway to move from an infrastructure and connection-driven industry to a services and application-solution driven industry.

EURECA framework shares CELTIC-PLUS cluster which is providing the needed support to the European industry. The participating countries in the CELTIC-PLUS are followed: Spain, Turkey, Sweden, Portugal, Poland, Norway, Israel, Ireland, Hungary, France, Finland, Germany, Belgium, Austria, United Kingdom and Switzerland. Each country has a responsible national public authority to address application.

In the time of this study, CELTIC-PLUS participants and interactions included major European telecommunications companies: this collaborations and interactions were enabling manufacturers such as Alcatel, Ericsson and Nokia and network operators including British Telecom, Deutsche Telekom and Telefonica to undertake R&D as well as the trial and evaluation of service concepts, technologies and system solutions at the CELTIC-PLUS' Pan-European Laboratory.

One of the main trigger to MACICO project and related investigations of the European Economic Community was the Schengen Agreement. The Schengen Agreement steered to the creation of Europe's borderless Schengen Area in 1995. The agreement was signed on 14 June 1985 between five of the then ten member states of the European Economic

Community near the town of Schengen in Luxembourg. It proposed the gradual abolition of border checks at the common borders by signatories. Proposal for measures included reduced speed vehicle checks which allowed vehicles to cross borders without stopping, allowing of residents in border areas freedom to cross borders away from fixed checkpoints and the harmonization of related visa policies.

In 1990 the Schengen Agreement was supplemented by the Schengen Convention which suggested the abolition of internal border controls and a common visa policy. The Schengen Area operates like a single state for international travel purposes with external border controls for travelers entering and exiting the area, and common visas, but with no internal border controls. Currently, Schengen Area consists of 26 European countries covering a population of over 400 million people.

1.1 Methodology

The MACICO study included the R&D, which comprised a continuum of R&D methods for increased understanding, and for building, improving and testing information-intensive artifacts and services, which were relevant both to the MACICO research and to the research strategy and R&D agenda at Laurea. The research rationale facilitated settings which were related to the integration of the MACICO project and activities of higher education functions, such as authenticity, emerge value, expertise networking and valuable relations between MACICO actors. Following from this, it was possible to understand a single R&D intervention in MACICO was as part of a larger collaborative network of R&D interventions and global knowledge transferring, collocation, scalability and dissemination in EU authority domain.

The integrative R&D models of MACICO build bridges between technologies, applications and services. It enabled research results to be transferred into products and services, and it created economic value returns among involved actors, such as related test environments, regional innovation systems and more global business actors. In the MACICO, it was understood that innovation alliances should be made between various stakeholders, particularly in science, business, and especially here as between politics and policy-based authorities.

In the R&D continuums of MACICO, vertical cooperation, namely lead innovations, such as described in next chapters, was geared toward certain services, applications and branches that benefit from specifically coordinated support from emergency technological domains. In collaboration and simultaneously with service platforms, technological alliances that further technological objectives were jointly created by science and solutions as well as aims of global business. Since the realization of study units included different types of future sense, which can be described by terms of "proactive, cooperation, co-design, co-creation, reflection and research activities".

Laurea's role in this "lead innovation MACICO system" was focused upon emergency service product innovations and the production of professional competences. In this integrative R&D model, the term "co-creation" as an activity of "mutual creation" pertains to an R&D collaboration, in which students and customers can be seen as "co-creators" of emergent values and information rather than as passive recipients of learned knowledge, goods and technology-based services. For this new cultural and higher educational change, the MACICO research focuses on "co-created" knowledge and "co-designed" products and services by encouraging the development of competitive "value co-creation" in the fields of safety, service and emergency-based authorities and MACICO related product development.

For consideration of the used tem "innovation" in this MACICO context: the setting of (Schumpeter, 1939) proposes five possible meanings to the term "innovation", followed: new goods; new processes; new markets; new sources of supply of new materials; and new organizational status. Here, probable, the most fitting for MACICO is setting by (Galanakis, 2006), which gives a broader meaning to the term "innovation", such as: the creation of new products; processes; knowledge or services by using new or existing scientific or technological knowledge, which provides a degree of novelty either to: the developer; the industrial sector; the nation or the world; or to succeed in the market place.

The one noteworthy methodological contribution of MACICO was the facilitation of a linear R&D framework and design for cyclic innovation activities that have research, action and quality returns. The system was a kind of "co-work system" within an innovation system framework and as a liberation process for innovative activities and support for knowledge-building rather than a fully automated process for innovation generation (Aanestad & Jensen, 2011; Alter, 2008).

In the MACICO studies, where the next methodological reflection was concerned, was in collective interpretation of related knowledge sources, technological elements and MACICO related solutions. The reasoning for the continuum of MACICO methods lies in the assumption that the MACICO consortium and activities of R&D-related higher education studies emerges value, expertise networking, value returns and relationships for involved actors and authorities (Pirinen, 2008).

In MACICO, the view of methodological continuum-focused and rigorous research was approached to be as a prerequisite for the sustainable developing and quality of networked expertise. In this context, the framework of the research continuum included: thinking and idea-building groups as co-creation forums; case study research for understanding; design research for building, improving and testing artifacts; services and methodology; and a "last-mile research" approach for general high-impacts and utility production, which in the end is addressed to value-building and economical returns on the national and global level (Pirinen, 2013; Rajamäki, 2014).

First, in MACICO the participants were involved in collaboration models in which achieved value comes from physical goods and artifacts but also increasingly from intangible things such as services, focused knowledge, and global relationships. In this shift of new emergent knowledge and the business model, the first empiric view can be compressed to the phrase "MACICO was R&D for transition to live", customers, and the role of higher education would be seen as "co-creators of value" rather than as passive recipients. This first knowledge-sharing dimension can also be described in more general terms as "thinking or idea-building space" or then as a "co-creation forum for pre-validation and synthesis of promising proposals for transition to live".

Next in MACICO, case study research was co-instructed extensively for bringing an understanding of a complex issue or object, and it can extend experience or add strength to what was already known through previous research, here understood as "focused knowledge continuums" (Yin, 2009). The implementation of case studies in MACICO emphasized the detailed contextual analysis of a limited number of events or conditions and their relationships, except when the relevant behavior cannot be changed or manipulated by researchers as advised in (Herr & Anderson, 2005). In addition, related case study lessons included such reference as: (Eisenhardt, 1989; Gerring, 2007; Miles & Huberman, 1994; Stake, 1995).

In MACICO, the case study inquiry relies on multiple sources of evidence, with data needing to converge in a triangulation fashion, and it benefits from the prior development of theoretical propositions to guide data collection and analysis. The term "triangulation" in MACICO refers to the usage of multiple sources of evidence such as: data sources, as data triangulation; among different evaluators, as investigator triangulation; perspectives of the same dataset, as theory triangulation; and multi-methodological approach, as methodological triangulation for improvements of continuum-focused methodology as research and learning approach (Campbell & Fiske, 1959; Patton, 1990; Robson, 2002).

Then, third in the MACICO research continuum, design research studies were considered to produce a viable and MACICO related artifact in the forms of a construct, model, method, or instantiation, and design science produces design science knowledge for the improvement of the activities of design and construction. In other words, in the setting of MACICO study, it produces the knowledge to implement and realize the emergency-related artifacts, services, methods and incipient innovations (Gregor & Jones, 2007; Hevner, March, Park, & Ram, 2004; Hevner & Chatterjee, 2010; March & Smith, 1995; Markus, Majchrzak, & Gasser, 2002; Simon, 1996).

Finally, probably the most reflective study efforts were concerned with the multi-methodological view of research and learning continuums. Here, our consideration was in line with setting that no particular research methodology should be regarded as the pre-eminent research paradigm, and no particular research methodology is sufficient by itself, as stated in (Nunamaker, Chen & Purdin, 1991). Following this, the focus of R&D outcomes of MACICO and evaluation would be in the prediction of research impacts, e.g., by way of using last-mile research, which includes three phases: proof of concept, which is close to the exploratory sciences; proof of value as the view in experimental sciences; and proof of use as an instance of applied sciences and engineering as referenced in (Nunamaker & Briggs, 2011). For remarks of future, our methodological proposal which first version is currently in press is titled as the continuum-focused methodology.

1.2 Learning by R&D

In this MACICO study, it can be concluded that learning was R&D related, it was realized as an integrative way of learning. Here, an individual learns along with a workplace, school, and R&D community, such as a research consortium of MACICO, as well as alongside a learning organization and across borders and disciplinary silos, as in a collective learning space that can be regional or individual-global oriented. Here, the research dimensions include learning, and an authentic research process and authentic research methodology were used for learning.

Then, in this MACICO study, the objectives of learning by R&D were associated through various formal and informal structures, such as R&D networks, actors and authorities, especially in developing students and learners to specialize in their areas of novel expertise where applicable knowledge was produced and mobilized in the collective R&D-related learning processes, which in this study were related to the externally funded R&D and MACICO research consortium's targets and the national research agenda.

Then, learning by R&D or learning within R&D of MACICO was addressed to the interactive collaboration within regional-national-international innovation systems and the development of regional focused and strategic learning purposes as well as regional capabilities and R&D profiles within trust-confidence relations and with regional-national governance policy in mind. In this study, learning by R&D within student-centered R&D was based on and included R&D and MACICO consortium interactions, and the term "student-centered R&D" comprised a student's mind-on and hands-on activities, social interaction, creating something new in learning within MACICO, and knowledge sharing and collaboration between individuals, communities of work, and global communities of R&D, see also reference "absorptive capabilities" in (Zahra & George, 2002)

The educational approach of this study was that learning by R&D shared a regional configuration, it employed R&D-related learning and knowledge sharing across industrial, service, governance and authority borders through regional-global R&D continuum and integration cf. regional configuration in (Harmaakorpi, 2004).

The reasoning for R&D-related learning and collaboration with higher education institutions and many other regional-national-international competence and knowledge producers, such as firms, entrepreneurs, authorities, funding organizations, and other academic institutions, focuses on the increasing importance of regional and national development and practical and scientific improvements.

In MACICO, the significant focus of higher education is on achieving a role as a cooperator and trusted partner of higher education functions, R&D networks, and research consortiums and on combining useful knowledge from multiple sources and co-creating it with other participating actors for novel and beneficial competences and capabilities related to authentic R&D projects, clusters, innovation systems, industry, research consortiums, and regional and national configurations. At the center of this focus is collective and R&D-related learning; here, the setting of MACICO study involves R&D and learning integration and collaboration activities with students, teachers, and regional networked R&D actors and authorities in shared MACICO environment.

In this MACICO study, the term "integrative model" or "integrative" refers to the student-centered integration of regional development, R&D, and higher education functions. The focus of an "integrative way" is on collaborative means of acting and learning in an interoperable and co-creative manner with other learners who are encouraged to develop their own ideas and train in competences to become developers and researchers at the regional-national-international level. In an integrative model, the learning transactions and increasingly R&D consortium-related knowledge transitions enable learners to contribute to their collective understanding, real targets, and regional capabilities as well as to focus on emergent innovations from their own ideas or more ready and focused lead-led innovation issues, such as MACICO issues, entities and mechanisms, in accordance with the themes of an international research consortium's targets and agenda. Confer advanced studies (Johansson & Ylinenpää, 2012; Rickne, Laestadius, & Etzkowitz, 2012).

Students of higher education are then at the center of the regional-global learning process, which conducts regional profiles, - capabilities, and - configuration by bridging novel knowledge and competences in a community of practice. In this MACICO study, the term "learner" refers to a student, teacher, researcher, or participant who enriches his or her own competence through collaborative R&D by sharing expertise and learning from others where R&D collaboration for learning is used, and "student" is used to indicate that a person is registered as a student in the database of the Ministry of Education and Culture.

Then, as a significant key purpose of this MACICO study is to address the form of higher education that focuses on the demands of the focused markets and its development, then, teachers and employer representatives must work together closely in an interoperative way as a collective learning community that can involve students and the implementation of study units in higher education and shared R&D, such as the activities of international research consortiums and work packages as knowledge absorptions and realizations in an integrative way. Confer "possible realizations of the focused university strategy and model" in (Clark, 2007)

In the operative environment of this study, higher education institutions are traditionally seen as contributors of new knowledge, services, and technology. However, MACICO is taking place with regard to cooperation in emergent value networks, co-created innovation, the contribution of pioneering innovations, and regional development affecting social and global development. In this view, new types of learning integration, trust, confidence, and collaboration are required for the stimulation of creative innovation in services, technology, the economy, and society. In the context of this study, it was expected that research conducted by learning and usefulness of new knowledge, as different forms of R&D-related learning that are based on the demand for development of the markets, can be used in the workplace to generate new competence and regional capability, which is the ability to do something, e.g., the regional capabilities to increase productivity and development in a region by using a research-oriented approach and support for a learner's

imagination and creativity in integrative learning transactions, especially in the sense of interactions and collaborative functions of higher education institutions and regional configuration, governance policy, and strategy scenarios.

In the context of this MACICO study, the terms "knowledge" and "learning" refer to understanding the complexity of the operative and authority related environment to identify the influences behind various regional-global phenomena, and knowledge refers not only to the governance of contents and applications but also includes the understanding of processes and practices by which information and R&D dissemination efforts are produced. The terms "collaboration" and "shared" address the realization of the authentic R&D that is implemented collectively in study units and learning in a student-centered and collective way within R&D action and regional R&D configuration settings.

In the MACICO, the terms "integrative learning space" and, for example, "MACICO research consortium," refer to internal, external, national, and international networks and forms of funded R&D consortia, which help participants to build their own communities of work and expertise and emergent value networks. Competent graduates of higher education would then have comprehensive expertise and capabilities in various disciplines. This implies gathering and processing information, reflecting on one's own experiences, sharing knowledge with others, and continuously developing one's own working methods, such as the learners' sustainable and lifelong growth and development. As remark of chapter, this MACICO type of integrative learning spaces improves the thematic targets of regional configuration, regional strategies, and the needs of workplace development.

References

Aanestad, M., & Jensen, T. B. (2011). Building nation-wide information infrastructures in healthcare through modular implementation strategies. *Journal of Strategic Information Systems*, 20, 161-176.

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems*, 17(1), 448-469.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin*, 56, 81-105.

Clark, B. (2007). *Creating entrepreneurial universities: Organizational pathways of transformation.* Bingley: Emerald Group Publishing Limited.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(1), 532-550.

Galanakis, K. (2006). Innovation process: Make sense using systems thinking. *Technovation*, 26(11), 1222-1232.

Gerring, J. (2007). *Case study research principles and practice.* Cambridge: Cambridge University Press.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems*, 8(5), 312-335.

Harmaakorpi, V. (2004). *Building a competitive regional innovation environment.* (Doctoral dissertation, Helsinki University of Technology Lahti Centre). Doctoral Dissertation Series.

Herr, K., & Anderson, G. L. (2005). *The action research dissertation: A guide for students and faculty.* Thousand Oaks: Sage Publications.

Hevner, A. R., & Chatterjee, S. (2010). *Design research in information systems: Theory and practice.* New York: Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75-105.

Johansson, J., & Ylinenpää, H. (2012). Can regional innovation systems be "constructed"? In A. Rickne, S. Laestadius & H. Etzkowitz (Eds.), *Innovation governance in an open economy: Shaping regional nodes in a globalized world* (pp. 208-230). London: Routledge.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251-266.

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A design theory for systems that support emergent knowledge processes. *MIS Quarterly*, 26(3), 179-212.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* Thousand Oaks: Sage Publications.

Nunamaker, J. F., & Briggs, R. O. (2011). Toward a broader vision for information systems. *ACM Transactions on Management Information Systems*, 2(4), 1-12.

Patton, M. (1990). *Qualitative evaluation and research methods* (2nd ed.). London: Sage Publications.

Pirinen, R. (2008). Integrative learning environments in perspective of regional development. *Pascal International Conference*, University of Limerick, 1(28), 1-10.

Pirinen, R. (2013). *Towards realization of research and development in a university of applied Sciences.* (Doctoral dissertation, University of Eastern Finland). Dissertations in Forestry and Natural Sciences, (No 108).

Rajamäki, J. (2014). *Studies of satelite-based tracking systems for improving law enforcement.* Jyväskylä Studies in Computing, Dissertation, (No 192).

Rickne, A., Laestadius, S., & Etzkowitz, H. (Eds.). (2012). *Innovation .governance in an open economy: Shaping regional nodes in a globalized world.* London: Routledge.

Robson, C. (2002). *Real world research* (2nd ed.). Oxford: Blackwell Publishing.

Schumpeter, J. (1939). *Business cycles: A theoretical, historical and statistical analysis of the capitalist process.* New York: McGraw-Hill.

Simon, H. (1996). *The sciences of the artificial.* Cambridge: MIT Press.

Stake, R. (1995). *The art of case study research.* Thousand Oaks: Sage Publications.

Yin, R. K. (2009). *Case study research design and methods* (4th ed.). Thousand Oaks: Sage Publications.

Zahra, S. A., & George, G. (2002). Absorptive capacity: A review, reconceptualization, and extension. *Academy of Management Review*, 27(2), 185-203.

Rauno Pirinen

2. *RELATED PROJECTS*

This second chapter describes the related research and development (R&D) projects as continuums alongside of the R&D scopes into the realizations of MACICO. The interrelated projects were examined based on what was already known and presented in relation to the MACICO. The chapter takes followed order of themes: technology evaluation and harmonization, mobile broadband, gateways and interoperability, information security, environmental risk management, decision making and operative activities, and finally description of MACICO related public safety research at Laurea. Here, the acronyms are especially difficult to remember, since both "certain acronyms and explanations" are retained through this chapter.

2.1 Technology evaluation and harmonization

2.1.1 THREE-COUNTRY PILOT

Establishment of MACICO was first approached by project called THREE-COUNTRY PILOT, realized between 2002 and 2003. The THREE-COUNTRY PILOT was mainly addressed to the future research, related needs and implications, such as: emergency call handling in remote networks, e.g., cross-border proposals which needed investigations and assistance; facilitation of automatic vehicle location information in cross-border and remote networks; Full Inter-System Interface (ISI); and validation and publishing of technical Terrestrial Trunked Radio (TETRA ISI) standard. The main focus of THREE-COUNTRY PILOT was addressed to voice applications, especially, TETRA in the region of Aachen–Maastricht–Liège.

In overall, THREE-COUNTRY PILOT project was the first project to the research of cross-border communication opportunities. Its objective was to standardize the international business environment and the way of communication which involved the project between the participated countries. THREE-COUNTRY PILOT project was addressed to investigate how the cross-border cooperation works between countries and how successful it is in practice. THREE-COUNTRY PILOT project was focused on improving crisis communication between authorities and the citizens. The target was to improve ways of communication within the project and to create a guidebook on how to act in emergency situations.

One advanced proposal of THREE-COUNTRY PILOT included foreign emergency calls which were recommended to be recorded and archived. This setting allowed access for the location information of the vehicles and enabled the progresses of a TETRA ISI (Terrestrial Trunked Radio) (Full Inter-System Interface) standard network. The meant of standardization was underlined in situations when a clear common will exist to interact with each other to develop effective information systems, and improve legacy systems to connect to each other and sharing. Expected benefit of the standardization was addressed to the modularity, parts of the product and terminology which can probably be produced more openly anywhere and be bought according to open tender-procurement processes.

The communication proposal developed for the first stage of the THREE-COUNTRY PILOT was suitable for use at the European internal borders in an expanded form. In particular, the following factors were considered: opportunity of an incident-related regular entry of operational forces in foreign communication groups; joint further training and language courses; agreements on common basic rules of radio communications; and development of communication structures incorporating the requirements of international communication.

The first stage of THREE-COUNTRY PILOT project was characterized by the lack of a system interface enabling all operationally necessary functionalities. As a consequence, data transmission and emergency calls were not tested between the country networks. However, practical and common tests by operational staff of involved security agencies based on realistic operational scenarios has already proven. In the first stage of the THREE-COUNTRY PILOT project, European TETRA (Terrestrial Trunked Radio) standard provided the communication requirements for the future emergence of a new dimension of co-operation of security agencies in Europe.

It was understood in the THREE-COUNTRY PILOT projects that further development of the necessary system interface and subsequent continuation of the project on testing emergency calls, telephony and data transmission functions is as prerequisite for the comprehensive and successful realizations into day-to-day operations.

In addition, organizational and operational-tactical measures should be furthered at the same time so that the results of THREE-COUNTRY PILOT can be developed into transferable model solution for cross-border communications throughout Europe. It is noteworthy, that the new technology can make it possible to realize a new dimension of cross-border and interdisciplinary co-operation which had not yet been developed in the time of THREE-COUNTRY PILOT project.

2.1.2 PROSIMOS

PROSIMOS: Priority Communications for Critical Situations of Mobile Networks project (CE-02775351/00-39) studied new possibilities for wireless emergency communication in national and international environments between 2010 and 2011. PRIMOS project developed critical communication models for the implementation of PCPMN (Priority Communications on Public Mobile Networks) and designed the related technical solutions. PROSIMOS project also took notice of emergency situation in border areas where it is imperative that neighboring countries can co-operate effectively. Here, the PMR (Private Mobile Radios) like TETRA (Terrestrial Trunked Radio) and TETRAPOL (a digital professional mobile radio standard) were realized in Spain. The focus of R&D were on PCPMN (Priority Communications on Public Mobile Networks) in crisis situations for emergency bodies when these networks become overloaded to the point that emergency workers have trouble getting critical calls through.

2.1.3 ACRIMAS

ACRIMAS: Aftermath Crisis Management System-of-systems Demonstration project (FP7-SEC-2010.4.1-1-261669) between 2010 and 2012. The ACRIMAS roadmap elaborated a systematic development process for crisis management systems, procedures and technologies in Europe, to be implemented within the demonstration project. The ACRIMAS focused for gradual evolvement of crisis management capabilities through demonstration and experimentation activities, transfer of related knowledge between stakeholders and by promoting an environment for co-development of crisis management technology and methodology where users contributes researchers work together. ACRIMAS further emphasized to community-building, which was considerably supported by the execution of the subsequent of second phase, bringing together the various key stakeholders and the available infrastructures in a case-by-case DE (Demonstration or Experimentation) activity.

2.1.4 PPDR-TC

PPDR-TC: The purpose of Public Protection and Disaster Relief Public Protection Disaster Relief Transformation Center project (FP7-SEC-2012.5.2-1) was to standardize communication devices and ensure the interoperability of wireless broadband services in Europe. The timeline of PPDR-TC project is between 2013 and 2015. The project investigates the current solutions used in wireless broadband and how they should be progressed. The purpose is to collect data and specify the system requirement, create use scenarios, evaluate the performance and specify validation opportunities. The result of the project is wider network coverage and interoperability to currents systems such as PRM (Private Mobile Radios), TETRA (Terrestrial Trunked Radio) and realization of TETRAPOL (a digital professional mobile radio standard). In addition, the aim of PPDR-TC is to find technical specifications for the solution, get answers to the phone operator's readiness to offer the service and development of technology and standards. The excepted outcomes of PPDR are such as recommendations for standardization of architectural realizations and techniques with the services.

2.1.5 OASIS

OASIS: Open Advanced System for Disaster and Emergency Management project (FP6-2003-IST-2-004677) between 2004 and 2008: The objective of OASIS was to define and develop an Information Technology framework based on an open and flexible architecture and using standards. OASIS intended to simplify the co-operation between the information systems used by rescue service organizations, in a local or wider environment. The OASIS proposal is as the basis setting of a European Disaster and Emergency Management system. This system order and supervision was addressed to support response and rescue operations in the case of wide range emergencies.

2.2 Mobile broadband

2.2.1 SDR

SDR: Software Defined Radio Forum was established in 1996. The SDR Forum is a non-profit corporation which is dedicated to support innovate use of spectrum and advancing radio technologies that support essential or critical communications worldwide. Members are bringing to forum their own know-how about SDR (Software Defined Radio), CR (Cognitive Radio) and DSA (Dynamic Spectrum Access) technologies in all-round markets. The meaning is to meet better emerging wireless communications requirements, to reduce costs and to standardize families of products, technologies, and services. The SDR Forum acts as leading environment for its members which includes over 100 memberships to collaborate to reach these objectives, arranging possibilities to network with customers, partners and competitors. The SDR Forum consist of commercial, defense, and civil government organizations, and involves wireless service providers, network operators, component and equipment manufacturers, hardware and software developers, regulatory agencies, and academia.

2.2.2 SECRICOM

The SECRICOM project's (FP7-SEC-2007-1-218123) topic was to create Seamless Communication for Crisis Management for EU Safety: the system that ensures end-to-end secure transmission of data and services across heterogeneous infrastructures with real time detection and recovery capabilities against interruptions, malfunctions and failures. There were 13 partners in project from eight EU countries and the timeframe of project was between 2008 and 2012.

2.2.3 EULER

EULER: European SDR (Software Defined Radio) for wireless in joint security operations project (FP7-SEC-218133) between 2009 and 2012. EULER addressed to demonstrate how the benefits of SDR (Software Defined Radio) can be leveraged in order to drastically enhance interoperability and fast deployment in case of crisis needed to be jointly resolved. The produced activities span the following topics: proposal for a new high-data-rate waveform for homeland security, strengthening and maturing ongoing efforts in Europe in the field of SDR standardization, implementation of SDR radio platforms, associated assessment of the proposal for high-data-rate waveform for security, and realization of an integrated demonstrator targeted towards users.

2.2.4 SALUS

SALUS: Security and interoperability in next generation PPDR (Public Protection and Disaster Relief) communication infrastructure project between 2013 and 2016. The SALUS project (EU-FP7-313296) is addressed to develop and prototype to the PPDR next generation that is compatible with legacy communication technologies and fully converged with the 4G evolutionary wireless paradigms as well as supporting robust and reliable transmission of broadband data. The SALUS addresses to design, development and validation of the next generation PPDR network concept: support TETRA (Terrestrial Trunked Radio); TETRAPOL functionalities; security; privacy; seamless mobility; QoS (Quality of Service); reliability for mission-critical PMR (Private Mobile Radio) voice; and broadband data services.

2.2.5 METIS 2020

METIS 2020: Mobile and Wireless Communications Enablers for the 2020 Information Society (CNECT-ICT-317669) project between 2012 and 2015. METIS 2020 is one of the current projects which are focusing solely on mobile broadband. METIS 2020 is the first international large-scale research project studying 5G. Here, the aim is to create a vision of 5G networks that can provide the answer for alarmingly increasing mobile data traffic and storages of massive amounts of data.

2.2.6 DAVINCI

DAVINCI: Design and Versatile Implementation of Non-binary wireless Communications based on Innovative LDPC (Low-Density Parity Check) codes (FP7-ICT-2008-216203) project between 2008 and 2010. The DAVINCI project was intended to develop a framework for the planning, introduction, and assessment of groundbreaking non-binary digital wireless transmissions based on new-type of LDPC

codes and integrated link level procedures for next generation wireless communications. The DAVINCI project proved that non-binary technology has a lot of potential to improve or substitute the binary technology in the long term to meet the high spectral efficiency requirements of next generation wireless multimedia communications. The DAVINCI serve as a reference for possible benefits of the non-binary technology for wireless communications and for other communication media. The expected benefits for the future are such as: improved capacity, quality of radio access networks, and more low-cost prices for higher quality services.

2.3 Gateways and interoperability

2.3.1 FREESIC

FREESIC: Free Secure Interoperable Communications project (FP7-SEC-2011-285205) between 2011 and 2014. The R&D of FREESIC focused to develop a communications that can be connected to other systems and to the parties to transfer information with another organization online and for to share related knowledge smoother. The proposal of FREESIC was based on a universal gateway with customizable adapters that enable connection of third-party infrastructures to the Unified Communication Network.

2.3.2 HIT-GATE

HIT-GATE: Heterogeneous Interoperable Transportable Gateway for First-Responders (FP7-SEC-2011-1-284940) was focused on the development and maintenance of the existing network infrastructure between 2012 and 2014. The purpose of HIT-GATE was to improve the communication between countries and develop existing information systems in order to have access to all of their work in terms of appropriate data. In the HIT-GATE environment, the creation of a technical solution was based on IP (Internet Protocol) technology and the basic idea was to use a gateway that can be integrated into existing organizations, networks and devices. The focus of HIT-GATE was in technical interoperability between networks based on standard protocols to facilitate implementation and standardization and different technologies and standards, e.g., TETRA (Terrestrial Trunked Radio), TETRAPOL, PMR (Public Mobile Radio), WiMAX (Worldwide Interoperability for Microwave Access) and GSM (Global System for Mobile Communications) data transfers.

2.3.3 GERYON

GERYON: Next Generation Technology Independent Interoperability of Emergency Services project (FP7-SECURITY-284863) between 2011 and 2014 was a co-operational project between three different EU-projects, such as FREESIC, Hit Gate and PPDR above. The GREYON project focused into the base for technical specifications with which to accomplish the goal of technologically independent equipment. The goal was also to describe the architecture needed for connecting the different network technologies with each other. The aim of the project was to create as an innovation a system that can link different technological solutions to each other using standardized integration interfaces.

2.3.4 ESS

ESS: Emergency Support System (FP7-SECURITY-21795) project between 2009 and 2013 was indented to R&D for create framework that can effectively manage synchronization of data and information flow between the different public authorities. The ESS project planned reliably transmitted filtered and pre-organized information streams to the crisis command system. The data flows in ESS were organized so that it can easily to be joined together with other available applications and databases. The project planned to provide open API (Application Programming Interface) for public authorities to add needed or customized applications. ESS project contributed on ISO (International Organization for Standardization) and industrial standards.

2.3.5 IDIRA

IDIRA: Interoperability of data and procedures in large-scale multinational disaster response actions (FP7-SECURITY-261726) is current research project funded by the European Commission of four years between 2011 and 2015. It is gathering eighteen partners to focus on the interoperability of data and emergency procedures in response to large-scale disasters. IDIRA project tests a multi-national disaster relief organizations facility in the ability to operate in a real situation and also tests and develops data transfer and communication tools. The focus of project prepares practical guidelines for practices, best practices in communication and contributes actors in the region such as commanders, disaster control personnel and emergency responders.

The main expected result will be a set of recommendations, best practices and lessons learnt concerning processes, structures and interfaces that contribute to more interoperability and efficiency in large-scale disaster relief operations. The mobile components by the IDIRA can be used by the commanding personnel prospect for flexible interaction with the information space. Interoperability aspects regarding the following topics are reflected: multinational resource management; procurement management; ad-hoc integration of sensor data and of external expert systems, such

as simulation into a shared situation and operations' picture; missed person tracing systems; and early situation awareness.

2.4 Information security

2.4.1 EMSCB

EMSCB: European Multilaterally Secure Computing Base project (governed by Federal Ministry of Economics and Technology Germany) between 2006 and 2007. EMSCB was addressed to the development of reliable open source standards that contribute to information security problems of traditional platforms. The design and development of the plat-form was based on the newest system technologies on the market. It was addressed also to the easily connected to devices such as PDA (Public Displays of Affection), smart phone and embedded system. The basic idea was to offer the user a more reliable system that can protect them better against spyware and make possible to secure the hard drive and secure user identification. The hardware would offer to user as a good protection from information breaks. The open source platform would enable upgrades that are independent from service providers and can be updated at any time. The expansion of electronic systems, trading and services in the world requires companies to develop the systems that can protect against security attacks and provide a safe way to handle secured data. In the current operating systems there are still major gaps in information security level that needs to be fixed.

2.4.2 OPEN_TC

OPEN_TC: Open Trusted Computing project (FP6-IST-027635) between 2005 and 2009. The focus of OPEN_TC project was to reduce the threats to the system, system errors and malfunctions. Here, the viewpoint was that operating systems are vulnerable to viruses, worms, spyware and malware. OPEN_TC project proposed an open Trusted Computing framework which architecture was based on security mechanisms provided by low level operating system layers with isolation properties and interfaces to Trusted Computing hardware. These layers made it possible to demonstrate enhanced trust and security properties of the platform for standard operating systems, middleware, and applications.

2.5 Enviromental risk management

2.5.1 CHORIST

CHORIST: Integrating Communications for Enhanced Environmental Risk Management and Citizens Safety (FP6-IST-033685) between 2006 and 2009 addressed to environmental risk management in relation to natural hazards and industrial accidents project and related to the development of technical solution in the area of early warning. Those technical proposals were focused to help authorities in their work to saving lives in major natural or industrial disasters. The project improved risk assessment report systems to get info from crisis area and also speed up message sharing between citizens and authorities in natural hazards and industrial accidents.

2.5.2 ASPIS

ASPIS: Autonomous Surveillance in Public Transport Infrastructure Systems (FP7-TRANSPORT-218513) project between 2008 and 2011 was targeted the development of a prototype surveillance system based on smart monitoring devices that capture data lone upon the occurrence of an incident, potentially dangerous for the passengers such like an explosion blast or the triggering of the fire detector. When triggered, these devices propagate the triggering to their neighboring devices and send an alarm. Successively, they upload the captured data to the central station providing a wide space and time-wise coverage of the potentially hazardous incident. Finally, they provide a dedicated bi-directional communication channel between the emergency center and the affected areas. If, for any reason, they do not succeed to establish communication, they serve as black boxes, preserving the data until they are physically recovered by the authorities. This system was mainly progressed for the unattended surveillance of public transport and other public spaces. It serves primarily for the prompt and reliable situation awareness during the early, most critical emergency phase, thus greatly facilitating the overall crisis response.

2.6 Decision making and operative activities

2.6.1 DISASTER

DISASTER: Data interoperability solution at stakeholder's emergency reaction (FP7-SECURITY-285069) project between 2012 and 2015. According to DISASTER, the emergency management and information exchange become more challenging in an international crisis episode and processes because of cultural, linguistic and legal differences between all stakeholders, especially first responders.

Misunderstandings between first responders slow down decision-making and make it more difficult. The recent spread and development of networks and Emergency Management Systems (EMS) has facilitated communication and improved emergency responses, allowing them to become more coordinated and successful in overcoming distances issues, and allowing decentralized decision-making when necessary and appropriate.

2.6.2 SICMA

SICMA: simulation of crisis management activities (FP7-SECURITY-217855) project between 2008 and 2010 marked to create computer-assisted tools for crisis managers in health service. The integrated suite of modeling and analysis tools accelerated the decision-making process. Results are possible to integrate to other emergency services organizations. Project's goal was to create computer assisted decision making for Health Service crisis managers. Better capability to make decision was executed by an integrated suite of modeling and analysis tools and also to provide impression into to the common behavior of the entire organization in response to crisis scenario. In SICMA, an integrated suite of modeling and analysis tools were progressed. With this tool decision makers can get support in the preparedness, e.g., before the accident occurrence and response, e.g., after accident occurrence phases. Selected scenarios were an armed terrorist attack and chemical terrorist attack. A case-study scenario clarified the needs, feasibility relevance and efficiency of the proposed approach. Results of the project was a prototype which contained modeling and simulation tools, graphical user interface (GUI) for user to generate a scenario, run a simulation and browse the results.

2.6.3 CRISMA

CRISMA: Modelling Crisis Management for Improved Action and Preparedness (FP7-SECURITY-284552) project between 2012 and 2015. CRISMA focuses on providing a support tool which will help local authorities, responders, communities and private sector organizations to prioritize the most effective disaster response and mitigation methods for various potential incidents. CRISMA project is coordinated by Technical Research Centre of Finland (VTT), CRISMA will use modelling and simulation technologies for evaluating the effects of crisis management measures on hypothetical scenarios. An integrated modelling system is being designed into CRISMA to simulate the most likely of crisis situations and more remote scenarios, the required measures, and their effects. Domino and multi-risk effects will also be taken into account; here the integrated modelling system will give opportunities to assess the impacts of natural disasters on chemical, nuclear and other industrial activities, and critical infrastructures. CRISMA Integration Project focuses on large scale crisis scenarios with immediate and extended human, societal, structural and economic, often irreversible, consequences and impacts. Typically, these crisis scenarios cannot be managed alone with regular emergency and first responder resources, but require multi-organizational and multi-national cooperation including humanitarian support.

2.6.4 U-2010

Project called U-2010: Enterprise next generation Network Vision 2010 and Ubiquitous IP Centric Government and Enterprise Next Generation Networks (FP6-IST-035003) was the demonstration project were among the ten activities in crisis and disaster situations in Europe. U-2010 project provided effective access to information for all parties involved in an accident and the use of new innovative solutions. The project trained persons performing in rescue area to communicate better and more smoothly by using existing services and networks. The project was also utilized in the unused channels of communication, and was redirected to another device in communication failures including such interest as: interconnecting existing services and networks; leveraging redundant communication channels; using automatic redirection and service transition in case of failures; using new research results in the area of wireless ad-hoc networks; and innovative communication technologies based on Internet Protocol version 6.

2.6.5 COSMIC

COSMIC: Contribution of Social Media in Crisis management (FP7-SECURITY-312737) between 2013 and 2015. In the key focus of COSMIC project, there is that social media is a phenomenal tool for disseminating information quickly and has become an integral part of everyday life around the world. Hence, recent years have marked a light the use of new communication media during crisis situations and disasters. Citizen journalism has proliferated around the world, where news, events and oddities are recorded by ordinary people and shared globally through mediums such as YouTube, Twitter, Facebook and other outlets. COSMIC project emphases to the development of scenarios that consider possibilities for their use in crisis situations by the public, officials and first responders, and examines the role of citizens as first responders, social activists and citizen journalists in new media communication, and the ethical issues and political consequences of citizen participation. The target is a set of guidelines for citizens, government authorities, first responders and industry for the most effective use of ICTs to aid citizen security during crises.

2.7 Related public safety research at Laurea

2.7.1 RIESCA

RIESCA: Rescuing of Intelligence and Electronic Security Core Applications (TEKES SEC 2007-2013 between October, 2007 and March, 2010). RIESCA was the first of our externally funded R&D projects. 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 target of RIESCA was to offer contributive and constructive solutions, such as design science research based solutions, focused to this problem. 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 (Pirinen & Rajamäki, 2010).

2.7.2 SATERISK

SATERISK: Risks of Satellites and Satellite Tracking System (TEKES SEC 2007-2013). The idea to study risks related to satellites was created by students at Laurea in 2008. 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 can 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. 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 example of future continuums and activities, there are two main spin-offs of SATERISK: the AIRBEAM FP7, and PERSEUS FP7 at Laurea. SATERISK also demonstrated that a student's expertise itself and student-workplace relations can trigger externally funded R&D projects (Pirinen, 2013; Rajamäki, Pirinen, & Knuuttila, 2012).

2.7.3 MOBI

MOBI: The target of a Finnish national research, development and innovation program, 'Mobile Object Bus Interaction' (TEKES SEC 2007-2013 between September, 2010 and October, 2013). MOBI focused to create a common ICT hardware and software infrastructure for all type of emergency vehicles. This infrastructure includes devices for voice and data communications, computers, screens, printers, antennas and cablings. Additionally, the interlinking with factory-equipped vehicles' ICT systems was researched. The project utilized the results of the related research project and aimed to develop product concepts, which included potential in both domestic and export markets. MOBI was a spin-off of by RIESCA. The R&D scopes of MOBI have been integrated to the realizations of study units since 2010. The MOBI project is concluded to (Rajamäki, 2014; Tikanmäki, Rajamäki, & Pirinen, 2014).

2.7.4 PERSEUS

PERSEUS: Protection of European borders and Seas Through the Intelligent Use of Surveillance (FP7-SECURITY-261748 between January, 2011 and May, 2015). PERSEUS represents the first demonstration project implemented by the FP7 Security Research Theme. The demonstration represents a novelty for the EU Framework programs. PERSEUS is addressed at large-scale integration, validation and demonstration of novel security systems of systems, and represents European flagships, providing a federative frame to join research in areas of significant European interest. PERSEUS is expected to deliver tested, demonstrated and validated recommendations and is coordinated by INDRA Sistemas S.A, with 29 partners (Pirinen, 2014).

2.7.5 AIRBEAM

AIRBEAM: AIRBorne information for Emergency situation Awareness and Monitoring (FP7-SECURITY-261769 between March, 2011 and February, 2015) is a Seventh Framework Programme (FP7) project related to crisis management. The goal is to develop a multi-platform approach to situational awareness for crisis management, especially utilizing Unmanned Aerial Vehicles (UAVs), aerostatic platforms and satellites. In addition to EADS, the AIRBEAM consortium includes 22 partners, including some of the largest high-tech companies in Europe. The role of Laurea is as the coordinator of first Work Package of AIRBEAM, which focuses on studying potential concepts of use and specifying end-user requirements. This work is in close collaboration with end-user organizations as continuum of MayFly.

2.7.6 CBPI

CBPI: Cross-Border Photonics Initiative (2007-2013 South-East Finland-Russia ENPI CBC between November, 2012 and November 2014) is Finnish-Russian collaboration project related to photonics technology. The project aims to increase regional economic development, transfer knowledge and

technology and increase cross-border scientific cooperation. The consortium includes five partners; four universities from Finland and Russia and one technology company. The other partners are highly respected in the field of photonics research and production. In CBPI project, Laurea UAS' focus is to test the latest Unmanned Aerial Vehicle (UAV) technology in simulated border areas. After the demonstrations, the data will be analyzed from the perspective of border security.

2.7.7 ABC4EU

ABC4EU: Automated Border Control Gates for Europe (FP7-SECURITY-312797 between 2014 and 2017) is European Union wide R&D project and involves a Consortium of 15 partners from 8 different countries. The purpose is to make border control more flexible by enhancing the workflow and harmonizing the functionalities of automated border control gates. Project started in January 2014 and will last for 42 months. The project is led by INDRA Sistemas S.A. from Spain. During the last years, many ABC Gates have been deployed in the main European airports, most of them as pilot projects intended to test their capability to improve the border crossing processes in aspects such as speed, security, automation, and false rejection reduction. In particular, harmonization would be required in areas as e-passports management, biometrics, gate design, human interface, parallel processes, signaling and interoperability.

2.7.8 EU_CISE

EU_CISE: European Union's Information Sharing Environment addresses to steps forward along the accomplishment of the European roadmap for Common Information Sharing and Distributed Systems and Services Environment. The current plan for timeframe of EU_CISE is between 01/12/2014 and 01/06/2017. The project attains the widest possible experimental environment of innovative and collaborative services and processes between European maritime institutions grosses as reference a broad spectrum of factors in the field of European Integrated Maritime Surveillance, arising from the European legal framework, as well as from studies, pilot and related R&D projects. ■

References

Pirinen, R. (2013). *Towards regional development by higher education institutions: An empirical study of a university of applied sciences.* (Doctor of Science (Technology), University of Oulu). Acta Universitatis Ouluensis, C Technica 449.

Pirinen, R. (2014). Studies of integration readiness levels: Case shared maritime situational awareness system. *IEEE Conference on Joint Intelligence and Security Informatics (JISIC)*, Hague. pp. 212-215.

Pirinen, R., & Rajamäki, J. (Eds.). (2010). *Integrative student-centered research and development work: Rescuing of intelligence and electronic security core applications (RIESCA). Sample of evidence series: Volume (1).* Vantaa: Laurea publications.

Rajamäki, J. (2014). *Studies of satellite-based tracking systems for improving law enforcement.* (Doctoral Dissertation). Studies in Computing. University of Jyväskylä.

Rajamäki, J., Pirinen, R., & Knuuttila, J. (Eds.). (2012). *SATERISK risks of satellite-based tracking: Sample of evidence series: Volume (2).* Vantaa: Laurea publications.

Tikanmäki, I., Rajamäki, J., & Pirinen, R. (Eds.). (2014). *Mobile object bus interaction designing future emergency vehicles: Sample of evidence series: Volume (3).* Vantaa: Laurea publications.

Seija Tiainen & Pasi Kämppi

3. MACICO PROJECT

The problem behind the MACICO (Multi-Agency Cooperation in Cross-Border Operations) project is that authorities in different countries, sometimes even different authorities in the same country, use their own separate professional mobile networks based on fragmented technological implementations. Roaming, interoperability, or common operational procedures do not exist. But in crisis situations and cross-border operations, the need of safe and secure communication is obvious. MACICO was launched to find solutions to improve interoperability of communication on all levels: users, operating procedures, services, service providers, and technology. The objective was better communication between security authorities and organizations and better public safety. The objective was also to find new business opportunities and create ideas for new services.

Rajamäki, J. & Aro, M. (2014). Multi-Agency Cooperation in Cross-Border Operations in the Field of Public Protection and Disaster Relief. International Journal of Education and Information Technologies, Volume 8.

Abstract— The technological aspects of TETRA (TErrestrial Trunked RAdio) ISI (inter-system interface) have been possible for more than a decade. ISI and interoperability between different organizations in different countries were already tested in 2003 in the Three Country Pilot, regarded as phase 0, and again in 2009 in the Rakel-Bosnet pilot project (phase 1). The basis of interoperability comes from EU Commission Council Recommendation on improving radio communication between operational units in cross-border areas (Doc. 10141/09 ENFOPOL 143 TELECOM 116 COMIX 421) of the 4-5 June 2009. This article introduces the Multi-Agency Cooperation In Cross-border Operations (MACICO) project. The initial purpose of the MACICO project is to point out the need for an ISI or similar interfaces between different public safety networks.

3.1 MACICO as an International Research Community

MACICO was a Celtic-Plus project. Celtic-Plus is part of EUREKA, an inter-governmental network of 41 members in Europe, including the European Commission. EUREKA funds and coordinates market-oriented R&D and innovation projects of industry, research centers, and universities across all technological sectors.

The project consortium of MACICO was formed by 9 partners from 3 countries and different industries (see table 3-1). Cassidian France was responsible for coordinating the project. The project started in December 2011 and lasted until May 2014.

Table 3-1: Consortium of Celtic MACICO

Company name (Leading contractor first)	**Country**	**Type**
Cassidian (Airbus De-fence and Space)	France	Industry
Ajeco	Finland	SME
Altech	Spain	SME
Cassidian Oy (Airbus De-fence and Space Oy)	Finland	Industry
Eolane	France	Industry
Genaker	Spain	SME
Laurea	Finland	University
Prescom	France	SME
Tradia I S.A (Abertis)	Spain	Telco

The budget of Celtic MACICO was over 9 M€, and it included 65.000 person years. MACICO partners received funding from their national funding organizations.

MACICO addressed six technical domains of Celtic. The main focus was Mobile & Wireless. But MACICO was also related to Networks, Services & Applications, Management of Services and Networks, CPE/N and Terminals, Security and Broadband Access Networks.

The MACICO project was divided into six work packages:

- **WP1: Project management;** gathers all efforts regarding the coordination of the project
- **WP2: End users requirements capture**; gathers all work related to the interaction with end-users. It is organised around a framework for gathering operational scenarios and requirements, as well as systematic methodology for harmonisation of needs at European level.
- **WP3: Architecture & Standard operating procedures**; compliant with users require-ments and scenarios, the architecture of interoperability means, and the operating procedures to deploy and use them will allow Security Forces authorities to appreciate the tools they could get, their capabilities and the risks that such interoperability could introduce in their already deployed PMR networks.
- **WP4: Implementation for multi-agency interoperability**; will provide the ISI technology. Significant improvements will be achieved with respect to feasibility, performance, reliability, speed and cost of operations thanks to radio communication.
- **WP5: Demonstration**; consists in showcasing the MACICO project achievements.
- **WP6: Dissemination and standardisation**; deals with efforts to promote the project achievements outside the consortium, in the community at large, and to setup the implementation of a standardisation roadmap. Standardisation aspects will be addressed in the project with particular focus on the collaboration with standard making and regulatory bodies with the aim of influencing the development of international standards. The project will establish links with ETSI, ITU, OMG, TETRA MoU, and other relevant standardisation organisations that have interests in the areas relevant to public safety communications. The presentation and the progress of the project will be available on a public website. For an efficient collaborative work we will create private site with forum, private messages and document sharing.

Laurea was the leader of WP2 (End-user requirements) and WP6 (Dissemination and standardization).Laurea also took part in other WPs, like WP5 (Demonstration). As part of WP6, Laurea implemented the logo of the project, web pages of MACICO (www.macico.com), and the virtual working

environment (www.macico.com/wiki), to be used by consortium members. The project plan of the international MACICO project is found in the Celtic Project Description: MACICO (2011).

Celtic Project Description: MACICO - Multi-agency cooperation in cross-border operations (2011). Unpublished

Abstract - MACICO will develop a concept for interworking of security organisations in their daily activity. It deals with cooperation of security organisations that do not use (in their day-to-day job) the same radio network, but in some missions could take benefit of a share of their respective infrastructure. Use cases such as pursuit of criminals across a border or close support of vehicles going through a border, disaster relief operations (water flood, earthquakes...) require security organisations from both countries to communicate together and to continue to communicate with their control room.

The members of an organisation must be allowed to use the foreign radio net-work to communicate. But the way to organize this foreign use of a radio net-work is to be defined and validated by security organisations authorities (availability of terminal for foreign users, their configuration, group communication over the border, ciphering mechanisms, control on gateways, ...)

The work of the project will be carried out in cooperation with the public safety organisations that will be in charge to define under which conditions members from foreign organisations a priori working on heterogeneous networks will be able to cross the borders and how and to whom they shall communicate, without putting in danger the security features of the radio network.

The requirements for these communications will be led on concrete use cases (such as France-Spain, France–Belgium, Switzerland-Germany, Switzerland-France and Finland-Estonia borders; content and demo location are to be discussed in the frame of the project). Interworking at the border will then address Tetra-Tetrapol, Tetra-Tetra, and Tetrapol-Tetrapol interworking as well. From these requirements, the definition on the way to deploy terminals to foreign organisations, the way to organize and to deploy the solutions including gateways, will be declined in any of interworking cases.

The test bed developed in the project will consist in proving the capability for the users to exploit the foreign radio network to communicate with all the members of the "border" communication (radio from both networks, control room from both networks). Of course the development of the necessary "gateways" that will allow the communication across the border will be part of the test.

The project is innovative because it addresses not only the interoperability issue, but also the complete procedure that accepts foreign users on a security radio network (which is a priori forbidden for them) and look for a solution that keeps the intrinsic security mechanisms of such networks. Moreover MACICO paves the way towards the development of strong and meaningful interactions between narrowband public safety and LTE broad band networks.

Drouglacet, Rajamäki, Tyni and Aro (2014) describe in their article the planning process and set-ting the objectives of MACICO.

Drouglazet, L., Rajamäki, J., Tyni, J. & Aro, M. (2014). Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14).

Abstract: - Multi-Agency Cooperation In Cross-border Operations (MACICO) is the Celtic-Plus project with nine partners from Finland, France and Spain. The duration of the project is Dec 2011 – May 2014. It develops a concept for interworking for security organisations in their daily activity. It deals with cooperation of security organisations 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 organisations from both countries to communicate together and to continue to communicate with their control room. The paper presents the MACICO research project.

3.2 MACICO as a National Research Community

In Finland, partners of the MACICO project, Ajeco, Cassidian Oy, and Laurea, had their own, individual projects and budgets, but they worked together in close co-operation. The funding of the projects came from Tekes – the Finnish Funding Agency for Innovation. Laurea's budget in MACICO was 1 M€.

Laurea's plan of exploiting the results of MACICO was to communicate end-user needs and requirements in a cost-effective and efficient way to developers and to bridge the communications between the public and private sector in order to make it easier to do business in Europe. To be able to fulfill all the plans, Laurea's MACICO project was extended to last until the end of 2014. One of the important activities during the last half of the project was to carry out an evaluation of operating procedures and technological solutions

in Viksu 2014, a young firefighter's camp in summer 2014. Other activities were, for example, to analyze and evaluate all the results from the demonstrations and publishing the results in this publication. To implement activities in Viksu 2014, the national MACICO community got new members from Eye Solutions and Viksu 2014 camp organization outside of the original national consortium (Airbus, Ajeco and Laurea). Eye Solutions is a partner of Ajeco and offers situational awareness solutions with ECC application and video clients to Android phones and tablets.

3.3 MACICO as a learning environment

Learning by Developing (LbD) is a pedagogical approach developed by Laurea University of Applied Sciences. In RD&I projects, the students, both bachelor and masters level, are responsible of implementing R&D-subprojects in their courses. The practical outcomes are project reports, articles and a thesis (in both bachelor and master level) as part of the projects. The previous projects, such as RIESCA (Pirinen et. el. 2010), SATERISK (Rajamäki et. al. 2012), and MOBI (Tikanmäki et. el.), have been excellent learning environments for students, teachers, researchers, and industrial partners. The MACICO project proceeded successfully with the same pedagogical approach. The study of Rajamäki (2014) gives a more detailed description how LbD-pedagogy was executed in practice.

Rajamäki, J. (2014). Externally Funded Research, Development and Innovation Projects as Learning Environments. Case: The MOBI project. 17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.

Abstract— Research, Development and Innovation (RD&I) projects are learning environments creating new skills and competencies for students, teachers, researchers, companies and public organizations. Our RD&I project model builds academic insights and competences by solving real problems for real people. This case-study describes the model through the MOBI project, whose project idea was developed in dialogue with lecturers and students; later on the dialogue was expanded to include a more extensive network with other students, teachers, researchers, companies (both device and service developers and end-users), public end-users and publicly-funded expert organizations for financing RD&I. MOBI has expanded not only to an academic multi-disciplinary collaboration but also collaboration with four companies and government officials as police and emergency departments. Our paper describes how the project was integrated into the study units and studies in general, as well as providing a description of the roles of different stakeholders when creating a learning environment. We will reclaim these lessons learned within our following RD&I projects, such as MACICO.

The students were involved with the MACICO project in several ways, depending on research approach. The Study units Development project (1st year Security management bachelor students) and Creating Innovations through Service Design can be mentioned as good practical examples. Especially Creating Innovations through Service Design, as a multi-disciplinary course, was suitable for the MACICO project. The course connects 3rd-year students from security management, business management, hospitality management, IT, etc. as a project groups with mixed skills. The groups work together to develop new, innovative service concepts by using Service Design model and methods (Moritz, 2005). MACICO acted as a real working environment to several interns and other students and offered interesting subjects of thesis to bachelor and master students. Several groups of master students also wrote scientific articles from the area of MACICO. Jokinen et al. (2014) briefly describe, in their article, how integration of the learning process and project work was done in MACICO.

Jokinen, E., Rajamäki, J., Karppinen, K., Tarkkanen, L. & Tiainen, S. (2014). Learning within research, development and innovation projects. Case: MACICO project. 17th In-ternational Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.

Abstract— Externally funded research, development and innovation (RDI) projects can be seen as a learning environment creating new skills and competencies for students, teachers, researchers, companies and public organizations. Laurea University of Applied Sciences' RDI project model develops academic knowledge and competencies by solving real problems in real-life situations. This paper describes the model through the MACICO project. This paper describes how the MACICO project and its demonstrations are integrated into the study units and studies in general, as well as providing a description of the roles and benefits of different stakeholders when creating a learning environment. Conclusions also reflect what needs to be taken into account when creating research demonstrations as student works.

Rajamäki, J., Daifi, M., Töyrylä, T., Alanko, M., Kiiski, P., Isohanhi, J., Kivelä, M., Viuhko, M., Nevalainen, J., Kuikka, H., & Tarkka, J. (2014). A Multinational Research Project as a Platform for Multi-Discipline Learning Environment. Three cases as a part of the MACICO project. 17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engi-neering Pedagogy.

Abstract— This paper presents how a multinational research project can act as a platform for multi-discipline learning environment and how a research project and student works can benefit from each other. The paper shows how three student works

are integrated in the Multi-Agency Co-operation In Cross-border Operations (MACICO) project. The students are creating scenario exercises that will be held for demonstrating the MACICO projects outcomes. The scenarios include a public safety communications network in extreme conditions, solutions in crowd management and real-time event coordination, and a use of social media in crisis communication.

By the end of the MACICO project, more than 130 students have been a part of it, earning more than 1100 ECTs. Seventeen students have done their thesis works and more theses are still in the process. Five Master's theses at Laurea have been completed. The results were presented at international journals, conferences, seminars and workshops; there were ten journal articles, 19 published peer-reviewed conference papers and three conference papers are under the review process. In addition to these, one doctoral thesis has been published by Dr. Rajamäki (2014) on the topic of the MACICO project.

References

Celtic Project Description: MACICO - Multi-agency cooperation in cross-border operations. (2011). *Unpublished.*

Drouglazet, L., Rajamäki, J., Tyni, J., & Aro, M. (2014). Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. *Proceedings of the 8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14).*

Jokinen, E., Rajamäki, J., Karppinen, K., Tarkkanen, L. & Tiainen, S. (2014). Learning within Research, De-velopment and Innovation Projects. Case: MACICO project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.*

Moritz, S. (2005). *Service Design. A practical access to an evolving field.* Köln: International School of Design.

Pirinen, R., & Rajamäki, J. (Eds.). (2010). *Rescuing of Intelligence and Electronic Security Core Applications, (RIESCA).* Vantaa: Laurea.

Rajamäki, J., & Aro, M. (2014). Multi-Agency Cooperation in Cross-Border Operations in the Field of Public Protection and Disaster Relief. *International Journal of Education and Information Technologies*, Volume 8.

Rajamäki, J., Daifi, M., Töyrylä, T., Alanko, M., Kiiski, P., Isohanhi, J., Kivelä, M., Viuhko, M., Nevalainen, J., Kuikka, H., & Tarkka, J. (2014). A Multinational Research Project as a Platform for Multi-Discipline Learning Environment. Three cases as a part of the MACICO project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.*

Rajamäki, J. (2014). Externally Funded Research, Development and Innovation Projects as Learning Environments. Case: The MOBI project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.*

Rajamäki, J. (2014). *Studies of Satellite-Based Tracking Systems for Improving Law Enforce-ment. Comprising Investigation Data, Digital Evidence and Monitoring of Legality.* Doctoral Thesis. Jyväskylä: University of Jyväskylä.

Rajamäki, J., Pirinen, R., & Knuuttila, J. (Eds.). (2012). *SATERISK – Risks of Satellite Based Tracking.* Vantaa: Laurea.

Tikanmäki, I., Rajamäki, J., & Pirinen, R. (Eds.). (2014). *Mobile object bus interaction - designing future emergency vehicles.* Vantaa: Laurea.

Pasi Kämppi

4. STAKEHOLDER ANALYSIS

Very often IT-projects are very technologically oriented, and they lack discussion with real end users and organizations. The equipment manufacturers and service providers are willing to maximize their profits, where attractive business cases emerge. Real user needs, not fitting to industry business models and being too marginal, fall out. When it comes to mission-critical communications in cross-border operations, the scenario is very complicated and bears the above-mentioned challenge. The services are funded by public financing, operating procedures differ between nationalities, people are facing language barriers, legislative regulation is very strong, and on the top of all this, organizations do not trust each other. The lack of trust, and also authorization, seems to be the biggest barrier for the implementation of the technological solutions, even if they are field proven and standardized.

To build more trust among stakeholders around mission-critical communications systems, the stakeholders must get familiar with each other and become aware of the problems on the research topic. An international research project like MACICO takes place in that phase. The research project demands that citizens, PPDR actors, industry, policy makers, and funding agencies work towards a common target: secure and reliable communication services for cross-border operations.

Chapter 4.1 gives a brief description of the stakeholders around mission-critical communications and research projects. Chapter 4.2 describes the end-user requirement analysis process in the MACICO project, and chapter 4.3 summarizes actual end-user requirements.

4.1 Recognizing Stakeholders

Dr. Jyri Rajamäki recognized, in his dissertation (Rajamäki, 2014), five different stakeholder groups. Dr. Rajamäki states that it is important to recognize all stakeholders and to understand their needs, expectations, goals, or objectives for a desired solution to a problem or an opportunity. He recognized citizens, targets, law PPDR actors, manufacturers and service providers, and policy makers, legislators, and funding agencies as separate groups. This section adds academies and research institutes as a group of its own.

Citizens

Citizens have an important role among stakeholders; they are funding the services for law-enforcement authorities as taxes. They need proper service in case of incident. However, the situation is quite diverse in practice. Most European countries are facing increasing health service costs and productivity growth in the public sector, which has been much slower than in the private sector. In practice, this means that the decreasing amount of public money is leading to a deteriorating situation for public services, including communication services for law-enforcement authorities. In the worst case, citizens will lose their trust in public safety and security services, which is detrimental for maintaining democratic order in civilized countries, and which ends up as a vastly bigger investment in safety by private companies and citizens.

PPDR actors

The term 'Public Protection and Disaster Relief' (PPDR) is used to describe critical public services that have been created to provide primary law enforcement, firefighting, emergency medical services, and disaster recovery services for the citizens of the political sub-division of each country. These individuals help to ensure the protection and preservation of life and property[1]. Public safety organizations are responsible for the prevention of and protection from events that could endanger the safety of the general public (Baldini 2010). Such events could be natural or man-made. According to Baldini (2010), the main public safety functions include law enforcement, emergency medical services, border security, protection of the environment, fire-fighting, search and rescue, and crisis management. Table 4-1 provides an overview of the various public safety organizations, their descriptions, and the functions they usually perform. One major challenge in defining a classification of public safety organizations at the European level is that, due to the non-homogenous historical development of public safety, similar organizations have different roles in different countries (Baldini 2010). A certified first responder is a person who has completed a first-aid course and received certification in providing pre-hospital care for medical emergencies. The majority of public safety organizations' personnel in the field are also certified first responders.

Table 4-1: Public safety organizations and functions (Source: Baldini (2010))

Public Safety Organization	Description	Functions
Police	The main objective of the police is law enforcement creating a safer environment for its citizen.	Law enforcement
Fire Services	With variations from region to region and country to country, the primary areas of responsibility of the fire services include: • structure fire-fighting and fire safety; • wild land firefighting; • lifesaving through search and rescue; • rendering humanitarian services; • management of hazardous materials and protecting the environment; • salvage and damage control; • safety management within an inner cordon; • mass decontamination.	Law enforcement, protection of the environment, search & rescue
Border Guard (Land)	Border Guard organizations are national security agencies which performs border control at national or regional borders. Their duties are usually criminal interdiction, control of illegal immigration and illegal trafficking.	Border Security
Coastal Guard	Coast Guard Services may include, but not be limited to, search and rescue (at sea and other waterways), protection of coastal waters, criminal interdiction, illegal immigration, disaster and humanitarian assistance in areas of operation. Coast Guard functions may vary with Administrations, but core functions and requirements are generally common globally.	Law enforcement, protection of the environment, search & rescue. Border Security
Forest Guards	Type of police specialized in the protection of the forest environment. It supports other agencies in fire-fighting, law enforcement in rural and mountain environment.	Law enforcement, protection of the environment, search & rescue

[1] *Note: the term Public Safety and Disaster Response, within certain regions, can also be construed as PPDR (from Project MESA TR 170 002 V3.1.1).*

Hospitals, field medical responders	The mission of the Emergency Medical Services (EMS) is to provide critical invasive and supportive care of sick and injured citizens and the ability to transfer the people in a safe and controlled environment. Doctors, Paramedics, Medical Technicians, Nurses or Volunteers can supply these services. They usually will also provide mobile units such as Ambulances and other motorized vehicles such as aircraft helicopters and other vehicles. The need for communications services for EMS providers inside and outside of the vehicles is vital in their work due to the fact they are nearly always in mobile resources that work in a wide variety of rural and metropolitan areas.	Search & rescue. Emergency Medical Services
Military	Military is the organization responsible for the national defense policy. Because military is responsible for the nation protection and security, it may also supports public safety organizations in case of a large national disaster. Military organizations are very well equipped with many different wireless communication systems with high degree of security and reliability.	Search & rescue. Emergency Medical Services
Road Transport Police Railway Transport Police	Transport police is a specialized police agency responsible for the law enforcement and protection of transportation ways like railroad, highways and others. Railway Transport police is a specialized police agency responsible for the law enforcement and protection of railways. In some cases, it is a private organization dependent on the railway service provider.	Law enforcement Law enforcement
Custom Guard	An arm of a State's law enforcement body, responsible for monitoring people and goods entering a country. Given the removal of internal borders in the EU, customs authorities are particularly focused on crime prevention.	Law enforcement
Airport Security Port Security	Airport enforcement authority is responsible for protecting airports, passengers and aircrafts from crime. Port enforcement authority is responsible for protecting port and maritime harbor facilities.	Law enforcement Law enforcement
Volunteers Organizations or Civil Protection	Volunteer organizations are civilian with training on a number of areas related to Public Safety and environment protection. They voluntarily enter into an agreement to protect environment and citizens without a commercial or monetary profit.	Protection of the environment, search & rescue.

Manufactures and operators

Doing business from the view of interoperability is extremely hard for both equipment manufacturers and operators. Equipment manufacturers have to invest in research and development to make interoperability technically possible, but operators are not willing to implement interoperability in their infrastructure without a clear revenue-generation model. Nobody knows the number of needed interoperable subscribers, and operators don´t know how to charge for the additional interoperability service. Additionally, the lack of trust and confidence is existent among operators. It seems that they are more focused on the side effects that interoperability will cause for their network infrastructure, rather than how to solve the interoperability challenge with the proper tools.

Policy makers, legislators, associations, and funding agencies

The Schengen Agreement launched the abolition of the border checks among the Schengen Countries in 1995. As the

target was to enable more fluent traveling between Schengen Countries, the Schengen Agreement states that Schengen Countries should prepare their law enforcement authorities for cross-border operations, including communication solutions. There is also a mutual agreement of first responder cross-border operations within the Nordic countries. After a few cross-border communication pilots with TETRA, and 20 years later, there is no single operative cross-border communication solution between any European countries. The availability of the commercial wireless broadband services has enabled the development of mission-critical communications again. The policy makers, legislators, associations, and funding agencies have started to discuss how to deploy wireless broadband services for law enforcement authorities. The policy makers and legislators are evaluating if it is possible to allocate dedicated frequency blocks for mission-critical communications; associations like TCCA and 3GPP have started to cooperate, and the EU Framework Programme for Research and Innovation has recognized the need of interoperability in their latest Horizon 2020 call.

Academies and research institutes

Academies and research institutes have a multifunctional role among stakeholders. Their task is to promote national and international research & development work, integrate students with research projects and industry, and create a neutral platform for discussion and innovation, where all participants are allowed to indicate the opinions of their own. The neutral platform for discussion and innovation is very important in research projects. The daily work of the law-enforcement professionals is highly restricted and regulated. As an example, the safety and security education program in Laurea can be seen as a platform that creates a neutral environment for learning and innovation.

4.2 End-user requirements' analysis process

Very often, engineers think that the technology itself solves a recognized problem. During the MACICO project, especially in the end-user requirements phase, it became quite clear that there is much more concerning end-user requirements than only technology. The researchers of the Laurea, Kämppi & al., decided to use triangulation to compose comprehensive end-user requirements. The researchers reviewed literature about previous projects, reviewed existing standards, and organized interviews with end users and experts. Additionally, they were able to create a five-layer model for recognizing all aspects of cross-border communications. (Kämppi, Tyni & Rajamäki, 2014).

Kämppi P., Tyni J., & Rajamäki J., (2014). Gathering End-user Requirements for the MACICO Public Safety Communications Project. International Journal of Communications, Vol 8, 21-28.

Abstract—The Multi-Agency Cooperation In Cross-border Operations (MACICO) project will develop 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. This paper comprises a useful reference on the standards and requirements identification related to interoperability of public safety communication systems, on the existing technological status and the immediate future activities.

The use cases have an important role for end-user requirement specifications: they give frames for the research process. The use cases for MACICO end-user requirements' analysis were derived from a real need but applied as fictional scenarios. The article by Mr. Kämppi & al. presents two fictional scenarios that were placed on the Finland-Sweden border area. The first scenario describes cross-border cooperation between Finnish and Swedish police when a heist takes place in Finland. As a communication point of view, the Finnish Police start the communication with the Swedish Police, when it is obvious that the criminals are going towards Sweden. The second scenario is based on emergency service cooperation on a border area. In this scenario, a Swedish citizen is injured in Sweden, but the first-aid unit resource is allocated from Finland. (Kämppi, Tyni & Rajamäki, 2014).

Kämppi, P., Tyni, J., & Rajamäki, J. (2014). Use Cases of the Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. 8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14), 209-212.

Abstract: - The Multi-Agency Cooperation In Cross-border Operations (MACICO) project develops a concept for interworking for security organisations in their daily activity. Considering both the end-users' requirements as derived from the compilation of surveys and the relevant bibliography, indicative use cases where MACICO could be applicable can be envisaged. In this study, a comprehensive analysis of different lower level deployment and testing stages and scenarios is included, while more complete use cases comprising complex multiple interactions among different elements of the MACICO ecosystem are presented in this study.

4.3 Specific end-user requirements

The MACICO-project end-user requirements' specification concentrates on technological requirements. The emphasis is on the professionals who are using mission critical communications services as a tool in their daily activities. The research reveals that a specific end-user requirement, e.g. group call or migration, creates requirements for the whole communication ecosystem. The researchers, P. Kämppi, J. Rajamäki and intern M. Aro, recognized four upper-level categories for specific requirements: external interface requirements, functional requirements for networks, functional requirements for terminals, and non-functional requirements. The most important requirements are the ability to migrate into foreign networks, group calls, features for secure communications, messaging services, emergency calls, and support for call queuing. The whole system, both the home and foreign networks, has to meet requirements for performance, reliability, availability, and security. (Kämppi, Aro & Rajamäki, 2014).

Kämppi, P., Aro, M., & Rajamäki, J. (2014). End-user Requirements for Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. 8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14), 183-190.

Abstract: - Public safety communications (PSC) comprise the determining factor of the effective intervention of the appropriate first responders (FR). The Multi-Agency Cooperation In Cross-border Operations (MACICO) project develops a concept for interworking for security organisations in their daily activity. Efficient PSC infrastructure and intelligent services over which emergency services sectors can be informed immediately as soon as an incident occurs and over which can be transmitted as much detailed information on the incident as possible, can render the FRs capable of handling effectively a great number of emergency situations. In this context, MACICO addresses interoperability issues not only on major crisis but also in day-to-day work which allows end users to be already familiar with the procedures with no specific training, and prepares a smooth migration to the future broad band networks. The study of the current worldwide situation regarding emergency services, the acquisition of an accurate vision of the needs of the potential end users of the MACICO platform comprise the initial steps towards the design and specification of the MACICO system. This paper comprises a useful reference on the requirements related to interoperability of PSC systems, on the existing technological status and the immediate future activities.

The MACICO project deliverable, D2.1 End-users Requirements Specification, summarizes all the research work regarding end-user requirements in the MACICO project. This outcome is a good example of how Laurea´s Learning by Development pedagogy is implemented into practice. Researcher P. Kämppi, Project Manager J. Tyni, intern M. Aro, and intern R. Leppänen put together the most relevant information for the mission-critical communication end-user requirements. The document covers previous projects, standardization, use cases, user interviews, and specific technological requirements. (Kämppi, Aro, Tyni & Leppänen, 2014).

Kämppi P., Aro M., Tyni J., & Leppänen R. (2014). MACICO D2.1 End-users Requirements Specification.

This document provides User Requirements Specification (URS) for TETRA and TETRAPOL communication systems in cross-border operations. The document describes functional and non-functional requirements.

TETRA is an open standard that is developed by European Telecommunications Standards Institute (ETSI). The target of standardization work was to define open interfaces to enable seamless interoperability between different network and equipment manufactures. TETRA standard contains features to allow interoperability between deployed national networks, but TETRA has been used in cross border operations only in pilots.

The first remarkable pilot was deployed in 2003. The Three Country Pilot was a project among The Netherlands, Belgium and Germany. The target was to connect the TETRA networks of all three countries using an Inter-System Interface (ISI phase 0). In simulated crisis, a specified group of civil protection authorities were able to communicate to each other on the Aachen – Limburg – Liège border area. The pilot was a success and many great lessons were learnt.

The second pilot was organized in 2010. Cassidian deployed another pilot project with ISI phase 1 where Swedish and German TETRA networks were connected to each other. This time the pilot was organized on a maritime area. Again, the pilot was successful and many new things were found.

The MACICO project implements the latest version of ISI interface (ISI phase 2) on top of TETRA architecture. MACICO also creates scenarios and user requirements for implementation and demonstrations. User requirements are based on results of previous projects, end users interviews and discussions with technical experts.

References

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

Kämppi P., Aro M., Tyni J., & Leppänen R. (2014). MACICO D2.1 End-users Requirements Specification. Available: http://macico.com/wp-content/uploads/2014/04/macico_d2_1_final_version-3.pdf

Kämppi P., Tyni J., & Rajamäki J., (2014). Gathering End-user Requirements for the MACICO Public Safety Communications Project. *International Journal of Communications*, Vol 8, 21-28.

Kämppi, P., Tyni, J., & Rajamäki, J. (2014). Use Cases of the Multi-Agency Cooperation in Cross-border Operations (MACICO) Project. *8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14)*, 209-212.

Rajamäki, J. (2014). *Studies of satelite-based tracking systems for improving law enforcement*. Jyväskylä Studies in Computing, Dissertation, (No 192).

Pasi Kämppi & John Holmström

5. TECHNOLOGICAL SOLUTIONS

Specifications are essential for deploying interoperability between telecommunications systems on a global scale. For TETRA, interoperability specifications have been available since the year 2000. For TETRAPOL, the situation is completely different, and there are no specifications for interoperability. For wireless broadband data services, the situation is even more challenging; TETRA is currently able to offer only a wireless narrowband data bearer and the end users are demanding reliable broadband services.

Standardization processes are typically long, and they are able to offer commercial solutions in the long run. Research projects, like MACICO, offer a possibility to improve current standards and the possibility for innovations in a more flexible way. A research project can develop solutions and propose them for the standardization workgroups. A research project can combine the best parts of all partners, academic thinking, and industry know-how.

Chapter 5.1 presents two traditional architectures and two new applications that are based on standardized TETRA ISI-interface. Chapter 5.2 concentrates on the TETRA-TETRAPOL interoperability solution, and chapter 5.3 proposes flexible user interface for TETRA communications in vehicular environment . Chapter 5.4 describes a robust wireless broadband data solution that is based on commercial data bearers.

5.1 TETRA-TETRA interoperability

The research paper concerning TETRA-TETRA interoperability is a good example of how academic research and industry know-how are effectively combined. In this research, researchers from Laurea UAS and experts from Cassidian combined their skills and experience to present four technical solutions for TETRA-TETRA interoperability. The first solution is called “peer-to-peer”, which is suitable for TETRA-interoperability proof of concepts or pilots. This solution is simple and cost effective. The second proposal presents a “mesh network” model that is suitable for medium-sized TETRA-interoperability configurations. The third architecture, “multinational network model”, describes a solution that offers TETRA-interoperability as a centralized service. The last solution combines satellite-based data with the “mesh network” model, and it is suitable for deploying TETRA ISI-interface with mobile platforms. (Kämppi, Rajamäki, Kervinen & Saijonmaa, 2014). Figure 5-1 presents a proposal for centralized TETRA interoperability service and figure 5-2 describes a proposal for TETRA interoperability service with mesh network and optional satellite base data connection.

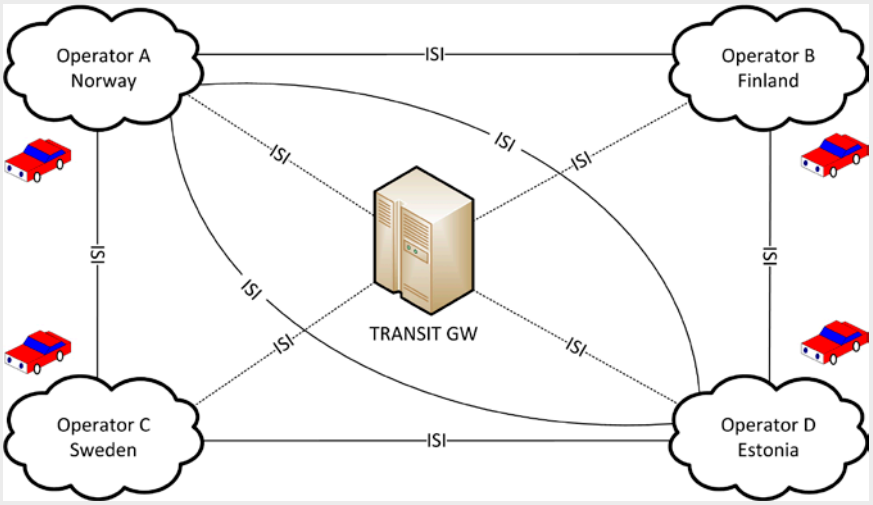


Figure 5-1 Proposal for centralized TETRA interoperability service

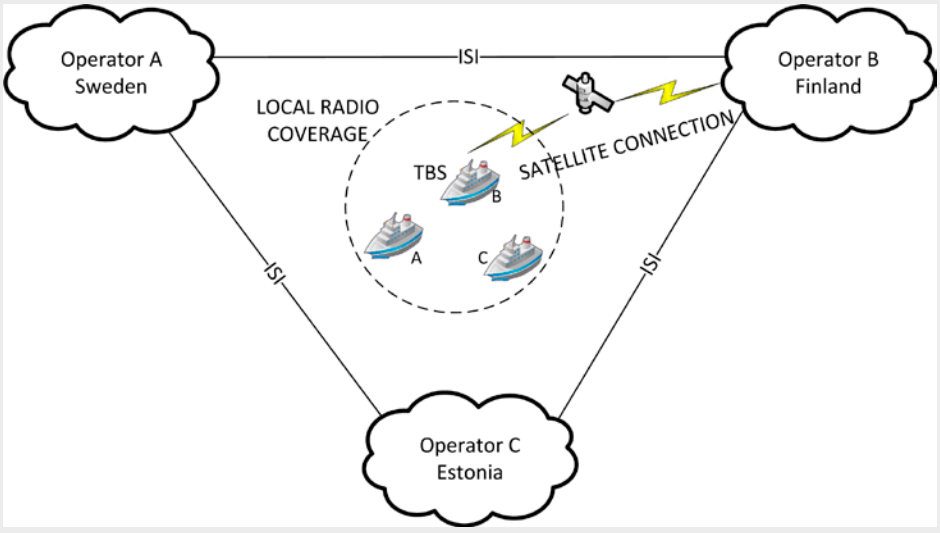


Figure 5-2 Proposal for TETRA interoperability service with mesh network and optional satellite-based data connection

Kämppi, P., Rajamäki, J., Kervinen, I., & Saijonmaa, J. (2014). Use Cases and Technical Solutions for Cross Border Operation Pilot. 8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14), 37-42.

Abstract—Interoperability has been available for TETRAtechnology since year 2000 but after a decade, there is no single operational interoperability implementation, used by end-user organizations, between operational TETRA networks. The Multi-Agency Cooperation In Cross-border Operations (MACICO) project paves way for an operational pilot in Finland cross border areas by bringing together end users, technology providers and researches already in the planning phase of a pilot. This study presents four use cases for the operational interoperability pilot with technical implementation models that are derived from the use cases.

5.2 TETRA-TETRAPOL interoperability

Mr. Kämppi presented a solution for TETRA-TETRAPOL interoperability at the PSCE conference in 2014. The solution uses Control Center Interfaces and an additional gateway between network exchanges for network interoperability. The gateway supports group calls, private calls, emergency private calls, emergency group calls, status messages, and SDS features. This solution can be deployed for remote sites or co-siting configurations. Figure 5-3 presents system architecture for TETRA-TETRAPOL solution.

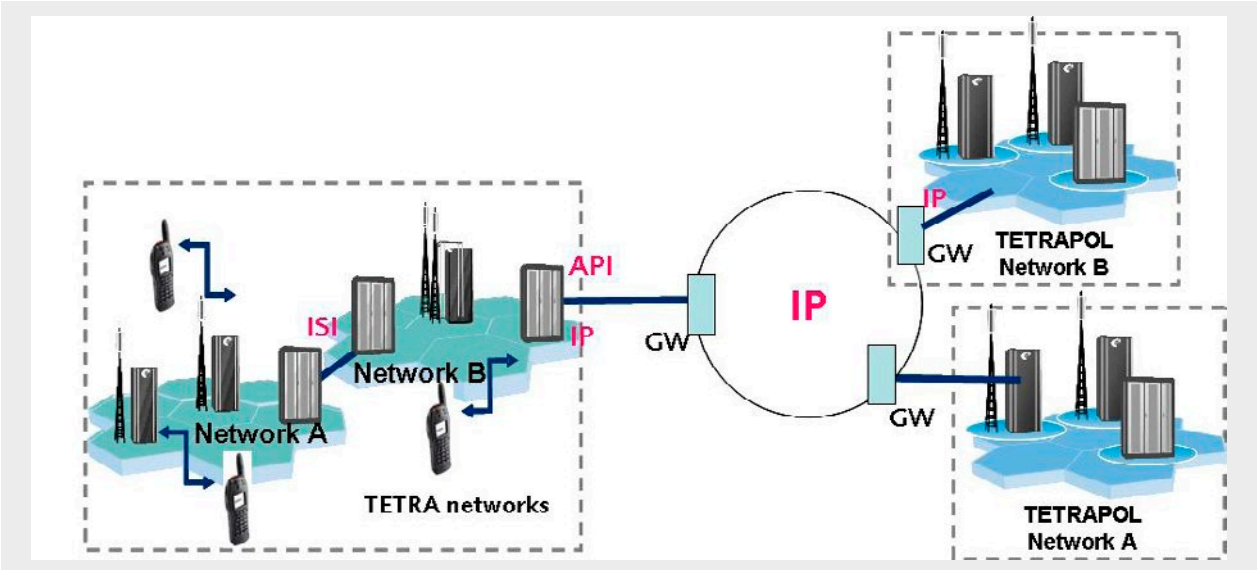


Figure 5-3 Architecture for TETRA-TETRAPOL solution.

Kämppi, P. (2014). MACICO project: Proposal for TETRA-TETRAPOL interoperability solution. Public Safety Communications Europe Conference. Gothenburg.

Abstract— Public safety communications (PSC) comprises the primary condition and requirement for the effective intervention of the public protection and disaster relief (PPDR) sectors. The Multi-Agency Cooperation In Cross-border Operations (MACICO) project develops a concept for interworking for PPDR organizations in their daily activity and paves way for interoperability between different wireless communication technologies. The MACICO project also brings together end users, technology providers and researchers to find out the best possible solutions for the cross border operations. Interoperability has been available for TETRA since year 2000 but there is no available standardized interface for TETRA-TETRAPOL interoperability. The MACICO project proposes a gateway based solution that makes possible to enable communication between TETRA and TETRAPOL networks. This study presents the principle of the proposed prototype and implementation models for service launching.

5.3 Next Generation Vehicle Voice Communication Solution

The TETRA radio terminal is an important part of daily operational procedures. The radio terminal has to be easy to use, and it has to be reliable in guaranteeing voice communication security, integrity, and availability. Laurea and Airbus Defense and Space launched a cooperation project to evaluate how the RCS9500-based TETRA voice communication solution could improve the workflow of a Finnish police field commander in a vehicular environment. Airbus Defense and Space provided the RCS9500 application that was integrated with hardware platform in Laurea's laboratory. The user-centric evaluation revealed that the end users were interested in new technological approaches, and the solution was seen as a step towards something new in the PPDR domain. The modular approach of RCS9500 made it possible to compose separate user interfaces for different user roles depending on operational situation, and it enables personal interoperability between different work roles in the command chain. The proposed solution is more complex compared to the current TETRA vehicle terminal, and it is important that all system components, including onboard computer, operating system, touch-screen display, multi-channel router, and the RCS9500 application, are robust and reliable. Figure 5-4 presents laboratory setup for RCS9500.

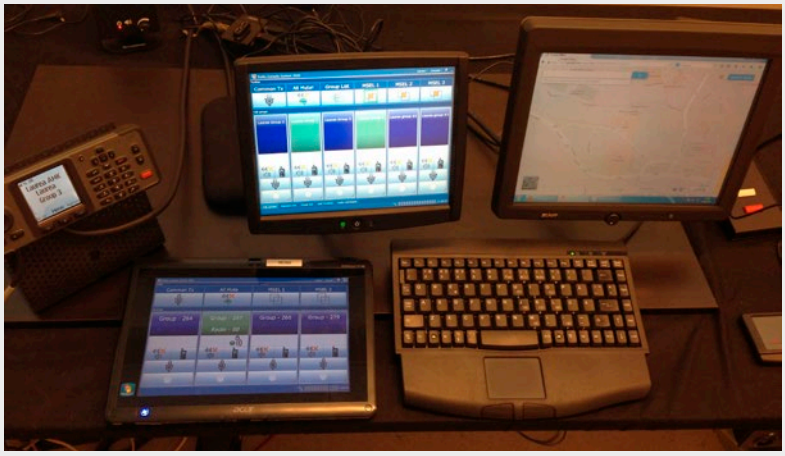


Figure 5-4 Laboratory setup for RCS9500

Roisko, V., & Kämppi, P. (2014). Feasibility study for adapting RCS 9500 into the vehicle environment: Case police field commander – Executive Summary. Unpublished manuscript.

The main idea of this research was to find out how real end users feel about adapting graphical TETRA UI into a vehicle, how the graphical UI of the RCS9500 could be configured according the needs of Finnish police officers, and what benefits the new system could enable in the vehicle as a working environment. The research process was divided into six parts: literature review, user interviews, designing preliminary layouts for RCS 9500 dispatcher, layout validation, designing the final layouts for RCS9500, and reporting.

The most important input concerning the layout design was the result of the interviews. They helped to understand the work of the police field commander, the operational activity of the police altogether, and the most important functions of the TETRA radio concerning the work of the police. The job of a field commander can roughly be divided in two roles: shift supervisor and scene commander. As a shift supervisor, he is responsible for managing daily routines, but in special situations his role is changed to a scene commander. Both roles have specific requirements for the communication equipment; the work is usually being done inside but sometimes also outside the vehicle. These two different roles of police field commander can be seen as potential use cases for RCS9500.

Three different UI layouts were created and validated with four users. The layouts presented different options for the same sort of usage. The number of talk groups and other features varied between the layouts. The setup included two Sunit touch screens, sizes 12" and 10". Currently, the 12" screen is reserved for the police field commanding system POKE. Therefore, it was decided that in this research, RCS9500 would be fitted to the additional 10" screen. After the validations, it was decided to create one improved layout that would combine the best elements from the three others used in the validation phase.

During the validation sessions, users made some suggestions to improve the presented layouts. Because RCS 9500 did not include all the proposed changes, it was decided to create an UI mock-up. The mock-up was created by modifying the screen shots taken from RCS9500. The purpose of the mock-up is to visualize the ideas concerning the TETRA radio UI designed to be used on the onboard computer of the police vehicle. The main features of the UI mock-up were user account, two tabs for talk groups with a maximum of six groups per tab, a group list tab for selecting the groups on the screen, and a status update tab. Every talk group element includes mute and pre-emptive TETRA call buttons. In addition, a five button toolbar including PTT, all mute, MSEL and volume control buttons is included.

Major benefits of the RCS9500, compared to the current radio device, are that selection of the talk group and identifying the person currently talking is easier because of the larger screen. The benefits of visualization of the talk groups are indisputable. When the user can select talk groups from one to five simultaneously on the screen, the information concerning the talk groups is significantly greater than with the current set-up. Switching between groups is fast if it happens between the groups presented on the screen simultaneously. It was also indicated that multi-selection of talk groups can be beneficial, especially for the field commander. An application like RCS9500 would also enable personal settings for the radio. Currently, the radio has one set of settings and different users are using it. If the application would include a user account, and every user would have personal settings, one could customize the UI in accordance with ones needs. This could increase the work efficiency of the police.

The introduction of the RCS 9500 to the police vehicle will still have certain challenges. Integration with other systems, especially

with the field commanding system, is an open question, which needs to be considered. Currently the status updates are sent via POKE. It is crucial to consider whether there will be more integration in the future with KEJO. Another question is the secondary display needed for the RCS9500. Audio management is also a critical issue. If there are multiple talk groups on the screen, and there is audio coming from multiple groups simultaneously, how will the audio be managed? One solution is to distribute it so that different talk groups are divided between different handheld radios and the speakers of the vehicle.

In addition to the issues already stated, one crucial issue to consider is theTETRA voice communication solution stability and reliability. In order for it to be possible to replace the current TETRA vehicle radio with another TETRA voice communication solution, the solution should be so stable that no backup system is needed. The proposed TETRA voice communication solution is considerably more complex compared to current TETRA vehicle radio. It consists of the RCS9500 application, the operating system of the onboard computer, the touch screen, the multi-channel router, and the onboard computer. All components have to be robust to guarantee voice communication security, integrity, and availability.

The end-user reception concerning the RCS9500 application was overall positive. Therefore, it might be that the RCS 9500 would have its place in the vehicle environment. Currently, the situation is the following though: there is only one touch screen on the dashboard of the police vehicle. Therefore, it can be said that the RCS9500 does not fit the vehicle in the current set-up of Finnish police vehicles. Another touch screen would have to be installed in order to use RCS9500 simultaneously with the field commanding system. In addition, it was discovered that certain functions of the RCS9500, including the group list feature, did not present the most optimal solutions for the vehicle environment. In the future, another touch screen can be motivated by new data applications. In any case, the ergonomical arrangements in police vehicles need to be revised due to the increasing usage of applications.

The most important topic in the future would be to arrange full-scale usability tests in an authentic-use environment. Some encouraging results concerning the RCS9500 usage in a vehicle environment were gained during this research, but the situation is always different in laboratory conditions than on the field. In addition it would be important to do more extensive user studies, including all of Finland. If the application is intended to be used nationwide, it is important to include the whole country in the user studies. It would also be beneficial to be involved with the development of KEJO. It would be sensible to investigate the possibilities for TETRA and KEJO integration. There is already some integration between POKE and TETRA, and if increased integration would help the police officers to work more efficiently on the field, it would be worth investigating.

Different options for the screens should be investigated. Also, different screen set-ups in the vehicle environment should be investigated. There are multiple possibilities with tablet computers and fixed touch screens; two fixed touch screens, one fixed touch screen and one tablet computer or two tablet computers for example. Introducing a tablet computer to the vehicle environment would, in principle, enable the mobility of applications if necessary. For example, the field commanding system could be used outside the vehicle in certain situations. The current touch screens are not always working in a required way. If more applications will be installed on the onboard computer, the touch-screen technology used in the vehicle has to meet the requirements of the use situation. Only then will it be reasonable to add more applications to the touch screen.

5.4 Towards Wireless Broadband Services for Critical Communications

The PPDR actors are demanding wireless broadband services for their daily activities, but the regulations and critical communications service providers are not able to meet the requirements. The regulators are struggling with frequency harmonization, and the service providers are lacking money for new investments. It is obvious that there is a market for the alternative wireless broadband solution instead of traditional dedicated network infrastructure deployments. This article, made as cooperation with academia and industry partners, proposes cost-effective solutions to adapt commercial data bearers for PPDR actors.

The basic idea is to combine separate commercial data bearers as a single transparent data path at the end-user point of view. Depending on end-user requirements or available commercial network infrastructure, the solution can be configured to simultaneously use different network technologies (TETRA, 2G, 3G, LTE) by commercial service providers. The heart of the proposed solution is a fully software-based DSIP protocol. The key features of the DSIP-protocol are the ability to hide existing commercial network infrastructure, fully automated data bearer control, in-built quality of service (QoS) support, and OSSTMM (Open Source Security Testing Methodology) audited network security. Figure 5-5 presents a proposal for DSIP-based wireless broadband solution for PPDR actors.

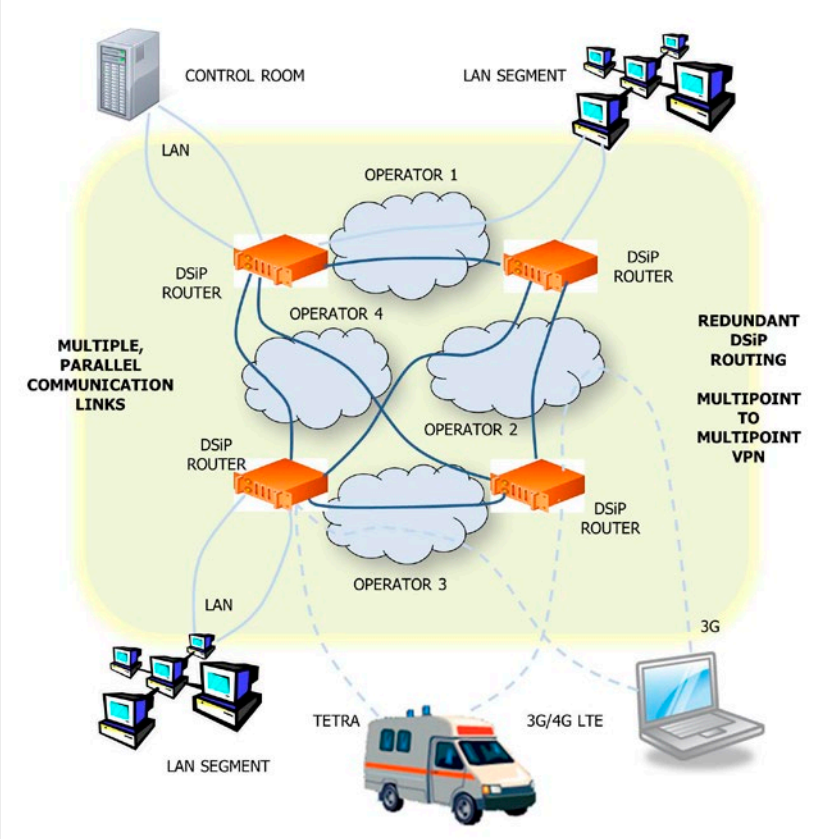


Figure 5-5 Proposal for DSIP-based wireless broadband solution for PPDR actors

Rajamäki J., Rathod P., & Holmström J. (2013). Decentralized Fully Redundant Cyber Secure Governmental Communications Concept. European Intelligence and Security Informatics Conference (EISIC), 176-181. doi:10.1109/EISIC.2013.39.

This paper focuses on future requirements of broadband data transmission of public protection and disaster relief, critical infrastructure protection and military, and presents the concept of redundant and secure data communication network system in the multi-organizational environment. We are proposing a fully decentralized architecture with optimized critical communication channels. Here, network actors and elements identify and authenticate by establishing physical connection. This concept also recommends, group level user-authorization mechanism for each participating organization. Their respective users of command and control centers are identified, authorized and authenticated to various data sources. The decentralized architecture concept is using the Distributed Systems intercommunication Protocol (DSiP). The concept is highly fault-tolerant in routine as well as crises operations. The software-based approach is independent of heterogeneous data communication technologies, IP networks and telecommunication operator services. The solution enables to build an effective and lasting cyber secure data network for multi organizational environment. Being a fully decentralized concept, networks of individual member organizations are virtually autonomous and hard to upset each other. That allows smooth message and information exchange to enable interoperability. ■

References

Kämppi, P., Rajamäki, J., Kervinen, I., & Saijonmaa, J. (2014). Use Cases and Technical Solutions for Cross Border Operation Pilot. *8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14)*, 37-42.

Kämppi, P. (2014). MACICO project: Proposal for TETRA-TETRAPOL interoperability solution. *Public Safety Communications Europe Conference*. Gothenburg.

Roisko, V., & Kämppi, P. (2014). Feasibility study for adapting RCS 9500 into the vehicle environment: Case police field commander – Executive Summary. Unpublished manuscript.

Rajamäki J., Rathod P., & Holmström J. (2013). Decentralized Fully Redundant Cyber Secure Governmental Communications Concept. *Intelligence and Security Informatics Conference (EISIC)*, 2012 European. 176-181. doi: 10.1109/EISIC.2013.39

Jyri Rajamäki

6. COMMON SERVICES AND OPERATIONAL PROCEDURES

This Chapter looks at common services and operational procedures in the field of public protection and disaster relief (PPDR) from an end-user point of view. By end-users, we mean individual first responders as well as PPDR agencies. This Chapter comprises five sections. The first section deals with mobile public safety voice and digital broadband services, their current state, and future operational needs. The second section studies co-operation between public safety authorities utilizing new technologies, such as unmanned aircraft systems (UASs). The third section focuses on border security, especially how to satisfy international information exchange needs. The fourth section examines law enforcement agencies' cross-border opera-tions and related information exchange needs. The last section concentrates on mul-ti-national tracking systems and services in the field of PPDR.

6.1 Mobile voice and broadband services

Wireless communications are critical to supporting the operational capabilities of PPDR organizations. The professional mobile radio (PMR) technologies currently used for PPDR communications offer a rich set of voice-centric services [e.g., push-to-talk (PTT) group calls] but have very limited data transmission capabilities and are unable to cope with increasing demands in the PPDR community for mobile data-centric applications. Introducing PPDR mobile broadband communications faces a number of technical and economic/business challenges (Ferrus, Pisz, Sallent, & Baldini, 2013). The current paradigm for PPDR communications provisioning based on dedicated technologies, dedicated networks, and dedicated spectrum no longer constitutes the main approach for introducing PPDR mobile broadband, and hence, new paradigms and innovative solutions are needed (Ferrus et al., 2013).

Finland is known globally for its high-tech information society. To meet the re-quirements of any society characterized as an information society, secure ICT sys-tems that fulfill the prerequisites of businesses, government and citizens are needed. An obvious scenario is to synchronize services with the available diverse network and information system services. That optimization is carried out for the objective in question, and the services must complement each other. The communication concept of the Finnish Government consists of many different networks, which can be roughly divided into four different levels of preparedness, as shown in Figure 1. First, the Defense Forces' strategic communications have the highest level of preparedness and also the largest budget (Benson, 2011). The second level is the secure data network for state officials, known as the TUVE network. It has about 30,000 users from the government ministries, defense forces, police, rescue units, and border guards. TUVE is a Finnish project aiming to implement a high level of preparedness by securing data communication services. The purpose is to elevate the level of protection and usability of data communications of security authorities and to remove the various dependencies of individual service providers. The key objectives are storing critical data in Finland and systematic monitoring and control of critical systems in Finland (Benson, 2011; Manni, 2011). However, a dedicated secure data network used by state officials cannot be ubiquitous and

suitable for all the needs that are vital to society. Therefore, the third level of the government's common secure communications requirements is mostly realized through public-private-partnership (PPP) together with the State IT Service Centre and commercial telecommunication operators. In the future, more extensive cooperation will be essential for the successful development of ICT services for Finland's security. The fourth level consists of commercial networks, and it has 60,000 governmental users (Lehti et al., 2009).

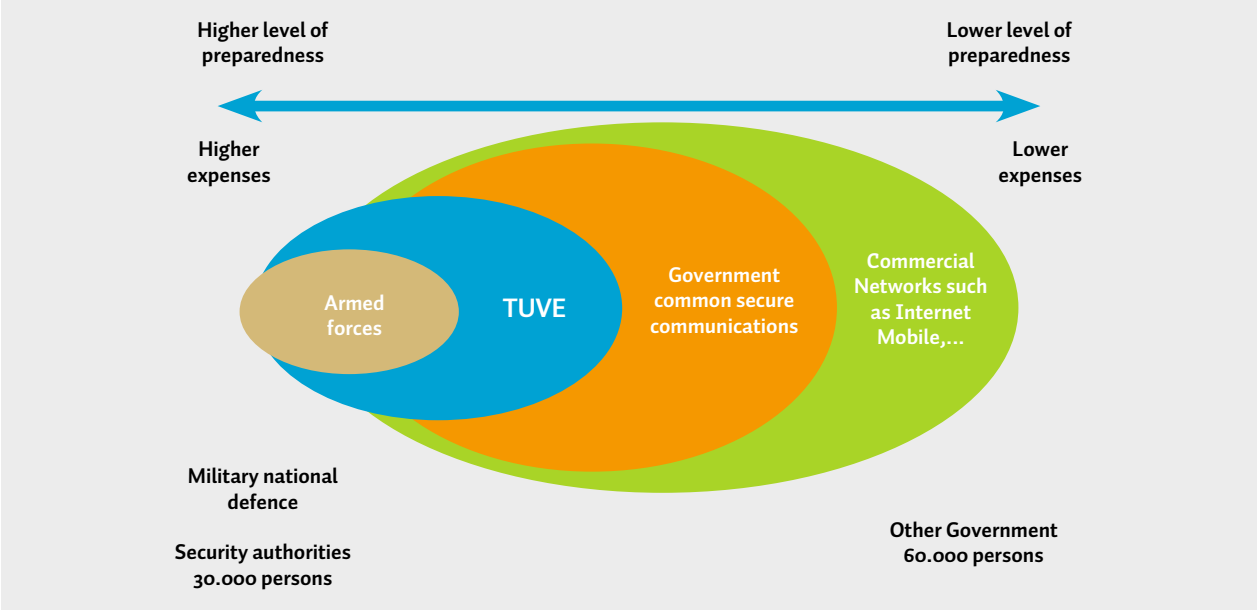


Figure 6-1. Communication concept of Finnish Government (Source: modified from Benson (2011))

The state-of-the-art commercial wireless technology evolution is long-term evolution (LTE) mobile broadband technology, which is currently positioned to be the dominant technology in future commercial mobile networks. LTE technology can provide a high bit rate and low latency IP connectivity service that can be used to deliver most of the PPDR data services currently in demand (Ferrus et al., 2013). In Finland, mobile communications of first responders 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 a 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.

The Finnish TETRA-based public safety network VIRVE has been fully opera-tive since 2002 with full domestic interoperability. It has 1,350 sites, all of which are electromagnetic pulse (EMP) protected with back-up power supplies. Statistics show the pool of users includes oversized consumers like rescue services (33%), police (21%), and military (15%) as well as social and health services (13%). There are also small consumers such as, the border guard, customs, air traffic-SAR (5.2%), and other authorities (1%). The rest is used by other individuals and organizations (Riippa, 2011). Every week, VIRVE transmits 800,000 group calls and 32 million short data service (SDS) messages (Riippa, 2011). The Finnish experience shows that GSM networks have been overloaded during emergency situations. That was witnessed in the high school massacres in 2007 and 2008 and during the summer storms of 2010. The VIRVE network, on the other hand, was operating normally.

Mobile data is essential in PPDR field operations. Data-intensive multimedia applications, e.g., real-time access to critical data, such as high-resolution maps or floor plans, on-field live video transmission from cameras on helmets to a central unit, and remote database inquiries, show great potential for improving the effectiveness and efficiency of PPDR operational procedures (Ferrus et al., 2013). More data will be transmitted as a result of increased cooperation between PPDR organizations. Currently, between 2013 and 2015, Finland is developing several new data systems for PPDR (Riippa, 2011). These systems will include (1) a joint command and control system, (2) a joint data system for investigating authorities, and (3) a joint field-command application. These systems will increase the transmission of situational pictures, which will result in data transfer demand. The master plan in Finland is to close permanently-fixed police stations and create a mobile office concept for police, which also means more data transmissions.

One of the main benefits that appeared within the TUVE project is that requirements for high security networks are specified at the ministry level. 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. 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, overly strict data security regulations may rule out the mobile utilizing of digital services in the field. However, most often, the biggest cyber threat is the so-called "insider threat", like the Snowden and Manning cases indicate.

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 mission-critical data and communication systems must be available and usable in all security conditions. This also concerns natural phenomena, outages, and cyber-attacks. Computational infrastructure must be scaled so that the relatively infrequent peak loads can be processed (Zaerens & Mannonen, 2012). Cloud computing and utility computing enables scaling (Rajamäki & Rathod, 2013).

Rajamäki, J., & Rathod, P. (2013). Leveraging benefits of standardized utility and cloud computing with service-oriented architecture in public protection and disaster relief. In S. Lopes (Ed.), Recent advances in computer engineering series, vol. 16 (pp. 74-80) WSEAS Press. Available: http://www.wseas.us/e-library/conferences/2013/Antalya/ITCN/ITCN-08.pdf

Abstract: The Public Protection and Disaster Relief (PPDR) organizations are using Information and Communication Technology (ICT) services in very heterogeneous and customized delivery methods. Majority organizations have tailored processes, contracts and technologies. In many cases, these are managed by internal and external suppliers. Currently, ICT field is going through many innovations as a process of evaluation in technologies. On the one hand, cloud computing, utility computing and service-oriented architecture (SOA) have shown promising potential. While on the other hand, these technologies are bringing various challenges. There is a gap in knowledge leveraging benefits of such technologies, especially in the fields of PPDR. This paper studies utility and cloud computing with service-oriented architecture in the context of ICT services. The study argues that all processes, technologies and contracts in utility computing should be standardized to leverage the full benefits of these innovative technologies in PPDR. Paper also discusses and describes the benefits of standardization as well as some potential issues due to lack of standardization.

6.2 Cooperation between authorities Case: Unmanned Aircraft System

The Finnish Government's Security and Defense Policy state that close cooperation between the authorities create cluster synergy effects by cutting overlapping functions and support functions, thus enabling an efficient use of resources (*Finnish security and defence policy 2009. government repor2009*). All public protection and dis-aster actors need accurate situational awareness and real-time pictures for sufficiently managing their missions. The SATERISK project research shows how satellite-based systems could be used for this purpose. However, we noticed that satellite-based systems are not enough, and local, more accurate services are needed. This is why we processed the MAYFLY project proposal, studying the novel usage of micro air vehicles for use in the security and public safety fields. Despite MAYFLY not being externally funded, its spin-offs, the AIRBEAM project and the CBPI project, were initiated in March 2011 and November 2012 respectively. Within the MACICO project, we have studied, for example, how the use of Unmanned Aircraft Systems (UASs) and Remote Piloted Aircrafts (RPAs) could improve the cooperation between authorities and how to develop new interoperable safety and security services (Tikanmäki & Tuohimaa, 2011).

Tikanmäki, I., & Tuohimaa, T. (2011). How real time picture and situational awareness can be improved by using unmanned aircraft systems (UAS)? Recent Researches in Communications, Electrical & Computer Engineering, WSEAS Press, 28-33. Available: http://www.wseas.us/e-library/conferences/2011/Meloneras/ACELAE/ACELAE-03.pdf

Abstract: This paper deals with the importance of expertise for improving situational awareness and real-time picture. As an example we use Unmanned Aircraft Systems (UAS). Our research process began by defining the topic and objectives as well as the theory of experience. Research material was collected through interviews and by analyzing scientific publications, newspaper articles and video clips. Most of the scientific publications from the subject concentrate only on the building, on the planning and on the technical properties of UAS. The unmanned model planes are used mainly for different military purposes at the moment. On the basis of this we ensured that we are studying this issue in question among the first ones in Finland. In this paper we use the method of case study research to improve the situational awareness and real-time picture by using UASs in organizations.

Prior studies reveal a need for networking between the authorities with regard to the cooperation of implementation of, for example, UASs (Taitto, 2007). Network-ing benefits of government activities are emphasized, because the authorities do not need a duplication of resources. None of the authorities are solely responsible for certain activities, because there is an exemplary cooperation between public authori-ties. The authority who is responsible for operation receives support from other au-thorities. The importance of cooperation in UAS usage is highlighted, because a number of different actors, such as police, rescue service, customs, and border con-trol authorities need the same kind of services. The service provider must be familiar with the various actors and must be able to meet the demand in the right way. Selecting a product for many different needs of operators must, therefore, give special attention. The importance of cooperation between authorities discovers an important subject to be developed (Tuohimaa & Tikanmäki, 2011).

Tuohimaa, T., & Tikanmäki, I. S. (2011). The strategic management chal-lenges of developing unmanned aerial vehicles in public safety organizations. Recent Researches in Communications, Electrical & Computer Engi-neering, WSEAS Press, 34-39. Available: http://www.wseas.us/e-library/conferences/2011/Meloneras/ACELAE/ACELAE-04.pdf

Abstract: This paper deals with the challenges of strategic management in public or-ganizations for improving situational awareness and real-time picture. A significant strategic management tool for operational activities is situational awareness including real-time picture creation. In this paper we use, unmanned aircraft systems (UAS) as an example for improving situational awareness and real-time picture creation. Persons acting on the ground, their leaders and other decision-makers should be able to exploit a real time picture of the situation when making decision. E.g. police, border control authorities, customs and fire departments need real-time picture of the situation. For decision-makers and their assistants, situational awareness means understanding about events, circumstances affecting these events, the objectives of various parties and possible options, which are needed to make decisions on a specific item or the whole thing. In society, the efficient use of resources is a sensible, economical and appropriate target. Strategy work requires a new perspective where actors must have the ability to see large complexes. Different entities interact with each other and strategic decisions require courage. Successful organizations create a successful strategy, implement it and are able to renew their strategies with the latest requirements.

Interagency cooperation is essential so that various actors have sufficient knowledge of others concepts, measures, resources and plans. Interagency coopera-tion aims at cost savings to increase efficiency. A good collaborative practice is a prerequisite for proper functioning (Taitto, 2007). Networking is a process where the corporate knowledge, values and skills combine the added value of productive activity, aiming at the promotion of competitiveness in the longer term (Toivola, 2006). Different levels of networking means that cooperation between organizations is needed; performing a similar task teams to cooperate, or individual experts formed a collaborative network. UAS-related cooperation with the authorities will act in all of the above mentioned areas (Tuohimaa, 2014).

Tuohimaa, T. (2014). Studies of unmanned aircraft systems from the perspective of operational use. Master's Thesis. Theseus, Laurea:Leppävaara. Available: http://urn.fi/URN:NBN:fi:amk-2014060912207

Abstract: This thesis consists of four international scientific publications. In my thesis I research the challenges of the unmanned aviation - political, economic, tactical and technical point of view. In addition, I bring forth those key "stakeholders", which each of those have their own efforts contributed to the unmanned aviation "as players" in the field: manufacturer, legislation, operator, customer, the end user, the business world, an object (human / infrastructure) and people, who are concerned about their privacy, as well as how 'Big Brother' is watching them.

Main goal of this thesis is to gain knowledge to understand who are the "players" of Unmanned Aircraft Systems (UASs) and what are the main challenges. I also try to find answers to next questions: Why networking is so important? Why people and public opinion are in so big role? I try to find possible solution to this theme by using framework, I have made. In this framework I use categories and dimensions, to increase general awareness of unmanned aviation.

I have developed this model on the basis of my earlier studies, to describe and facilitate the role of the different actors and their activities. This framework helps to perceive, how much the unmanned aviation has both "visible" and "invisible" actors, how much they relate to each other, and what is the interaction between their relationships. By this knowledge, I hope, it is much easier to understand the complex of the unmanned aviation.

There are surprisingly many matters affecting of the unmanned aviation, and most of those matters will not even been noticed at once. The unmanned aviation is much more than the acquisition of the system, and then starting the flight operations. One of the main objectives, of this thesis, was to get the reader to discover, how much there are different challenges of unmanned aviation.

I'm not trying to create a list of all themes affecting of unmanned aviation, and in this thesis, highlighted themes are definitely only a part of the total categories. One of my main goals in this thesis, is to get the reader to think about the unmanned aviation taken as a whole and take account of the challenges of the unmanned aviation.

Aviation Safety is one of the most important cornerstones of the unmanned aviation. This is going to be a particular challenge for many parties. I think that within a few years society will face completely new and different challenges, such as privacy. Different challenges do not only affect public organizations, but also in citizens' daily life. In the future unmanned aviation-related research and development will become even more prominent.

Large public events have temporary command centers for general and field management, where liaison officers from different actors allow coordination of ac-tions. Command centers usually have representatives from the police, the event organizer, rescue services, border guards, customs, and the military. Depending on the nature of the event design and operation, there may also be other public authorities (Taitto, 2007). Based on the above, for example, the police command centers' main tasks in Finland are to support police management functions, situational awareness, and real-time picture, maintaining the pre-trial measures, external and internal information, and support services. Tasks include also working in collaboration with emergency response centers and other authorities' command centers. Cooperating is challenging and leadership rises to the very important role when operating with different authorities' operations. The situation picture can be improved by developing and expanding operational cooperation and mutual interaction between the authorities. Extensive cooperation between the authorities allows the development of the real-time picture and situational awareness. The development of multi-government tactics and sharing of expertise in matters of safety and training increases the efficient use of joint resources. For complex tasks of planning, designing, and coordination, based on multi-government functions, a real-time picture is essential. Legislation must be in line both at the international and national levels. RPA systems will be the business of future, and it has been said that the RPA systems can be equated with the early days of aviation. Research and development is in a key position at the first step (Tikanmäki & Rajamäki, 2012).

Tikanmäki, I., & Rajamäki, J. (2012). Exploiting security, safety and situa-tional related services by using remotely piloted aircrafts. 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE'12), 50-55. Available: http://www.wseas.us/e-library/conferences/2012/Rovaniemi/INEE/INEE-08.pdf

Abstract: The purpose of this study is to find out what kind of services can be designed by utilizing Unmanned Aircraft Systems (UAS). This study provides an un-derstanding of the current obstacles for producing these services. The legal UAS issues in public and private organizations are examined. The biggest challenge in using Unmanned Aircraft Vehicles (UAVs) is that legislation does not recognise enough a UAV as an aircraft. Training and other requirements for the operator and the actual flyer are unspecified for UAS-operations. UAVs development is waiting for standardization. The aim of this research is to analyze and assemble summary about this issue by using data triangulation. From the research perspective there are needs for UAS and also social general ignorance how UAS can be exploit in civilian use. Challenge for cooperation in this particular case is to reconcile the needs of different actors - public and private - under common interests. The market has a huge economic promise for different UAS classes. By other means than utilizing UAS, the same benefits are diffi-cult to be achieved; therefore societal benefits are particularly high. UAS would significantly increase the number of the biggest priorities of safety, security and environmental issues.

With regard to the development of UAS services, networking is very important, especially for a small country with limited resources. One player is unable to cope on its own for systems implementation and use of it. That is why network creation is vitally important and obtains synergies from a wide-scale deployment of the UAS-based services (Tikanmäki, Tuohimaa, & Ruoslahti, 2012).

Tikanmäki, I., Tuohimaa, T., & Ruoslahti, H. (2012). Developing a service innovation utilizing remotely piloted aircraft system (RPAS). International Journal of Systems Applications, Engineering & Development, Vol. 6(4), 279-287. Available: http://naun.org/main/UPress/saed/16-293.pdf

Abstract: Co-operation between authorities is at the beginning of new challenges. When authorities co-operate successfully, this prevents duplication of efforts and increases efficiency. Many public authorities have at the moment and in the future same needs for equipment and systems. Operational and command centers of

authorities (for example, police and rescue service), have potential needs to improve continually their situational awareness and a real time picture.

Related research and development (R&D) in public and private sector has an important role already today. Research and development is in a key position at first step. The importance of safety is the key element when operating on the air. A well planned system takes notice of the end user and is made in co-operation with the equipment manufacturers and end-users. One of the main challenges is to accompany manufac-turers and end-users.

Public and private co-operation is needed and it must be increased. Legislation must be in line both with the international and national levels. Legislation does not sufficiently or even at all detect the UAS activity. Developing this kind of service innovation is in an important and challenging role for three reasons; 1) various actors need to be able to meet the demand of the right way, 2) it must give a special attention for many different needs, and 3) because of the inadequate aerial legislation as for unmanned aviation.

6.3 Border security

The main target of EU border security is to safeguard European values and in-terests, such as freedom of movement, fundamental rights and rule of law. Border control includes border checks, border surveillance, and risk analysis (Laitinen, 2011). According to Laitinen (2011), its main objectives are migration management, crime mitigation, and facilitation of cross-border traffic. In the near future, there will be many new ICT systems and digital services for border security. With regard to border control, there will be digital systems and services for border checks, border surveillance, and risk analysis.

In the EU, many new information exchange systems and networks are under preparation as "smart borders." The Commission has suggested the establishment of a registered traveler program (RTP) for frequent, pre-screened, and pre-vetted third-country travelers, and an entry/exit system (EES) allowing electronic recording of the time and place of entry and exit of third-country nationals. These programs require elementary development towards an automated border check (ABC) process. Frontex (the EU Border Agency) is facilitating the sharing of actionable information related to border control between EU Member States by the creation of EUROSUR, the future European integrated border surveillance system (Ameyugo, Art, Esteves, & Piskorski, 2012). A concept is being developed in EUROSUR that focuses on enhancing border surveillance in order to (1) reduce the number of illegal immigrants who enter the European Union undetected, (2) reduce the number of deaths of illegal immigrants by saving more lives at sea, and (3) increase the internal security of the EU as a whole by contributing to the prevention of cross-border crime. The first and the third concepts are mainly related to border management, as most illegal immigrants enter the EU through border checks in airports, harbors, and land borders; the second concept is exclusively related to border surveillance.

Figure 6-2. Four-tier access control model (Source: modified from Laitinen (2011))

Figure 6-2 presents the so-called "Four-tier access control model" applied in Europe. This model maintains that only a part of the border security activities are carried out at the border. All tiers require access to ICT systems of border security. For example, most in-land activities employ mobile digital services. Also, many seasonal border crossing points (BCPs) need mobile systems, because fixed systems are too expensive for all seasonal BCPs. All mobile systems require secure mobile communications and information exchange systems and procedures that are studied in the MACICO project.

Ruohomäki (2012) has studied a public key infrastructure operation model for the financial sector companies. He has also evaluated his model (Ruohomäki, 2012). The study of Rajamäki and Ruohomäki (2013) continues the subject and presents an information exchange procedure for border surveillance and other law enforcement activities (Rajamäki & Ruohomäki, 2013).

Ruohomaki, Petteri (2012) Public Key Infrastructure operations model. Theseus: Laurea (Master's thesis). Available: http://urn.fi/URN:NBN:fi:amk-2012053111005

Abstract: My thesis is divided in two parts. The first part deals with the Public Key In-frastructure operations model and the second offers an evaluation of that model. The thesis answers how to provide efficiency and consistent Public Key Infrastructure functionality to a company. The main question is how a company can identify the counter-party player securely. A company must be able to trust outputs and inputs.

The model is based on Information Security Forum best practices and it is built for the companies in the financial sector. Being one of the most regulated sectors, the requirements are set high. This is the reason why the model should have possibilities for easy implementation implement to other environments. Model built on multiple standards and best practices.

The evaluation phase is grounded on the financial sector Public Key Infrastructure project. This project is part of Single Euro Payments Area financial changes. The project length exceeds three years, and it uses all model phases. For this reason the company Public Key Infrastructure project is optimal for evaluating the Public Key Infrastructure operations model. Model evaluating should answer on whether the model is usable and it be implemented to other environments.

This thesis relies on the Design research method, the final product being the Public Key Infrastructure operations model. Design science contains two principle activities: build and evaluate. Building the artifact demonstrates how it works. In this study building means the process of constructing the actual artifact, the Public Key Infrastructure operations model. Evaluation, for its part, is the process of terming how well the artifact works. Specific criteria must be set up for successful evaluation. This mean that when to build artifact as Public Key Infrastructure operations model so functioning may not be well understood.

The thesis result is the artifact of Public Key Infrastructure operations model. This model offers the first steps on what must be done in the Public Key Infrastructure project. It provides a partial answer on how to develop faster, more efficient, and safer Public Key Infrastructure services. The thesis results are derived from a real Public Key Infrastructure project, but these kinds of projects are comparable with one another.

Rajamäki, J. & Ruohomäki, P. (2013). Multi-Agency Cooperation in Cross-border Operations: Information Exchange between Law Enforcement Authorities. Proceedings of the International Congress of Engineering and Informatics, pp. 271-279, Asia-Pacific Education & Research Association, Taipei, Taiwan.

Abstract: The nature of crime has internationalized. Therefore the transmitting of tracking and other status information between Law Enforcement Authorities should become an everyday business. The goal of this paper is to present a possible solution for international cooperation between authorities. The proposed solution is based on Public Key Infrastructure operation model built for the financial sector companies.

6.4 Cross-border law enforcement operations

International warehouses of crime involved in smuggling, drug and human trafficking, and terrorism are becoming a stronger threat to European security. This increases the need for European collaboration and information sharing related to investigation technologies; cross-border usability and interoperability of investigation tools have to be guaranteed. Rajamäki (2014) studies new cross-border processes and technical solutions that would facilitate their combat against international organized crime (Rajamäki, 2014).

Rajamäki, J. (2014). Software Intensive GNSS-based Tracking Systems for Improving Law Enforcement. WSEAS Transactions on System and Control, Vol. 9, 629-639. Available: http://wseas.org/wseas/cms.action?id=7651

Abstract: Law enforcement agencies (LEA) constantly seek new cross-border processes and technical solutions that would facilitate their combat against international organized crime. This paper studies how new types of satellite-based tracking sensors, mobile monitoring stations and their associated communication channels for LEA can be understood and designed taking into account the chain-of-custody and monitoring-of-legality requirements. The empirical data was collected within four research projects in 2007-2014. The theoretical framework is built on the design theory of software-intensive systems. For improving law enforcement processes, the three main functions (crime investigation, chain-of-custody and monitoring-of-legality) should be considered all at once. Comprising their separate information systems will avoid triplicate workload. It also will enable multiple other benefits, such as transparency of surveillance and giving a new tool for commonly agreeing of the balance between surveillance and privacy.

Joint cross-border investigations are challenging, as the LEA practices and technologies used in technical operations and legal procedures have big differences and incompatibilities. This leads, for example, to slow or hindered information exchange, endangering the success of entire investigations. Viitanen et al. (2010a) focus on cross-border surveillance operations dealing with time-critical data communication between multinational organizations. This problem is common among LEAs. Criminals are working more often abroad due the European integration, but LEAs do not have common protocols and procedures in regard to how to pass information among each other. Particularly machine-to-machine communication in cross-border covert operations has not yet been researched.

In traditional organizations, knowledge tends to flow along organizational lines, from the top to the bottom. The knowledge might be created in lower parts of the organization, but usually, it must first go to the top, and only from there can it spread out. This pattern seldom results in making knowledge available in a timely fashion and where it is needed most. Also, dependency of individual employees may cause vulnerabilities to information flow, especially in cross-border cases (Vii-tanen, Happonen, Patama, & Rajamäki, 2010).

Preventing crimes is a very time-critical business, and LEAs are usually very traditional and hierarchical organizations. This seems to be a troubling combination, although the long tradition also has good aspects. Time criticality has forced shortcuts in the normal operational passing of information in most of the hierarchy. In most cases, information is sent and used in a timely manner. Information can flow across organizational lines, reaching the right people who can use it in a way that best serves the goal of the organization in question. But, if the case is unique or not often repeated, you might end up in a situation that no longer offers shortcuts. Then the information will start to go up and down the ladders of the hierarchy, and the moment is lost. This problem is prominent in LEAs' cross-border operations (Rajamäki & Viitanen, 2014; Viitanen et al., 2010).

Rajamäki, J. & Viitanen, J. (2014). Near border information exchange procedures for law enforcement authorities. International Journal of Systems Applications, Engineering & Development. Vol. 8, 2015-2020. Available: http://www.naun.org/main/UPress/saed/2014/a042014-082.pdf

Abstract: European integration has increased organized crime, e.g. the transport of illegal goods in Europe. This means that the transmitting of tracking and other status in-formation between nations and their Law Enforcement Authorities (LEAs) should be-come an everyday business. The goal of this paper is to find possible bottlenecks in in-ternational cooperation between LEAs and to find possible solutions for them. The fol-lowing area can be considered as a part of the MACICO (Multi-Agency Cooperation In Cross-border Operations) Celtic Plus research project. The target of the paper is to pre-sent administrative and technical solutions to improve multi-organizational tracking solutions. Namely, the goal is to make it possible to create a timely situational picture in joint multinational and interagency operations. This paper will provide guidance for preparing appropriate plans and doctrine proposals for joint operations and training. Also technical solutions and bottlenecks are briefly covered in this paper.

6.5 Multinational Tracking Systems

The SATERISK project studied risks associated with satellite-based tracking, especially whether the use of tracking generated additional risks (Rajamäki, Pirinen, & Knuuttila, 2012). The MOBI project aimed to create a common information and communication technology (ICT) infrastructure for all emergency response vehicles (ERVs), and navigation and tracking are one of the most important services needed in all ERVs (Tikanmäki, Rajamäki, & Pirinen, 2014). As regard tracking, the MAC-ICO project studied cross-border operations.

A global navigation satellite system (GNSS) is a satellite navigation system with global coverage. GNSS-based navigation has become part of daily life. Timing, orientation, positioning and navigation are deeply embedded in the lives of every-one. The use of GNSS is still growing—a recent market research report predicts that the GNSS market will likely double by 2016 (ABI Research, 2011). At the moment, only the United States NAVSTAR Global Positioning System (GPS) and the Russian GLONASS are globally operational GNSSs. China is planning to expand its regional Beidou navigation system into the global Compass navigation system by 2020. The European Union's Galileo positioning system is a GNSS in its initial deployment phase. The European Commission launched its first two operational satellites in Oc-tober 2011, and the Galileo system is scheduled to be fully operational by 2020 at the earliest.

The actual GNSSs vary, but generally they consist of three major segments: the space segment, the positioning equipment segment, and the control segment. For example, the space segment of GPS consists of a system of 24 space-based satellites, of which three are spares. The GPS satellite orbital radius is 26,561.7 km, and each satellite has a 12-hour orbit. Precise time is provided by a redundant system of rubidium and/or cesium atomic clock boards for the space vehicle. Each GPS satellite is capable of continuously transmitting L1 and L2 signals (L1 = 1575.42 MHz and L2 = 1227.6 MHz) for navigation and timing, and an L3 signal for nuclear detonation

data (O'Brien & Griffin, 2007). It is also capable of receiving commands and data from the master control station and data from remote antennas via S-band transmissions.

In general, the GNSS receiver compares the time a signal was transmitted by a satellite with the time it was received. The time difference, along with the location of the satellites, allows the receiver to determine the user location. Signals from a minimum of four different satellites are required to determine the three-dimensional position. The receiver usually consists of an antenna assembly, radio frequency (RF) receiver, data processor, control/display unit, power supply, and interface unit (O'Brien & Griffin, 2007).

The control segment commands, uploads system and control data to the space vehicles, monitors their health, and tracks the space vehicles to validate ephemeris data. The control segment of GPS consists of a master control station located in Colo-rado Springs; five remote monitor stations are located in Hawaii, Ascension Island, Diego Garcia, Kwajalein, and Colorado Springs; three ground antennas are located at Ascension Island, Diego Garcia, and Kwajalein and a Pre-Launch Compatibility Station, which can also function as a ground antenna, is located at Cape Canaveral (O'Brien & Griffin, 2007).

A tracking system combines navigation and telecommunications technologies. When the SATERISK project ended, Rajamäki (2012) analyzed it results and achievements from the point of view of cross-border operations. With regard to cross-border operational procedures, both technical and legislative risks should be taken into account (Rajamäki, 2012).

Rajamäki, J. (2012). Cross-border satellite-based tracking: Needs, approach, benefits and competition. Ubiquitous Positioning, Indoor Navigation, and Location Based Ser-vice (UPINLBS), 2012, 1-8. doi:10.1109/UPINLBS.2012.6409747

Abstract: The aim of this study is to provide an improved understanding of the structural characteristics and the dynamic evolution of cross-border satellite-based tracking services. The study is based on the results and lessons learned from the SATERISK research project executed 2008-2011, with special attention taken how to utilize that knowledge within a new safety and security services. In this context, the NABC (Need, Approach, Benefits and Competition) approach is used. The study shows that most satellite-based tracking systems and services do not form a coherent whole. With the risk analysis procedures and tools developed in the SATERISK project, a unique risk profile for each use case can be created. This enables better products and services for both public and private security organizations.

All tracking systems are relatively complicated, and they consist of many tech-nical segments, such as the three GNSS segments (space, tracking/positioning equipment, and control), a communication segment, a data processing segment, a user interface for external applications, and an end-user segment. The basic principle of a GNSS-based tracking system is that a tracked device is positioned by GNSS, and positioning data are delivered for post-processing via mobile networks, the Internet, or a secure network (Kämppi & Guinness, 2010). The system is complex and vulnerable to many kinds of cyber-attacks (Kämppi, Rajamäki, & Guinness, 2009). In cases where receiving satellite signals is not possible, alternative methods can be used. Rajamäki, Rathod and Kämppi (2014) present a modular system-level description of an improved tracking system for emergency response. Within GNSS systems, a tracking device calculates its location itself and sends this information for post-processing. In most other system, location of the tracking device - 'tag' - will be calculated by the system and the tag sends no location data. However, with current knowledge, the integration of these different technologies is realizable (Rajamäki, Rathod, & Kämppi, 2014).

Rajamäki, J., Rathod, P., & Kämppi, P. (2014). A redundant tracking system for public safety and emergency response: Reporting past research, present findings and future directions. International Journal of Systems Applications, Engineering & Development, 8, 76-83. Available: http://www.naun.org/main/UPress/saed/2014/a202005-163.pdf

Abstract: Tracking is playing very significant role in modern public safety and emergency response. There are many tracking technology available. Such as the geographic information systems (GIS) and global navigation satellite systems (GNSS) have transformed local, national and international emergencies and disasters response services. GIS/GNSS technologies offer great deal of assistance in public safety and emergency response enabling emergency management agencies to efficiently allocate resources, model risk and direct emergency response and recovery personnel. On the one hand, these technologies are bringing many innovative advantages to organizations responsible for public safety and emergency response. While on the other hand, it brings many challenges. For example, current GNSS-based tracking systems have serious technical flaws and vulnerabilities. This paper is reporting our research studies conducted in various projects and it also presents our finds including a detailed modular system-level description for a hybrid tracking system including control, space, tracking, communication, data processing, end-user and external applications segments. The paper further discusses and suggests how the technical vulnerabilities of GNSS-based tracking systems could be avoided considering hybrid tracking segment and multi-channel communication paths. The paper is also exploring future possibilities to provide smooth tracking for public safety and emergency response.

References

ABI Research. (2011). *High precision GNSS market set to increase almost 100% by 2016*.

Ameyugo, G., Art, M., Esteves, A. S., & Piskorski, J. (2012). Creation of an EU-level information exchange network in the domain of border security. *Intelligence and Security Informatics Conference (EISIC)*, 2012 European, 356-358. doi:10.1109/EISIC.2012.55

Benson, Y. (2011). *Authority IT serving national security, VIRVE Day -Seminar*, Helsinki.

Ferrus, R., Pisz, R., Sallent, O., & Baldini, G. (2013). Public safety mobile broadband: A techno-economic perspective. *Vehicular Technology Magazine, IEEE*, 8(2), 28-36. doi:10.1109/MVT.2013.2252273

Finnish security and defence policy 2009. Government report (2009). (Prime Minister's Office Publications 13/2009 ed.). Helsinki: Prime Minister's Office. Available: http://vnk.fi/julkaisukansio/2009/j11-turvallisuus-j12-sakerhets-j13-finnish/pdf/en.pdf

Kämppi, P., & Guinness, R. (2010). Technical risk analysis for satellite based tracking systems. *Integrated Communications, Navigation and Surveillance Conference*, Herndon. M3-1-M3-16.

Kämppi, P., Rajamäki, J., & Guinness, R. (2009). Information security risks for satellite tracking. *International Journal of Computers and Communications*, 3(1), 9-16.

Laitinen, I. (2011). Role of border control in the new EU security architecture and an update on Frontex activities. *Situation Scope Seminar*, Äkäslompolo.

Lehti, M., Pursiainen, H., Volanen, R., Luoma, R., Timonen, P., Hagman, R., & Kana-ne, I. (2009). *Promoting the availability of secure telecommunications networks*. Helsinki: The Ministry of Transport and Communications Publication.

Manni, K. (2011). *Security communications – possibilities and challenges*. VIRVE Day -Seminar, Helsinki.

O'Brien, P. J., & Griffin, J. M. (2007). *Global positioning system systems engineering case study*. Hobson Way: Wright-Patterson AFB, OH: Air Force Center for Systems Engineering (AF CSE), Air Force Institute of Technology (AFIT).

Rajamäki, J., Pirinen, R., & Knuuttila, J. (Eds.). (2012). *SATERISK - risks of satellite-based tracking: Sample of evidence series*. Vantaa: Laurea-University of Applied Sci-ences, Leppävaara Unit.

Rajamäki, J. (2014). Software intensive GNSS-based tracking systems for improving law enforcement. *WSEAS Transactions on System and Control*, Vol. 9, 629-639.

Rajamäki, J., & Rathod, P. (2013). Leveraging benefits of standardized utility and cloud computing with service-oriented architecture in public protection and disaster relief. In S. Lopes (Ed.), *Recent advances in computer engineering series*, vol. 16 (pp. 74-80) WSEAS Press.

Rajamäki, J., Rathod, P., & Kämppi, P. (2014). A redundant tracking system for public safety and emergency response: Reporting past research, present findings and future directions. *International Journal of Systems Applications, Engineering & Development*, 8, 76-83.

Rajamäki, J., & Ruohomäki, P. (2013). Multi-agency cooperation in cross-border operations: Information exchange between law enforcement authorities. *Proceedings of the International Congress of Engineering and Informatics*, 271-279.

Rajamäki, J., & Viitanen, J. (2014). Near border information exchange procedures for law enforcement authorities. *International Journal of Systems Applications, Engineering & Development*, 8, 2015-2020.

Rajamäki, J. (2012). Cross-border satellite-based tracking: Needs, approach, benefits and competition. *Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS)*, 2012, 1-8. doi:10.1109/UPINLBS.2012.6409747

Riippa, H. (2011). *The future of PPDR networks in Finland – requirements and options*. Unpublished manuscript.

Ruohomäki, P. (2012). *Public key infrastructure operations model*. Espoo: Laurea-ammattikorkeakoulu.

Taitto, P. (2007). Tavoitteena hyvät käytännöt. Teoksessa Heusala, Anna-Liisa–Taitto, Petteri & Valtonen, Vesa (Toim.) *Viranomaisyhteistyö–hyvät Käytännöt*. Pelastusopiston Julkaisu.D-Sarja, 1, 2007.

Tikanmäki, I., & Rajamäki, J. (2012). Exploiting security, safety and situational relat-ed services by using remotely piloted aircrafts. *3rd International Conference on En-ergy, Environment, Devices, Systems, Communications, Computers (INEEE'12)*, 50-55.

Tikanmäki, I., Rajamäki, J., & Pirinen, R. (Eds.). (2014). *Mobile object bus interaction - designing future emergency vehicles*. Vantaa: Laurea.

Tikanmäki, I., & Tuohimaa, T. (2011). How real time picture and situational aware-ness can be improved by using unmanned aircraft systems (UAS)? *Recent Researches in Communications, Electrical & Computer Engineering, WSEAS Press*, 28-33.

Tikanmäki, I., Tuohimaa, T., & Ruoslahti, H. (2012). Developing a service innovation utilizing remotely piloted aircraft system (RPAS). *International Journal of Systems Applications, Engineering & Development*, Vol. 6(Issue 4), 279-287.

Toivola, T. (2006). *Verkostoituva yrittäjyys. Strategiana Kumppanuus*. Edita Prima Oy, Helsinki.

Tuohimaa, T. (2014). Studies of unmanned aircraft systems from the perspective of operational use.

Tuohimaa, T., & Tikanmäki, I. S. (2011). The strategic management challenges of de-veloping unmanned aerial vehicles in public safety organizations. *Recent Researches in Communications, Electrical & Computer Engineering, WSEAS Press*, 34-39.

Viitanen, J., Happonen, M., Patama, P., & Rajamäki, J. (2010). Near border proce-dures for tracking information. *WSEAS TRANSACTIONS on SYSTEMS*, 9(3), 223-232.

Zaerens, K., & Mannonen, J. (2012). Concept for the construction of high security environment in public authority cloud. *Embedded and multimedia computing technology and service* (pp. 401-408) Springer.

Jyri Rajamäki

7. TRUST BUILDING

Public protection and disaster relief (PPDR) operations are more and more depend-ent on networks and data processing infrastructure. Incidents, such as natural hazards and organized crime, do not respect national boundaries. As a consequence, there is an increased need for European collaboration and information sharing related to public safety communications (PSC) and information exchange technologies and procedures. This was the reason why the MACICO project was initiated (J. Rajamäki, 2014d).

Jyri Rajamäki (2014) Plenary Lecture 3. Multi-Agency Cooperation in Cross-border Operations, 8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14)

Extended abstract: Multi-Agency Cooperation in Cross-border Operations (MACICO) is the Celtic-Plus project with 9 partners from Finland, France, and Spain; duration Dec 2011–May 2014. It develops a concept for interworking of 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 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. The plenary lecture presents the scope and results of the MACICO research project achieved so far. The main conclusion of the MACICO project is that technological interoperability challenges are easy to solve; the only drag is the economic situations, meaning that PSC operators are not investing in developing their networks. However, operational interoperability challenges are much more difficult, because the main problem there is distrust between public safety authorities.

According to most studies and interviews carried out within the MACICO project, the topic "trust building" could be seen as the most important issue with regard to multi-agency cooperation.

Cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. According to DIGILE (2014), it is important to complement the currently dominating "cyber security as a barrier" perspective by emphasizing the role of "cyber security as an enabler" of new business, interactions and services, and recognizing that trust is a positive driver for growth.

Public safety infrastructure is becoming more and more dependent on unpredictable cyber risks. Everywhere present computing means that PPDR agencies do not know when they are using dependable devices or services, and there are chain reactions of unpredictable risks. If cyber security risks are not made ready, PPDR agencies like all organizations will face severe disasters over time (DIGILE, 2014). In the future, Finland could be a globally recognized hub for trusted and trust-enhancing digital services based on top-level cyber security solutions and services actively developed and maintained in international cooperation by leading experts and companies (Ahokangas et al., 2014).

Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world, and it has the following themes: security technology, situation awareness, security management and resiliency, as shown in Figure 7-1 (Ahokangas et al., 2014). Situational awareness is needed for having correct understanding of security inci-dents, network traffic, and other important aspects that affect security. Security technologies are needed for protection. Human aspects have to rule in via security management. Consequently, resilient systems and infrastructures are able to resist and recover from disturbances (Ahokangas et al., 2014).

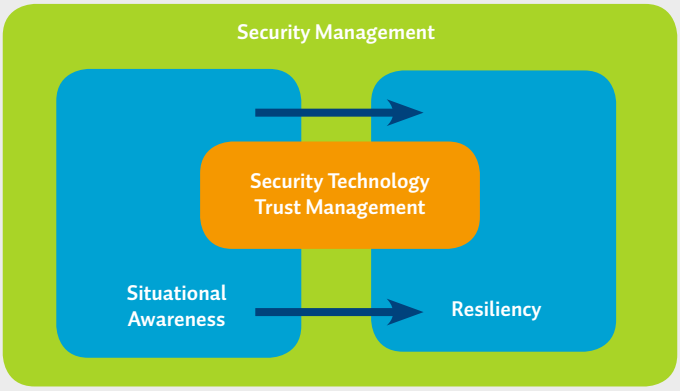


Figure 7-1 Themes of trust building (Ahokangas et al., 2014)

7.1 Security technologies

According to Akohankgas et al. (2014), security technologies are technical means for fulfilling the recognized security requirements of the system, and for building resilient systems with dependable hardware and software that can also meet future security challenges. They continue that security technologies enable the technical protection of infrastructure, platforms, devices, services, and data.

7.1.1 Securing network infrastructures

The MACICO project widely researches and develops cyber secure interconnecting of different voice and data communication networks for public safety. With respect to European mission-critical public safety communications, TETRA or Tetrapol are widely used and recommended. There are no other improved standards available at the moment. Data transmission over TETRA is rather slow and will not satisfy future needs. However, it is extremely reliable, regardless of its low capacity communication. Wideband data (TEDS) is an effort towards improved data services (Nouri, Lottici, Reggiannini, Ball, & Rayne, 2006), but TEDS falls short of current and future needs. However, a dedicated PPDR mobile data network independent of public mobile networks may not be available in Europe until 2020.

Roaming refers to the situation when a device is moving outside of its home network. Roaming can create a situation where the mobile device is not able to deliver location data via SMS, GPRS, 3G or 4G. Roaming between TETRA networks is not in operational use, creating threats within remote border districts where people could stray across the borderline. The Inter-System Interface (ISI) forms part of the TETRA standard suite, and it defines the connectivity between two independent TETRA networks. The main purpose of ISI is to allow cross-border communications between European nations for effective co-operation of security organizations in case of major incidents, such as international crimes or natural disasters. Another initial objective was to create large homogeneous networks based on different infrastructures from various manufacturers. However, this proposition has been too complex to achieve because of the substantial differences between TETRA implementations. The first roaming agreements were set up in Scandinavia for GSM. Now, the same should be done with TETRA ISI roaming. The ISI between Norway and Sweden is, in fact, under implementation. The MACICO project's R&D of voice communications includes TETRA-TETRA, TETRA-Tetrapol and Tetrapol-Tetrapo interoperability as well as TETRA over LTE services.

With regard to data communications technology, the MACICO project's main research area is Distributed Systems intercommunication Protocol (DSiP). The decentralized architecture based on DSiP is highly fault-tolerant in normal conditions as well as in crises (J. Rajamäki, 2012). The software-based approach is independent of different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables the building of a practical and timeless cyber-secure

data network for the multi-organizational environment, which, being fully decentralized, is hard to injure. The networks of different organizations are virtually fully separated, but if required, they can exchange messages and other information that makes them interoperable.

Rajamäki, J. (2012). Redundant multichannel public safety communications network for public protection and disaster relief (PPDR) organizations. 3rd International Conference on Energy, Environment, Devices, Systems, Commu-nications, Computers (INEEE'12) (Best paper reward). Available: http://www.wseas.us/e-library/conferences/2012/Rovaniemi/INEE/INEE-09.pdf

Abstract: All Public Protection and Disaster Relief (PPDR) organizations across Europe have multiple similar needs. A common cyber secure voice and data network for PPDR brings synergy and enables interoperability; separate networks are wasting of resources. This paper focuses on future broadband data communication needs of PPDR actors and presents a new fully redundant data communications network structure for Public Safety Communications (PSC). The architecture is decentralized and all critical communication paths have fully redundancy. Although having common physical connections, all network actors and elements (multichannel routers, nodes) are identified as well as every organisation's all user levels and their rights to different data sources are known. The network architecture based on the Distributed Systems intercommunication Protocol (DSiP) is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent from different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables to build a practical and timeless cyber-secure data network for PPDR environment, which being fully decentralized is hard to injure. The networks of different organizations are virtually fully separated, but if wanted they can exchange messages and other information which makes them interoperable.

Proposed solutions using DSiP achieve cyber security objectives mainly by preventing cyber-attacks against critical communications channels, reducing vulnerabilities against current network infrastructure, and minimizing damage and recovery time if a cyber-attack is carried out. In September 2012, Louhi Security Oy security-audited the DSiP solution, giving it high credentials. The purpose of the audit was to locate and identify potential cyber-risks in the DSiP system. The audit was conducted based on methods from the OSSTMM (Open Source Security Testing Methodology). Both commercial and open source tools were used in the audit. According to the audit, the DSiP system provides a high level of reliability and security for applications demanding uninterruptable communication and extended usability.

7.1.2 Mobile platform security

The Finnish way to provide digital services to the field for public protection and disaster relief actors is via their vehicles. From emergency response vehicles' point of view, the root of continuums of different Finnish research and development projects is as follows: First, the RIESCA project studied, for example, procurement and maintenance procedures of different critical information systems that support society and patrol cars have such critical information systems. Second, the MOBI project researched the integration of patrol cars' electric, electronic, and ICT systems. It also equipped a demo vehicle. Third, the SATERISK project studied different kinds of technical, operational, and legislative risks with regard to satellite-based tracking and navigations. These are vital services for patrol cars. Fourth, the TUVE – Information Security Network project, provides the communications infrastructure for Finnish patrol cars. Fifth, KEJO – field command system, develops a common field command system for all Finnish PPRD actors. Sixth, VITJA – the reforming project of the Finnish polices information systems, replaces almost all major operational information systems used by the Finnish police. RIESCA, SATERISK and MOBI were Laurea's R&D projects. TUVE, KEJO and VITJA are national projects in which Laurea has no official role. The MACICO project develops a concept for interworking of different security organizations in their daily activity.

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 (J. Rajamäki, 2014c). However, more multidisciplinary research is needed.

Rajamäki, J. (2014c). The MOBI project: Common mobile digital services for all public protection and disaster relief (PPDR) vehicles. In J. Music (Ed.), Recent advances in computer engineering, communications and information technology (pp. 120-125) WSEAS Press. Available: http://www.wseas.us/e-library/conferences/2014/Tenerife/INFORM/INFORM-16.pdf

Abstract: The MOBI project results that all public protection and disaster relief (PPDR) actors have many similar applications in their vehicles 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, and need of inventory of equipment. The study shows that information and communication technology (ICT) systems should be designed as modular system

where individual modules could be replaced without the need to change other parts of the whole system. The modules are 1) a vehicle infrastructure and power management layer, 2) a communications layer, 3) a service platform and common services layer, and 4) an actor-specific services layer. Some aspects, such as security, power efficiency and product safety regulations run through all the layers. According to our approach, although police patrol cars, fire trucks and ambulances are different their communications layer as well as their service platform and common services layer could be identical. This enables interoperability between PPDR organisations and first responders, at least at technical level.

Within the duration of the MOBI and MACICO projects, the society has changed radically; application of social media has exploded, and the authorities from advanced countries have taken these matters into account when developing their digital services for public safety (Akhgar, Fortune, Hayes, Guerra, & Manso, 2013). 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 (J. Rajamäki et al., 2014). Kantarci and Mouftah (2014) present a framework where the Internet can enhance public safety by crowd management via sensing services that are provided by smart phones equipped with various types of sensors. Their trustworthy sensing for crowd management concept can enhance the utility of the public safety authority up to 85% (Kantarci & Mouftah, 2014).

Rajamäki, J., Knuuttila, J., Suni, O., Silanen, H., Tuomola, A., & Meros, P. (2014). How to empower policemen and their vehicles: A multiple case study analysis of seven public safety related ICT projects. International Journal of Systems Applications, Engineering & Development, 8, 238-249. Available: http://www.naun.org/main/UPress/saed/2014/a102014-083.pdf

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.

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, overly strict data security regulations may rule out the mobile utilization of digital services in the field. However, most often, the biggest cyber threat is the so-called "insider threat", such as the Snowden and Manning cases indicate. When taking 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 (J. Rajamäki et al., 2014).

7.1.3 Identification and privacy protection

According to Ahokangas et al. (2014), *"secure user identification and authorization are necessary features in most secure systems, and well-known technologies exist for their implementation. Typically, processes and data objects are associated with an owner, represented in the computer system by a user account, who sets the access rights for others."* However, most digital services for the PPDR sector are supplied via stand-alone systems with-out built-in safe-guards. Trust and control have typically been viewed as opposites or substitutes (O'Leary, Orlikowski, & Yates, 2002). The society is presented as "soft surveillance, knowledge and non-forgetting history data" by Finnish futurologist Mannermaa (2008). He believes that every action of the authorities must be tracked, and surveillance should be commonly agreed upon and transparent. The public feels they have lost control over their own data, and they do not know who handles their personal data, when it is being handled, and for what purpose. They also believe that there are enforcement and application problems. The concern of the public about the collecting and handling of their personal data can be answered by increasing the transparency of these operations (Mannermaa, 2008). Jyri Rajamäki's academic dissertation (J. Rajamäki, 2014e) widely researches this phenomenon among others.

Rajamäki, J. (2014e). Studies of satellite-based tracking systems for improving law enforcement: Comprising investigation data, digital evidence and monitoring of legality. Jyväskylä Studies in Computing, Jyväskylä: University of Jyväskylä, Available: https://jyx.jyu.fi/dspace/bitstream/handle/123456789/44087/978-951-39-5789-6_vaitos06092014.pdf?sequence=1

Abstract: Law enforcement agencies (LEAs) constantly seeks new technological recording, retrieving and monitoring solutions that would facilitate their combat against or-ganized crime. This dissertation is interested in how new types of satellite-based tracking sensors, mobile monitoring stations and their associated

communication channels for LEAs can be understood and designed, taking into account the chain-of-custody and monitoring-of-legality requirements. The empirical data for the eight cases of the dissertation were collected within four research projects from 2007 to 2014. The theoretical framework is built on the systems of systems theory and the normative design theories of information infrastructures and software-intensive systems. Satellite-based sensors and systems benefit LEAs when tracking non-cooperative targets. However, management of numerous electronic tracking devices within many simultaneous crime investigations has proven to be a demanding task for LEAs. Complications have spawned many lawsuits and negative publicity. These episodes have diminished citizens' trust in a constitutional state. It has been verified by means of participative observations that LEAs have a tendency to create two-level systems: some that work on the streets and others that are valid in the courts of justice. The importance of transparency is emphasized at all EU administrative levels. However, LEAs concentrate only on data acquisition rather than on making their operations transparent throughout. Because of the privacy protection of suspects, investigations and data acquisition cannot be made public. However, these operations could be so transparent that the criticism and control made by citizens is possible to come true. To improve LEAs' processes, the three main functions (crime investigation, chain-of-custody and monitoring-of-legality) should be considered together. Combining their separate information systems will avoid tripling the workload. It will also lead to additional benefits, such as transparency of surveillance and a new tool for achieving a balance between surveillance and privacy.

A global trend is to increase the use of cloud service technology when providing critical services. Data has gone into cloud and will not come back to end users' devices. Also, government data has already gone to a cloud, and in the future, more and more of critical government data will migrate to cloud servers and services. According to Ahokangas et al. (2014), *"partnerships between cloud service providers and security solution providers will become more common. We will see emerging of cloud service specific solution providers as well. Identity management and encryption will be most important cloud security services to be offered. These services will be eventually offered for small to medium size business as well. We will also see emergence of cloud security standards ... Challenges are that quite often cloud service providers believe that security is just an end user issue and firewall means security. Therefore, currently, we do not have proper cloud security standards and we lack of awareness of a true understanding of comprehensive cloud security"* (Ahokangas et al., 2014). Within the MACICO project, Rajamäki and Rathod (2014) have studied utility and cloud computing with service-oriented architecture (SOA) in the field of public protection and disaster relief. All processes, technologies, and contracts in utility computing and service-oriented architecture should be standardized to leverage the full benefits of these innovative technologies in PPDR (J. Rajamäki & Rathod, 2014), and a framework is required in order to assure that the quality of service in multi-supplier governance is high enough and meets the expectations of all parties.

Rajamäki, J., & Rathod, P. (2014). How standardized utility cloud services and service-oriented architecture benefits in public protection and disaster relief? International Journal of Computers and Communications, 8, 86-93. Available: http://www.naun.org/main/UPress/cc/2014/a222012-133.pdf

Abstract: All emergency response service providers in developed countries are using In-formation and Communication Technology (ICT) tools and technologies. Recent studies shows majority of the public protection and disaster relief (PPDR) organizations are using ICT services in very heterogeneous and customized delivery methods. Many organizations have tailored processes, contracts and technologies. PPDR organizations are lacking supporting infrastructure and expertise hence ICT services are managed by internal and external suppliers. On other side, ICT field is going through constant in-novations as a process of evaluation in technologies. Cutting-edge technologies including cloud computing, utility computing and service-oriented architecture (SOA) can be beneficial in emergency response services. Advancement in these technologies is constantly bringing various challenges. This paper is investigating use of utility cloud ser-vices and service-oriented architecture in public protection and disaster relief operations. The paper studies and compares cloud and utility computing the context of ICT services. The paper is also investigating design principles of service-oriented architecture to leverage benefits in PPDR. The study argues that all processes, technologies and contracts in utility computing and service-oriented architecture should be standardized to leverage the full benefits of these innovative technologies in PPDR. Further, it also discusses and describes the benefits and disadvantages of standardization and lack of standardization respectively.

7.2 Security management and governance

The "weakest link" of security is the human and organizational aspects of information security. According to Ahokangas et al. (2014) *"although risk assessment methods and information security plans and policies are nowadays an essential part of many organizations, the managerial aspects of information security still remain challenging, especially in emerging technological contexts. The incentives for information security investments remain a black box, despite the fact that the lack of budget for information security solutions is repeatedly reported as a top challenge. Finally, management executives still lack an understanding of information security requirements and importance. Therefore, for organizations to be able to develop and employ technical solutions that will find human resources as an ally for security protection rather than as an enemy, security management and governance is essential."*

7.2.1 Security policy development and implementation

Information security policies are the main element used to communicate security work practices to ICT stakeholders (Ahokangas et al., 2014). KATAKRI is a Finnish national security auditing criteria that is based on several ISMS standards and best practices. The criteria are divided into four main areas: (1) administrative security, (2) personnel security, (3) physical security, and (4) information security. Areas are not meant to be used independently. It is instructed to take all four areas into account when performing an accreditation audit using KATAKRI. Laurea University of Applied Sciences has a long experience of applying KATAKRI as a tool for improving organizations' security policies. In pursuance of the MACICO project, a multiple case study analysis (J. Rajamäki, 2014b) has been prepared. It consists of five individual cases studies that research how KATAKRI is suitable for different types of organizations. Four of these individual cases were published as theses (Kimiläinen, 2011; Kojo, 2013; Laitinen, 2013; Martiskainen, 2012) and one was a conference paper (J. Rajamäki, 2014a).

Rajamäki, J. (2014b). Information security policy development and implementation piggybacking onto Finnish national security auditing criteria KATAKRI. The 5th European Conference of Computer Science.

Abstract: The "weakest link" of security is the human and organizational aspects of information security. Nowadays, risk assessment methods and information security plans and policies are an essential part of many organizations. However, the managerial aspects of information security often remain challenging, especially in emerging technological contexts, and management executives lack an understanding of information security requirements and importance. KATAKRI is a Finnish national security auditing criteria that is based on several information security management system standards and best practices, including four main areas: (1) administrative security, (2) personnel security, (3) physical security, and (4) information security. This multiple case study analysis consists of five individual cases studies that research how KATAKRI is suitable for different types of organizations. The cross-case conclusions examine what type of usability KATAKRI has in information security policy development and implementation in general. The results revealed that organizations have deemed the security policy useful. However, the individual contents and practices of the different security policies differed quite a lot from each other. In particular, the companies found particularly the implementation of security policies within their organizations to be a challenge.

Kojo, J. (2013). Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla (Autentication of security management level in Finnish authority unit using National Security Auditing Criteria). Theseus: Laurea. Available: https://www.theseus.fi/bitstream/handle/10024/69750/kojo_ont_25112013.pdf?sequence=1

Abstract: The main objective of this thesis was to authenticate the security management level in the Finnish authority unit. Authentication was performed using the National Security Auditing Criteria (Kansallinen turvallisuusauditointikriteeristö ie KATAKRI). The other objective was to examine what type of usability National Security Auditing Criteria have in such an authority unit. This was not an official audit in the National Security Auditing Criteria, even if the verification was adapted from the actual security audit process. Security assessment was also limited only to the administrative security ie security management and its requirements for the increased level (III).

This thesis was a qualitative research project, the research methods of which were document analysis, interviews and observation. The hermeneutical method was used as the qualitative research genre. The primary data collection method was the review of security documents, the second method was structured interviews with questions based on the National Security Auditing Criteria and the third method was observation, in practice monitoring the security management activities of the target unit.

The initial section of this thesis consists of the theoretical framework of research and the theory of security audits. Those are followed by the audit of the object, describing the whole audit process and showing the development of the result analysis. The results were drawn up on the result analysis that formed the basis for a summary of developments to the security management. If necessary, these developments can be used by the object to improve their level of requirements and administrative security or to form a development plan for security. The results of security management were also recorded in this report as an appendix.

As a result of this thesis project a comprehensive, security-perspective report on security management about the unit was obtained. Importing the National Security Auditing Criteria to the authorities' environment seemed to be highly challenging at first. However, time by time the author learned how to apply observations to the requirement levels of National Security Auditing Criteria and to the operating environment. National Security Auditing Criteria as a tool was not already familiar to the unit. However, low awareness could create some authenticity to processes of interviews and observations. If the audit should be carried out exclusively with

documentation and its information, would authentication of requirement levels would be inadequate.

This security audit formed as a pre-audit for the unit. If the unit carried out the official National Security Auditing Criteria's audit process, this audit report could help to prepare for it considerably better. Based on the result analysis of the audit report it can be stated that the security management level of the authority unit could not reach the requirements of the increased level (III) of the National Security Auditing Criteria on administrative security. However, the object reached the maximum level of requirements of the base level.

Laitinen, O. (2013). Yrityksen turvallisuuspolitiikan laatiminen (Drafting a company's security policy). Theseus: Laurea (Master thesis). Available: https://www.theseus.fi/bitstream/handle/10024/61821/Opinnaytetyo_Olli_Laitinen_versio%20V.pdf?sequence=1

Abstract: Security within entrepreneurship is an essential factor in the preservation and growth of Finland's international competitiveness. In order to achieve its strategic goals, a company must guarantee the security of its people, its reputation, information, assets and environment. The creation of a company's security policy is the starting point for goal-directed and systematic security management. The security policy is a declaration of the significance of security in the company's business. Additionally, the security policy defines the company's policies and practices for personnel collaboration.

The aim of this work is to outline the drafting process of a security policy and the best procedures for defining its content. An additional aim is to formulate a model for a company's security policy and to provide recommendations for its implementation.
The basis for the empirical research was formed by interviews carried out in four companies. The interview framework used the National Security Auditing Criteria (KATAKRI). The National Security Auditing Criteria are a mutual security criteria for officials and companies for unifying the communal security procedures and to improve self-monitoring and auditing. The National Security Auditing Criteria are an auditing tool used by the officials when carrying out inspections on the level of security within a company or a community.

The results of the work reveal that companies have deemed the security policy useful, since all companies had already composed their own security policy (or a similar docu-ment). On the other hand, the individual contents and practices of the different security policies differed quite a lot from each other. There was a lack of a common operation model, so this work aims to even out discrepancies in the future. In particular, the companies found particularly the implementation of security policies within their organizations to be a challenge.

As a result of the work, a model for a company's security policy is included as an at-tachment. It is meant to be freely utilized by all Finnish companies and organizations.

Martiskainen, M. (2012). Sisäinen turvallisuus-auditointi aikuiskoulutusoppi-laitoksessa (Internal security audit in an adult education centre). Theseus: Laurea. Available: https://publications.theseus.fi/bitstream/handle/10024/46248/Martiskainen_Mona-Kristiina.pdf?sequence=1

Abstract: This thesis focuses on how an adult education centre can prepare internally for a security auditing process. The purpose of this thesis is to achieve administrative security control by internal audit. Internal audit is based on the National Security Auditing Criteria KATAKRI and it is executed in an authentic learning institution environment. The need for this thesis is practical: research results serve security management in general and offer one tool to control security issues in the school environment.

The first section of this thesis presents the prevailing and the ideal security situation of the adult education centre. The target level was set at the recommended level of KATAKRI administrative security because it meets best the needs of the examined education centre. The research methods used are observation and literature overview. As a result, the thesis describes a model of an internal auditing process in an adult education centre. The results are presented from a continuing development point of view, utilizing the Deming PDCA (plan-do-check-act) cycle model.

Security matters of different learning institutes have recently had a great deal of media coverage. The results of this thesis show that education centres are ready to work for a better security level. However, problems occur due to lack of time resources, explicit tools or adequately defined goals. These weaknesses have a negative impact on the development of security culture.

Kimiläinen, M. (2011.) Yritys X:n henkilöstö-turvallisuuden ja fyysisen turvallisuuden esiauditointi Kansallisella turvallisuusauditointikriteeristöllä (Pre - audit of personnel security and physical security based on The National Security Audit Criteria). Theseus: Laurea. Available: https://www.theseus.fi/bitstream/handle/10024/33694/Kimilainen%20Mikko%20ONT%20Raportti.pdf?sequence=1

Abstract: The purpose of this thesis w as to execute a pre - audit to Company X in the fields of personnel security and physical security. The pre - audit was based only on The National Security Audit Criteria, called in Finnish "Kansallinen

turvallisuusauditointi-kriteeristö (KATAKRI)". The study was executed from a consultant's perspective and with the principles of a functional thesis. The objectives of this study were to compare the state of Company X's personnel security and physical security fields with KATAKRI's demands. The study was defined to cover only the personnel security and physical security sections of KATAKRI. For both of the audited security fields, were chosen their own objective levels of KATAKRI. One of the objectives of the study was also to evaluate the compatibility and usefulness of KATAKRI compared to the needs of Company X. One of the reasons for evaluating it, was to examine possible benefits that the company might receive from an official KATAKRI audit. In addition one of the purposes of the study was to develop steps to improve the deficiencies found based on the audit. The study itself consists of four main categories: context, theory basis, execution of the study and conclusions. The context depicts the operational environment, theme, execution stages and definitions of the study. The theory basis forms a scientific based information basis to the study and the execution study describes the audit process and its results. The conclusions category consists of the evaluations of the audit results and the improvement steps. The objective of the study was to produce results from two different perspectives: evaluating the compatibility and usefulness of KATAKRI and the fulfilling of the KATAKRI's audit requirements. The results of the audit were relatively good. Almost all the requirements were met by both the personnel and physical security sections and the identified deficiencies were only minor. The biggest challenges with the results concerned the compatibility of KATAKRI. The challenges were ma inly affiliated with some obscurities and interpretational challenges. There were also many audit requirements that were not suitable f or Company X. The main challenge occurred to be the question, whether a whole security section of KATAKRI can be a p proved in an audit even though all of the requirements of the audit questions in that particular section are not met. As for the conclusions, it can be noted that the study was in its entirety useful for Company X. The company gained a fair view of the level of its audited operations and objects compared to the requirements of KATAKRI. Most of all the company gained knowledge and understanding of KATAKRI's compatibility for the company's requirements. With the study Company X is able to weigh the pros and cons of a real official KATAKRI standardization audit and to evaluate its usefulness for the company itself.

Rajamäki, J. (2014). Challenges to a smooth-running data security audits. Case: A Finnish national security auditing criteria KATAKRI. Proceedings of the 2014 Joint Intelligence and Security Informatics Conference.

Abstract: An information security management system (ISMS) provides controls to protect organizations' most fundamental asset, information. KATAKRI is a Finnish national security auditing criteria that is based on several ISMS standards and best practices. It was initially intended to be used by public sector to audit private sector service providers, but it has been adopted also as a baseline of requirements for private sector security standards. First, this paper explores the expectations for security auditing criteria, processes and auditors. The case study research (CSR) was conducted in the form of interviews (n=25), questionnaires (n=45) and observations. Second, a design science research (DSR) exploits the combined CSR results for designing a model for a well-run ISMS audit. The CSR results shows that the different goals of a security audit can be in conflict. The results also indicate that KATAKRI has defects due to its inconsistency. One task of auditing processes should be collecting information about shortcomings of applied criteria. This paper's new model for KATAKRI audits includes this activity.

7.2.2 Information security investment, incentives, and trade-offs

Many organizations see investments in security technologies as a mandatory cost, which does not increase productivity (Ahokangas et al., 2014). However, these investments should be seen as positive and critical for stakeholders, which e.g. raise their standings among competitors and customers. Laurea University of Applied Sciences is going to change the mentality towards information security among all stakeholders via, for example, developing education for leading auditors of KATAKRI. The first KATAKRI-leading auditor training program was designed by Merja Rajamäki's (2011) master's thesis (M. Rajamäki, 2011). A second study (J. Rajamäki & Rajamäki, 2013) was finalized after the first realization of the training program. Jääskeläinen (2014) continued with how Laurea's pedagogical strategic choice, Learning by Developing (LbD), can be made of good use (Jääskeläinen, 2014). Based on the above-mentioned studies, an improved model for KATAKRI audits was presented (J. Rajamäki, 2014a).

Rajamäki, M. (2011). Pätevyysmalli turva-auditointi-koulutukselle - tapaustutkimus Laurean Auditoinnin johtaminen –opintojaksosta (Developing a competence model for security auditor specialization studies Case study: Laurea's Management of Auditing study module). Theseus: Laurea (Master thesis). Available: http://www.theseus.fi/handle/10024/278/browse?value=Rajam%C3%A4ki%2C+Merja&type=author

Abstract: The national criteria for security auditing, KATAKRI, were published in No-vember 2009. One of KATAKRI's aims is to combine the actions of authorities when they are verifying the security level of a company or other corporation by carrying out security auditing. KATAKRI is also intended to help companies and corporations when they are developing their own security level.

There is a definite need to teach both the content of KATAKRI and security auditing, but no specific training has been arranged yet. The academic level, content and requirements of security auditing training have not yet been defined. The basic assumption behind any security auditing training course is that the authorities can trust the quality of the training and the expertise of those people who have undertaken it.

The purpose of this case study is to find out what is expected from a security auditor, what kind of competence the auditor should have, and how the security auditing training should be developed to correspond with the needs of the security field. The empirical research was conducted in the form of interviews and two questionnaires. The interviews were based on the new Management of Auditing study module description compiled by Laurea University of Applied Sciences, Leppävaara campus. Nine experts in the security and safety fields were interviewed about the content of the study module as well as other essential matters related to auditing. In addition, one questionnaire was circulated to postgraduate students at Laurea to find out whether they would be interested in that study module and their opinions on its content. A second questionnaire was delivered to the very first students at Laurea who had taken the Management of Auditing module to gather their feedback.

The combined results of the interviews, the questionnaires, and examination of the content of the existing Management of Auditing module showed that deep knowledge of the security field as well as the competence to manage the overall picture of security is required from security auditors. Furthermore, it was concluded that qualifications for security auditors should be created in accordance with ISO Standard 19011:2002 be-cause it provides such a good competence model.

In light of the above, it is recommended that the academic level, content and requirements of future audit and security auditing training should be clearly defined and the quality of the training should be standardized and certified. It would then be possible to plan and implement a security auditor specialization course. This course of study would be a natural module for Laurea to offer to students from different security branches who want to deepen their know-how of the overall security field by taking an optional specialization course which would count towards their Master's Degree.

Laurea is a prestigious and recognized trainer in the security field in Finland. There are no other universities or universities of applied sciences where it is possible to graduate with a Bachelor's or Master's Degree in Security Management. Therefore it would be the most suitable educational establishment to offer such specialized training.

Rajamäki, J. and Rajamäki, M. (2013). National Security Auditing Criteria, KATAKRI: Leading Auditor Training and Auditing Process. Proceedings of the 12th European Conference on Information Warfare and Security, 217–223.

Abstract: The National Security Auditing Criteria, KATAKRI, were published in 2009, revised in 2011, and version III is currently under revision. The root of KATAKRI is to preserve the confidentiality of any confidential and classified information held by the organisation concerned. One of KATAKRI's aims is to combine the actions of authorities when verifying the security level of a company or other corporation by carrying out security auditing. From the enterprise operators' point of view, the focus of security auditing is to eliminate unfair competition and maintain an equal opportunity field for operators. Another of KATAKRI's aims is to improve national security when Finnish Defence Forces or other security authorities apply subcontracting. KATAKRI is also intended to help companies and corporations when they are developing their own security level. The purpose of this case study is to find out: what is expected from the security auditing process and from the leading auditor; what kind of competence the auditor should have; and how the security auditing training and qualification should be developed to correspond with the needs of the security field. The empirical research was con-ducted in the form of interviews, questionnaires and observations made as a student during the first KATAKRI leading auditor course executed 2/2/2012–12/12/2012. The combined results showed that deep knowledge of the security field and competence to manage overall security is required from security auditors. Furthermore, it was concluded that qualifications for security auditors should be created in accordance with ISO Standard 19011:2011, which provides a very strong competence model. In light of the above, it is recommended that the academic level, content and requirements of future audit and security auditing training should be clearly defined, and the quality of the training should be standardised and certified. The results also indicate that KATAKRI version II still has defects due to its inconsistency. One task of auditing processes should be collecting information about KATAKRI's shortcomings, and they should be systematically analysed. Future leading auditor courses would be suitable scenes to an-alyse shortcomings and to propose improvements to KATAKRI. KATAKRI should be revised every second or third year.

Jääskeläinen, V. (2014). Monologista dialogiksi—Katakri-pääauditoijakoulutuksen kehittäminen (From monologue to dialogue —development of Katakri lead auditor training. Thesis. Theseus. Espoo: Laurea. Available: https://www.theseus.fi/handle/10024/77208

Abstract: The subject of the thesis project was Katakri (National Security Auditing Criteria) lead auditor training held in Laurea University of Applied Sciences. The purpose of this research-based development project was to create a research based education

model that contains key features of Learning by Developing. Learning by Developing is a pedagogical model used by Laurea University of Applied Sciences.

The research approach of the thesis project was qualitative. The empirical data was collected using three methods: learning café, wish list technique and mind map. The data was collected within a two-hour development session. The session was attended by Katakri lead auditor training teachers and teachers of the Security Management Degree Programme as well as other staff from Laurea University of Applied Sciences and Security Management students. During the session a number of attendees invented development proposals as individuals and in teams. The development ideas were related to key figures of Learning by Developing. The purpose behind combining the selected methods and participants was to gather a wide range of development proposals from different perspectives.

The gathered research material was interpreted using abductive reasoning, meaning that the subjective and collective proposals of the attendees were compared with the theoretical part of the thesis project. The conclusion chapter contains the new education model. The model is divided into two parts: learning events in which the teacher is present and remote exercises. The educational content is based on the National Security Auditing Criteria. The education model emphasizes team work, authentic audits, diverse student assessment, sharing of experiences and research-based reporting. The conclusion of the thesis project is intended to help develop the Katakri lead auditor training.

Rajamäki, J. (2015). Cyber Security Education as a Tool for Trust-building in Cross-Border Public Protection and Disaster Relief Operations. IEEE Global Engineering Education Conference [In review].

Abstract: Public protection and disaster relief (PPDR) operations are more and more dependent on networks and data processing infrastructure. Incidents such as natural hazards and organized crime do not respect national boundaries. As a consequence, there is an increased need for European collaboration and information sharing related to public safety communications (PSC) and information exchange technologies and procedures - and trust is the keyword here. According to most studies and interviews carried out within the Multi-Agency Cooperation in Cross-Border Operations (MACICO) project, the topic "trust-building" could be seen as the most important issue with regard to multi-agency cooperation. Cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world. It is important to complement the currently dominating "cyber security as a barrier" perspective by emphasizing the role of "cyber security as an enabler" of new business, interactions and services - and recognizing that trust is a positive driver for growth. Public safety infrastructure is becoming more and more dependent on unpredictable cyber risks. Everywhere present computing means that PPDR agencies do not know when they are using dependable devices or services and there are chain reactions of unpredictable risks. If cyber security risks are not made ready, PPDR agencies like all organizations will face severe disasters over time. Investing in systems that improve confidence and trust can significantly reduce costs and improve the speed of interaction. From this perspective, cyber security should be seen as a key enabler for the development and maintenance of trust in the digital world, and it has the following themes: security technology, situation awareness, security management and resiliency. Education is the main driver for complementing the currently dominating "cyber security as a barrier" perspective by emphasizing the role of "cyber security as an enabler".

7.3 Situation awareness

According to Ahokangas et al. (2014), cyber situation awareness is a key factor to prevent, identify, and protect from the cyber incidents, and if, for example, a cyber-attack happens, to recover from the attack. Pullinen (2012) develops a model for protecting critical systems. The model also includes an operational picture of the statuses of critical information systems (Pullinen, 2012).

Pullinen, M. (2012). Kriittisten tietojärjestelmien suojaaminen kyberuhilta (Protection of Critical Information Systems against Cyber Attacks). Theseus: Laurea. (Master's Thesis). Available: http://www.theseus.fi/bitstream/handle/10024/46341/Pullinen_Mika.pdf?sequence=1

Abstract: Critical infrastructure is nowadays more and more dependent on information systems. This thesis introduces cyber-attacks which have had impact on critical information systems around the world. By describing Finnish legislation and key actors on the field of information security, one can make conclusions about Finnish national capabilities to defend our critical Information systems. Cyber warfare capabilities of some nations which are strongly investing in the cyber domain, are also shortly described. Most common attack and defence methods are introduced along with those methods that can especially pose a threat to critical information systems.

Recommendations to improve protection of critical systems are created based on the work done during composition of the thesis. The recommendations include the necessity to define which systems are critical. Furthermore, creating information security auditing criteria focusing on critical systems is suggested. The criteria should not only be based on the security classification of the data processed on the system. The effects that system malfunction or interruption of services would cause should be also considered. Design Science is used as a research approach in the thesis.

Design science is used for creating something new. The thesis introduces a model that can be used as an extra tool to protect critical systems. A new artefact is created based on Hevner's seven guidelines. The model can be developed further to an application. Model includes a threat analysis of state and nonstate actors. The model also includes an operational picture of the statuses of critical information systems.

Information Security of national Critical Information Systems can be significantly improved with this new defence model. The thesis highlights the growing meaning of in-formation warfare alongside traditional warfare.

7.4 Resiliency

"Resiliency is about adapting to changing conditions, in the case of information security, based on run-time situation awareness and a priori risk analysis. The resiliency of critical infrastructures such as communication networks, energy production and distribution and industrial plants is vital to the society. Without proper protection and development with cyber security in mind, the modern society relying on these infrastructures would be extremely vulnerable to accidental and malicious cyber threats (Ahokangas et al., 2014)."

The RIESCA project started Laurea's research with regard to resilience of cyber-physical system (CPS) that are critical to the day-to-day functioning of any techno-logically advanced society. Some of these CPSs are wide, critical infrastructures, sprawled across different countries, such as power-distribution networks, requiring cyber-secure, cross-border telemetric connections. Other CPSs, such as urban-built infrastructures, have several simultaneous stakeholders whose cooperation is critical. This requires interoperable systems/services for communications and secure services.

Rajamäki, Ahokas, and Rathod (2013) applied solutions from MACICO into the field of power distribution by studying Distributed Systems intercommunication Protocol (DSiP) for combining multiple telecommunication channels in Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are used for controlling the power stations and protecting power distribution. Therefore, secure data transfer between control center and power stations is critical. Current telecommunication networks used for the SCADA do not provide the required capacity for real-time video streaming, and a standard Internet connection does not provide the required reliability and security. DSiP combines all these telecommunications resources into a single system (J. Rajamäki, Ahokas, & Rathod, 2013).

Rajamäki, J., Ahokas, J., & Rathod, P. (2013). A redundant communications solution for critical infrastructure protection and SCADA systems. Interna-tional Journal of Communications, 1(1), 109-11.

Abstract: Securing an electricity distribution network is equally crucial to securing other critical infrastructure (CI) components. Many critical infrastructure components are operating and controlling by Supervisory Control and Data Acquisition (SCADA) systems. Very SCADA system is also controlling the power network. In the modern infrastructure, these SCADA controlled systems are connecting to standard corporate networks for various reasons. Critical infrastructure and SCADA systems require higher resilient communication channels compared to the corporate network. This infrastructure and the system also demand equally high level of security along with a corporate network. Organizations must use standard base network as a part of solution in order to have resilient communications networks. These combined networks such as TETRA, 3G, LTE, ADSL and satellite have varied level of bandwidth and built-in security features. Recently the additional feature such as a live video stream transported on the critical infrastructure and SCADA networks. These data are transporting in the same logical communications channels without disturbing the SCADA command traffic. This paper aims to propose a new model to combine these networks to produce a highly resilient and secure communications network. The proposed communication system is built-on the Distributed Systems intercommunication Protocol (DSiP) that combines the contradicting requirements to a uniform and easily maintained system. The same requirements apply to 'Multi-Agency Cooperation in Cross-border Operations (MACICO)' project, part of an International Celtic Plus project. The proposed DSiP system is reusable for various needs and is adaptable to future network technologies.

Rajamäki, Rathod, Ahlgren, Aho, Takari, and Ahlgren (2012) discourse on the resili-ence of cyber-physical systems (CPS). Their study addresses technical security solutions for safe school environments (J. Rajamäki et al., 2012). Aho and Rajamäki (2013) continue the theme applying the results and lessons learned from the Security and Safety in the Universities project (cf. (Kreus et al., 2010), executed during 2009-2010. Interoperability between different actors plays a key role when keeping the school environment safe (Aho & Rajamäki, 2013).

Rajamäki, J., Rathod, P., Ahlgren, A., Aho, J., Takari, M., & Ahlgren, S. (2012). Resilience of cyber-physical system: A case study of safe school environment. Intelligence and Security Informatics Conference (EISIC), 2012 European, 285-285. doi:10.1109/EISIC.2012.10

Extended abstract: Modern critical infrastructure includes a combination of computational and physical components, known as a cyber-physical system (CPSs). Often, urban-built infrastructures represent a critical node within the intertwined networks of an urban area. Current school environments are examples of CPSs, including automatic access controls (AACs), guidance and alarm systems (GASs), digital clocks, heat and motion identification sensors, and remolding spaces such as classrooms. A safe school environment can be created using parallel methods, such as preventive, proactive, and readiness for reactive resilience. This paper focuses on needs for improved understanding of school security solutions, mainly covering readiness for reactive methods of security.

AAC tags can be identification cards, wristbands, necklaces, and others. The person who has a tag can be identified. These persons can be teachers, staff, students, or someone who need access. This solution allows access into building facilities to only identified, authorized people. Students can move around without tags during the day in the public area that is not locked, like most of the classrooms, or they have identification cards to get access to labs and other facilities. Children in the daycare wear a special wristband that helps identifying them, enhancing cost savings with automating routine operations. The heat and air conditioning systems can automatically set a correct working level when the system identifies a number of people in the building. AAC is linked to video surveillance, working in public areas and entrances. Video surveillance is used for two purposes: 1) in crisis situations, recordings can be explored and handed over to the police, and 2) to count the number of people in the variable areas. Normally, classes are not monitored, as teachers have control over accessing student spaces. However, there can be a provision of class monitoring for major events or bigger classes. During off-hours, all the safety measures are active, and all persons should have their identification cards, and all movements in the school will be registered in the system. Doors cannot be opened when the video surveillance system detects more than one person tries to enter in an 'only one person' at a time entrance. Analyzing software counts the number of people that enter or leave the area. The camera must be positioned almost perpendicular on top of the doorway. Another option is to install thermal cameras in every room, to count the exact number of people in a room. This technology does not reveal the identity of people in the room, so nobody's privacy will be compromised. The school has heat and movement sensors installed in every room's roof structures. Sensors can identify the number of people in every room. Digital clocks being used for dual capabilities exist in all rooms. In a normal situation, they display time, but within problematic situations they show the alarm code. Alarms can be set automatically or manually. A manual setting has an additional feature of identifying problematic spaces. The alarm shows various codes for alerting people to hide or leave the room, also alerts about required help in the space. The alarm is displayed in all spaces, classrooms, and corridors of the problem situation. The alarm system can be monitored and controlled from the safety room and from each teacher's desk, using a touch-screen computer. The system can also be used by the specific application that is installed to a laptop computer and mobile phones. The software will be planned as simple and user friendly. Security aspects must be taken into account when designing the software.

In threat situations, communication software and services are attached with high im-portance. There cannot be gaps in communication between people inside the school and the authorities outside of the school.

Aho, J., & Rajamäki, J. (2013). How to improve safety of school environment: A case study of safe school in Finland. Urban Planning and Design Research, Vol. 1(Iss.21), 19-24. Urban Planning and Design Research, 1(21), 19-24. Available: http://www.seipub.org/updr/Download.aspx?ID=3772

Abstract: The school infrastructures closely intertwined in critical node of networks in urban area. Modern critical-system infrastructure includes combination of computational and physical components, known as cyber-physical system (CPS). However, a comprehensive approach to develop resilience concept for a combination of such systems, as they are often designed in modern urban areas, has not yet been approached thoroughly. The aim of this paper is to provide an improved understanding of a safe school environment as well as to pose cost effective and transparent school security systems. The paper is based on the results and lessons learned from the "Security and Safety in Universities" project executed during 2009-2010 and the results will be applied within a building process of a new school campus in Finland. Based on the results of our case study, it is proposed that a safe school environment should consist of two important components of cyber-physical security: (1) technical control and timely notification of emergency situations and (2) a safety room. The first component includes: access control, camera surveillance, sensor monitoring, technical guidance to the exit and informing. Safety room is designed to monitor the safety and emergency management and information technology.

7.5 Future research and development needs

PPDR agencies' present-day digital systems do not support cross-border cooperation. In addition to technical challenges, the distrust between agencies (especially in the field of law enforcement and crime investigation) causes trouble. Unfortunately, this distrust also exists at the national level, and even between units of one organization. However,

common digital systems and operational procedures could increase the trust between parties. The European Network of Law Enforcement Technology Services (ENLETS) was established as a sub-group of the Law Enforcement Working Party of the EU Council in 2008. ENLETS' vision is to be the leading European platform that strengthens police cooperation and bridges the gap between the users and providers of law enforcement technology. The core group members of ENLETS (The Netherlands, The United Kingdom, Finland, Belgium, Poland, and the prevailing EU's presidency country) should develop common procedures to apply new law enforcement technology. In the future, these procedures could be extended to other European countries as well as other fields of PPDR.

As Ahokangas et al. (2014) say, a very important change is needed, where the mental picture of cyber security should be changed from "threat, crime, attack" into "trust". In Finland, KATAKRI should be redeveloped towards a tool that encourages and simplifies sharing of mission-critical data between PPDR actors.

References

Aho, J., & Rajamäki, J. (2013). How to improve safety of school environment: A case study of safe school in Finland. *Urban Planning and Design Research*, Vol. 1(Iss.21), 19-24.

Ahokangas, M., Arkko, V., Aura, T., Erkinheimo, P., Evesti, A., Frantti, T., . . . Vepsäläinen, P. (2014). *Strategic research agenda for cyber trust*, DIGILE.

Akhgar, B., Fortune, D., Hayes, R. E., Guerra, B., & Manso, M. (2013). Social media in crisis events: Open networks and collaboration supporting disaster response and recovery. *Technologies for Homeland Security (HST)*, 2013 IEEE International Conference On, 760-765. doi:10.1109/THS.2013.6699099

DIGILE. (2014). In the pipeline: Cyber trust. Retrieved from http://www.digile.fi/Services/researchprograms/cybertrust

Jääskeläinen, V. (2014). Monologista dialogiksi—Katakri-pääauditoijakoulutuksen kehittäminen.

Kantarci, B., & Mouftah, H. T. (2014). Trustworthy sensing for public safety in cloud-centric internet of things. *Internet of Things Journal, IEEE*, 1(4), 360-368. doi:10.1109/JIOT.2014.2337886

Kimiläinen, M. (2011). Yritys X: N henkilöstöturvallisuuden ja fyysisen turvallisuuden esiauditointi kansallisella turvallisuusauditointikriteeristöllä.

Kojo, J. (2013). Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla.

Kreus, J., Pelkonen, N., Ranta, T., Turunen, T., Viitanen, J., & Vuoripuro, J. (2010). *Korkeakoulun turvallisuuskäsikirja – vakavien henkilöriskien hallinta.* Helsinki: Edita Prima Oy.

Laitinen, O. (2013). Yrityksen turvallisuuspolitiikan laatiminen.

Mannermaa, M. (2008). *Jokuveli: Elämä ja vaikuttaminen ubiikkiyhteiskunnassa.* WSOYpro.

Martiskainen, M. (2012). Sisäinen turvallisuusauditointi aikuiskoulutusoppilaitoksessa.

Nouri, M., Lottici, V., Reggiannini, R., Ball, D., & Rayne, M. (2006). TEDS: A high speed digital mobile communication air interface for professional users. *Vehicular Technology Magazine, IEEE*, 1(4), 32-42. doi:10.1109/MVT.2006.343629
O'Leary, M., Orlikowski, W., & Yates, J. (2002). Distributed work over the centuries: Trust and control in the hudson's bay company, 1670–1826. *Distributed Work*, , 27-54.

Pullinen, M. (2012). Kriittisten tietojärjestelmien suojaaminen kyberuhilta.

Rajamäki, J. (2012). Redundant multichannel public safety communications network for public protection and disaster relief (PPDR) organizations. *3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE'12).*

Rajamäki, J. (2014a). Challenges to a smooth-running data security audits. case: A finnish national security auditing criteria KATAKRI. *Proceedings of the 2014 European Intelligence and Security Informatics Conference.*

Rajamäki, J. (2014b). Information security policy development and implementation piggybacking onto finnish national security auditing criteria KATAKRI. *The 5th European Conference of Computer Science.*

Rajamäki, J. (2014c). The MOBI project: Common mobile digital services for all pub-lic protection and disaster relief (PPDR) vehicles. In J. Music (Ed.), *Recent advances in computer engineering, communications and information technology* (pp. 120-125) WSEAS Press.

Rajamäki, J. (2014d). Plenary lecture 3. multi-agency cooperation in cross-border op-erations. *8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14)*.

Rajamäki, J. (2014e). Studies of satellite-based tracking systems for improving law enforcement: Comprising investigation data, digital evidence and monitoring of legality.

Rajamäki, J., Ahokas, J., & Rathod, P. (2013). A redundant communications solution for critical infrastructure protection and SCADA systems. *International Journal of Communications*, Vol. 1(No 1), 109-117.

Rajamäki, J., Knuuttila, J., Suni, O., Silanen, H., Tuomola, A., & Meros, P. (2014). How to empower policemen and their vehicles: A multiple case study analysis of seven public safety related ICT projects. *International Journal of Systems Applications, Engineering & Development*, 8, 238-249.

Rajamäki, J., & Rajamäki, M. (2013). National security auditing criteria, KATAKRI: Leading auditor training and auditing process. *Proceedings of the 12th European Conference on Information Warfare and Security*, 1, 217-223.

Rajamäki, J., & Rathod, P. (2014). How standardized utility cloud services and ser-vice-oriented architecture benefits in public protection and disaster relief ? *International Journal of Computers and Communications*, 8, 86-93.

Rajamäki, M. (2011). Pätevyysmalli turva-auditointikoulutukselle:-Tapaustutkimus Laurean auditoinnin johtaminen-opintojaksosta.

Rajamäki, J., Rathod, P., Ahlgren, A., Aho, J., Takari, M., & Ahlgren, S. (2012). Resilience of cyber-physical system: A case study of safe school environment. *Intelligence and Security Informatics Conference (EISIC)*, 2012 European, 285-285. doi:10.1109/EISIC.2012.10

Riku Leppänen & Pasi Kämppi

8. AUTHENTIC EVALUATIONS, CASE: VIKSU 2014

The security domain is demanding skilled employees that are able to work in both operational and technological working environments. Employees have to also work more and more directly with end users, and they have to be able to improve existing operating procedures. Laurea´s pedagogical model, Learning by Development, is the educational answer for this challenge. Learning by Development allows students, lecturers, researchers, end users, and industrial partners to work together in an authentic learning environment. In the MACICO project Laurea's pedagogical approach was carried out ideally in Viksu's 2014 Young Firefighters' Camp during the summer of 2014. The students created a virtual disaster scenario, where they evaluated how the camp organization handled the crisis situation and how technological solutions supported operational procedures.

Chapter 8.1 gives an overview of the Viksu 2014 camp. Chapter 8.2 describes the evaluation of Viksu 2014 camp's operational procedures. Then, chapter 8.3 focuses on the MACICO project-related technologies and future research topics which arise from the demonstrations.

8.1 VIKSU 2014

Laurea University of Applied Sciences and its partners, Airbus Defence and Space Finland, Ajeco Ltd., and Eye Solutions Ltd., have demonstrated and studied the TETRA network and other communication actions. The demonstrations were held at the Viksu 2014 Young Firefighters' Camp in Pori, Finland. The main objective was to conduct research which benefits the MACICO project and participating organizations. Viksu 2014 is an international firefighters' camp held once every four years. The camp is dedicated especially for young voluntary firefighters and had over 3000 attendees, gathering people from different voluntary fire brigades around the world.

The overall MACICO project's objective at the Viksu 2014 camp was to test and research various communications-related methods provided by the partner organizations. Research was done in the form of demonstrations made by Laurea's students as thesis subjects and scientific publications from the 28th of June to the 2nd of July 2014.

Airbus Defence and Space Finland provided the camp with a portable TETRA network and 40 TETRA radios in order to support the daily activities. The TETRA network, its functions, and operability with the camp organization was observed and tested during a major disaster rehearsal. The disaster rehearsal was based on an imaginary downpour hitting the camp's training area, resulting in a multi-casualty emergency situation.

8.2 Evaluation of operational procedures

The disaster rehearsal was planned and executed by Laurea's Security Management student Harri Aaltonen. Aaltonen analyzed the effectiveness of the camp organization's communication. The TETRA network communication assessment was carried out and network channels were recorded. In the field, observers made notices of, for example, communication

behavior and discipline. The network's capabilities were claimed to be sufficient for regular camp use. In demanding situations, the capabilities were not enough with the current amount of TETRA training and skills of the camp organization. The MACICO project gained valuable information of the TETRA network action and functionality in a temporary organization environment, which changes and acts once every four years. Picture 8-1 illustrates a part of the actions and technologies used in the rehearsal.

Picture 8-1. Natural disaster rehearsal (Photo: Tapio Mäkinen)

Aaltonen, H. (2014). Simulated natural disaster in Viksu 2014 Young Firefighters' Camp.

Extended abstract: The objective of this study was to develop a multi-disciplinary cooperation model for organization in the case of a major disaster. The study was part of the MACICO project. The following research question was posed: How should organization be coordinated in a major disaster? The Viksu 2014 organization was interested in testing its crisis management capabilities in extreme conditions after their last update of a rescue plan. The simulated disaster was planned to be more or less like the one which hit the Sonisphere rock concert, organized in Pori, Finland, in 2010.

The methods used in the study were observation, interviews, and document analysis. The monitoring was arranged by the observers who carried recorders and took notes during the simulation. The radio communications were recorded via two TETRA radios. The interviews were carried out after the simulation on how it succeeded by their standards, and what could have been done otherwise. The observed and interviewed people were either managers or per-sonnel from the security sector. The simulated disaster was compared to the emergency and crisis communication plans.

The observation of simulation referred that most of the problems were related to communication. In the most urgent moments, the capacity of the TETRA network was not enough. The middle managers, in some cases, had more calls than they could answer. In most cases, the calls were either missed or the answering times delayed. As a consequence, the calls were made with too vast distribution in many cases. The recordings of the radio communication showed that there were problems in radio discipline, which might have had an influence on the network capacity.

The observation of simulation revealed that there were managing models that apparently were planned but had not been written down in the plans. One of these models was an order from the head of the camp organization to make changes in organizational hierarchy during the crisis. The records also showed that the current emergency and crisis communication plans were too independent. All of the plans would have worked out alone, but in a multi-organizational situation, one plan did not take any other plan into account.

The first conclusion was that the communications needed adjustment in a crisis situation. The training of radio communications for personnel is the first suggestion. The duties of middle management need to be determined to correlate with resources. As a solution, the middle management needs to be released from the radio to focus on leading and maintaining the situational awareness. The second conclusion was that the distribution of situation awareness needed a better protocol. Changes in situation did not reach the management as soon as it was possible. The third conclusion is that silent information of crisis management models must be transferred to plans.

This study only took into account Viksu's cooperation models without authorities. The next step would be to take into account other organizations. A further step would be to study the importance of volunteers as assistants of authorities in the near future. The decreasing number of authorities' resources has an impact to such studies.

Live demonstrations also included a multi-casualty simulation exercise, which was incorporated into the major disaster rehearsal. In the exercise, 25 campers were given specific injury descriptions, which were developed by students Taneli Assinen and Janne Kemppainen from Laureas' Programme in Nursing. The exercise focused on studying multi-casualty situation management in rescue and medical service situations. Primary TRIAGE (ABCDE approach aiming to determine the priorities of patient treatment, picture 8-2) evaluation was conducted by the camp's emergency medical services.

Picture 8-2. Natural disaster rehearsal (Photo: Tapio Mäkinen)

Assinen, T., Kemppainen J. (2014). Emergency medical service actions in simulated multi-casualty situation. Case: Viksu 2014.

Extended abstract: The subject of this study was the medical emergency services actions in a multi-casualty situation. The study was part of a natural disaster rehearsal, performed in Viksu 2014 Young Firefighters' Camp on June 30th at Kirjurinluoto, Pori, Finland. The study focused on multi-casualty situation management and primary triage. The study's objective was to find out how the emergency medical service manages a mass casualty situation compared to their multi-casualty event protocol, and to observe the implementation of primary triage algorithms.

Theoretical framework was based on current domestic and international academic material. For creation and evaluation purposes, it was crucial to build strong knowledge in triage algorithms and evidence-based practices in multi-casualty event management. In order to create realistic trauma descriptions, knowledge in traumatology was also needed. In addition to substance sources, study was based on qualitative research methodology. The empirical data was collected from recorded radio communication interviews at the camp from emergency medical staff and by observers. In the interviews, the emergency medical personnel that participated in the simulation were asked to describe their role in the simulation and how the simulation progressed by their standards. The observation focused on two aspects: observation of the triage unit leader and triage personnel and observation of coordination and control of the triage area.

Twenty-five patients with varying trauma descriptions formed the script for the simulation that day. Patients were placed in an open-ground area full of large tents. The area was limited to consist of 16 tents and patients were placed both in- and outside of the tents. Each patient had a trauma description card which included information in accordance with the ABCDE-approach. The simulation started with information about one patient with an open head wound. The full scale of the situation was revealed after the first emergency medical unit arrived on the scene.

The outcome was mainly successful for the emergency medical service; primary triage was completed fairly quickly, and patients with minor trauma were cleared from the scene. The observation reports and interviews showed that there were problems with communication between triage units and fire department units. Because of communication problems, the search of the area was not conducted in the most organized way. Evaluation of the implementation of the triage algorithms proved to be challenging. Implementations of three of the five main criteria in primary were observed: ability to walk, palpation of radial pulse, and evaluation of the level of consciousness. Because of the nature of the situation, the implementation of the other two main criteria (checking/opening airways and counting respiratory rate) were not evaluated.

In addition to the natural disaster, other live demonstrations were executed in the camp environment. Samu Iiskola, a student from Laurea's Security Management Program, focused on observing human-made disturbances and accidents. Iiskola performed an assessment of the internal communication of the camp during basic activities of a regular camp week.

Iiskola, S. (2014). Can Viksu 2014 Young Firefighters' Camp's present security and preparedness plans respond to accidents and disturbances caused by people?

Extended abstract: This thesis was part of the MACICO project, at the Viksu 2014 camp which covered different areas in the camp. The main focus point of the project was in communication. The objective of the thesis was to find out how well the camp organization had prepared resources and plans for possible threat situations, and how well those plans could be executed. The threats included were all accidents or disturbances caused by human factors. The thesis question left out natural disasters. The first objective of the thesis was to security audit the camp. The second objective was to see how well information was shared with different camp units and how that could be developed.

The thesis inspected the camps security and rescue plans and other written instructions for the employees and the campers themselves. Observations were to determine if the security theories meet with the week-long practical camp life. Observations, photographs, and interviews collected during the camp were used to form a basis on how well the preparedness and communication was in hand, especially how well employees, other than camp leaders and security personnel – first-aid workers, camp fire department, and security officers - knew about camp safety.

There was also an active part of the thesis during the camp which was a scenario for stealing money from a camp kiosk. The theory used in the scenario is from IT-threats called "social engineering". The subject uses public knowledge gained from webpages, observations of the organization, and what the subject wants the employees to see in order to get to the object. This scenario did not use brute force or tools to achieve the goal, but only talking. The scenario gave information about how employees outside of the security field handled unexpected situations and how they shared information.

The scenario brought up developing points in money handling and information sharing. The employees believed the subject's initial story, but they didn't give the money after phoning their supervisor, and they didn't inform the security officers. Other scenarios – a group fight, major food poisoning, and fire - were planned but not implemented. They could not be organized safely within the camp area, even if simulated, as they would have required much resource and real-like situations for authentic reactions. These scenarios wouldn't have brought more information to this thesis as they would have concerned the security units, and their work was documented in Harri Aaltonen's thesis.

The first conclusion of the thesis is that, as a whole, the Viksu 2014 organization has prepared well for different kinds of threats. Second, more focus would be needed in communication and how well security planning is incorporated into reality. The preparedness plans were well written and distributed amongst the different camp units, but most employees hadn't read it thoroughly beyond the security personnel and camp leaders. Third, it's difficult to monitor all 3000+ campers in such a huge area, so an outsider could easily get inside the camp. Fourth, a nearby town brought curious teens and other more down-trodden people looking for something to take. The tent area should be supervised more efficiently during the day and extra attention given to perimeter security at the nighttime. Fifth, different unit leaders communicated well with each other, but this should also be incorporated to the employees.

To develop the camp security, there should be more communication within each unit. If other units observe an outsider, they should inform the security officers quickly. A thorough information meeting before the camp starts, within each unit, is necessary for all the employees to know what is required of them beyond just doing their own job. The thesis has made a quick info-package for camp security officers to remind them of what is expected from them and how the camp security differs from normal security situations. Other packages were made for employees handling money and how they should be prepared.

Camp security could be researched further by using more scenarios in the next camp. Observations could be made on how theft sightings are informed to the security officers. Information could be gathered from a multiple threat situation. For example, first a theft scenario in which subjects try to fill a nearby car before anyone notices them. A second threat could be where thieves set a fire, so they can steal amidst the chaos and escape more easily. A security survey could be given among the employees and campers alike to gain knowledge on how they observe security and safety in the camp.

8.3 Evaluation of next generation situational awareness system

Two Finnish high-end technology companies, Ajeco Ltd. and Eye Solutions Ltd, provided a situational awareness system for Viksu 2014. The companies have created a unique solution that combines robust telecommunications platform with real-time situational monitoring. The students of Laurea evaluated how the integrated solution supported camp personnel crisis situation management procedures.

The solution is based on Ajeco's telecommunications platform that integrates 2G, 3G, 4G, and satellite capabilities. Various data bearers are combined to ensure the continuous and high security information flow between a command center and field operation units. Eye Solutions provides a situational awareness system that integrates real-time information distribution with communication services. The

system contains real-time video streaming, group communication with voice and text messaging, and location services. The command center and one field operation unit was built by Ajeco and Laurea, using Ajeco's and Eye Solutions' high-end technology. The technical architecture is presented in figure 8-3.

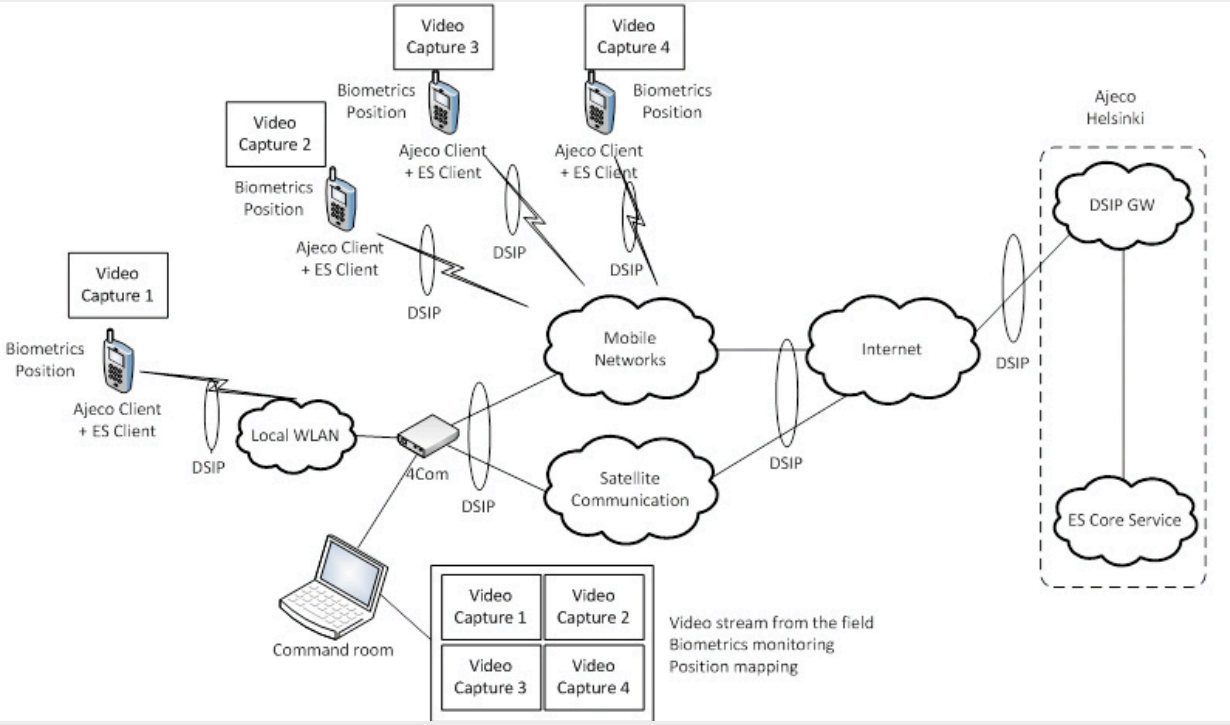
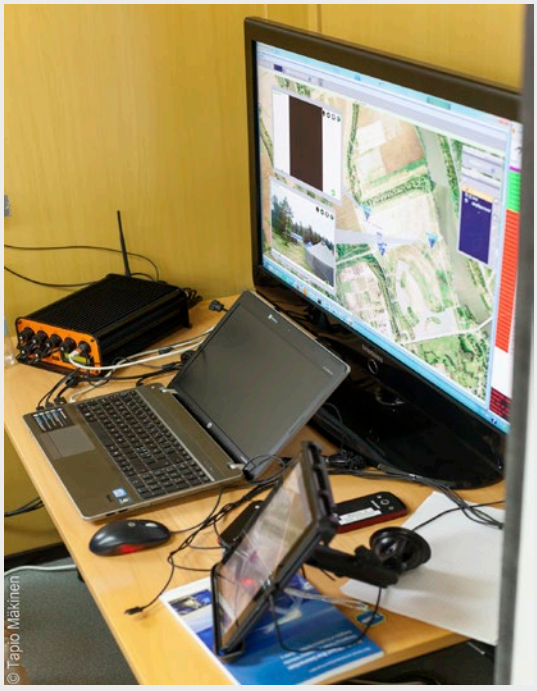


Figure 8-3. Technical architecture



Picture 8-4. Command center (Photo: Tapio Mäkinen)

Two of Laurea's students studied Eye Solutions' system in order to evaluate its usefulness as a communication tool for the camp organization. The objective for the MACICO project was to test and evaluate Ajeco's solutions through the observation of Eye Solutions' system and its functionality. Viktor Harvio from Laurea's Security Management Program participated in the Viksu camp to research the possibilities of the situational awareness system in rescue operations.

Harvio, V. (2014). Use of real-time video in rescue operations – Current state and future prospect.

Extended abstract: The main purpose of this bachelor's thesis is to explore how real-time video from a ground perspective is currently utilized in rescue operations. The object is to investigate the added value that real-time video brings into rescue operations and how to utilize it. As video quality, package compression, and encryption technology are constantly develop-ing, these also provide possibilities for field commanding and situation awareness. A review of earlier studies in this field reveals that research of the subject has previously focused mainly on army and police operations. New technology provided for real-time video use may facilitate field commanding by giving it tools to increase situational awareness and consequently improve rescue operations.

The first research question aims to clarify what kind of value real-time video adds to the situation awareness in rescue operations. The second question addresses the manners and situation it can be utilized in. A third object is to find issues that should be improved for further development of real-time video systems for rescue operations. The study focuses in the per-spective of rescue services where a research gap lies in. It is narrowed to only cover video use from a ground perspective, thus excluding aerial surveillance.
The study is conducted as a case study, in which qualitative methods are applied: a literature review, a scenario, and interviewing. Interviews include professionals of different fields: fire fighters, paramedics, community service officers, and other experts in the field of safety. As for the empiric part, a small-scale field test was performed alongside the Viksu 2014 Young Firefighters Camp, in which a real-time video, utilizing a situation awareness application, was tested as a tool for the event security and safety sector. The real-time video software was provided by Eye Solutions.

The preliminary study results indicate that there is potential for wider utilization of real-time video in situational commanding among rescue operations, as they may provide a different type of an angle to the formation of awareness. However, additional technical instruments can create an additional risk as they can fail. Added information can also create an overflow of information if badly managed. Yet to come is more expert interviews and compiling of theory. The study is scheduled to be ready in December 2014. Further empiric research, testing, and development of similar systems, in terms of i.e. scenario-testing, add-on equipment and data terminal equipment, is suggested

Jussi Simola from Laurea's Master of Business Administration in Information Systems program also participated in the camp to gain more insight for his article regarding the MACICO project's partners' unique communication solution. The focus was to research how real-time video would benefit the management of public protection and disaster relief resources. The research results were submitted to a scientific conference.

Simola, J. & Rajamäki, J. (2014). Using a Real-time Video to Allocate Public Protection and Disaster Relief Resources in Rescue Service Process. Case: Natural Disaster in the Viksu 2014 Young Firefighters Camp. 5th European Conference on Computer Science.

Extended abstract: The objective of this study was to research the advantages of real-time video in a simulated natural disaster. A simulation of a natural disaster was held in the Viksu 2014 Young Firefighters' Camp as part of the international MACICO project. A high-security communication platform, developed by Ajeco Ltd. and Eye Solution Ltd.'s, situational awareness -software for smartphones and C2-systems formed a unique command center. Functioning of the center was tested in connection with the exercise.

The material of this study was gathered by interviews, on-field observations, and a literature review. Also, the researcher had interaction and discussions with the rescue workers throughout the exercise.

Samsung Xcover-2 android-smartphones were installed onto the rescue workers' uniforms. One smartphone was installed on a fire truck. During the exercise, there were one to three observers overlooking the information flow in the command center. Operations were recorded and analyzed. Preliminary results of the rehearsal show that a smartphone that has been in-stalled in a PPDR (Public Protection and Disaster Relief) vehicle needs remote control from the command center. The overall picture is dependent on where the PPDR vehicle is placed at the scene of the accident. The rehearsal also revealed that a view from above would help the commanding personnel notice rescue workers' movements and detailed objects from a wider area.

The results of the study indicate that watching real-time video ties people down, and they cannot participate in operational action at the same time. A command center requires more than one person to manage situational information flow. Responders are usually carrying their own smartphones on the field. Used solutions enable PPDR officials and partners to install and deploy applications easily. Applications might allow first responders to use their own smartphones for emergency communications in situations where communication with a primary network becomes difficult. Decision makers must establish priorities for response in large-scale disasters when the total demand for rescue services is greater than

the PPDR or-ganization´s capacity to respond. Delivered real-time video allows a command center to allocate resources in the right proportion.

The study can be summarized so that the studied technology is essential for authorities in the future. Having the right piece of information at the right time can literally save lives, money, and resources. Real-time situational awareness solutions should be integrated for different PPDR actors work during accidents.
The event showed that it would be important to investigate if real-time situational awareness solution with Micro Air Vehicles (MAV) affects the overall pictures view between authorities in the future. Remotely piloted or programmed MAVs with cameras could bring advantages for emergency and rescue services. PPDR actors could use MAVs to record an aerial view of a natural disaster. Information about filmed or photographed locations would be sent in real-time to the command center. Decision makers in command centers need a greater situational awareness picture to allocate resources more efficiently.

After the Viksu 2014 camp was over, a demand to research the usability of real-time information more exclusively was brought up by Laurea's representatives and partner organization. Riku Leppänen, Laurea's Security Management student and intern for the MACICO project began to develop a thesis regarding the usefulness of a real-time situational operation view for field operation leading. The key focus of the study is to research what type of situational information is beneficial for rescue service authorities. The thesis is completed in cooperation with Laurea, the Emergency Services College, Eye Solution Ltd., and Ajeco Ltd.

Leppänen, R. (2014). Evaluation of situational operation view for field operation leading.

Extended abstract: After the MACICO project's demonstrations in the Viksu 2014 camp, a demand was brought up by Laurea's representatives and partner organizations to continue researching the Eye Solution Ltd's. situational awareness system. After the summer of 2014, cooperation with Eye Solution Ltd. and Ajeco Ltd. continued, and was commenced with the Rescue Service College Finland. All partners expressed interest and need for research in the field of real-time situational operation view.

The thesis focuses on evaluating the types of information that are useful for the authorities in rescue service situations. The main objective of the study is to identify and research rescue service use cases where situational operation view can be applied. The preliminary chosen use cases are a wildfire and a dangerous chemicals accident. Use cases are studied and different types of functions for situational awareness information are identified. The functions are cross referenced with all identified use cases and similarities are analyzed. Ultimately, one of the use cases is chosen for verification. Verification is executed as live demonstration on the Rescue Service College's premises in Kuopio, Finland, at the beginning of the year 2015.

The knowledge base for the thesis is built up by doing a literature review and by having user-centric theme interviews with experts associated closely with the areas of chosen use cases. The use case which is chosen for verification is selected in cooperation with the partner organizations. During the verification event, observation is the main method used in the field and in a command center to gain research material. A group interview is conducted after the demonstration to collect information that wasn't realized during the event.

Information received from the demonstration is used to create an overview describing which parts of situational operation view are justifiably beneficial for rescue operations' field leading. The study is to evaluate the usefulness of real-time situational operation view and to provide a basis for analyzing the subject. The research results will provide the partner organizations with valuable information of the possible business opportunities regarding situational awareness information services in the rescue operations branch.

The premeditated effect of the study is to provide a basis for research in a field which is a subject for the future and hasn't been researched a great deal in the past. Assuming the study finishes as expected, it will generate new research subjects for both participating universities for future use. In case many new research topics are discovered, the participating universities can even gather suitable people to apply for a research project.

The study is scheduled to be completed in spring 2015. ■

References

Aaltonen, H. (2014). *Simulated natural disaster in Viksu 2014 Young Firefighters' Camp*. Unpublished manuscript.

Assinen T., Kemppainen J. (2014). *Emergency medical service actions in simulated multi-casualty situation*. Case: Viksu 2014. Unpublished manuscript.

Harvio, V. (2014). *Use of real-time video in rescue operations – Current state and future prospect*. Unpublished manuscript.

Iiskola, S. (2014).*Can Viksu 2014 Young Firefighters' Camp's present security and prepar-edness plans respond to accidents and disturbances caused by people?* Unpublished manuscript.

Leppänen, R. (2014). *Evaluation of situational operation view for field operation leading*. Unpublished manuscript.

Simola, J. (2014). *Using a real-time video to allocate public protection and disaster relief resources in rescue service process – Natural disaster in Viksu 2014 Young Firefighters' camp*. Unpublished manuscript.

Simola, J. & Rajamäki, J. (2014). Using a Real-time Video to Allocate Public Protection and Disaster Relief Resources in Rescue Service Process. Case: Natural Disaster in the Viksu 2014 Young Firefighters Camp. *5th European Conference on Computer Science*.

Jyri Rajamäki, Tapio Savunen, Heikki Riippa & Juha Knuuttila

9. DISCUSSION

This chapter consists of four subjects. First, Jyri Rajamäki, from Laurea, assesses the success of the MACICO project from a research organization's point of view. Then, Tapio Savunen, from Airbus Defence and Space, discusses the business models with regard to public safety cross-border communications. Heikki Riippa, from the National Police Board, expresses the future research needs from a public protection and disaster relief actor's point of view. Finally, Juha Knuuttila, from Laurea, discusses the possibilities of widening the customer base for PPDR communications, taking into account the societal changes from public to private in securing our communities and public places.

9.1 Success of the MACICO project

Jyri Rajamäki

To pursuit criminals across a border is a difficult task today, because the intervention teams of the police on both sides of the border cannot communicate with each other. One of the reasons is that their radio systems cannot be linked easily. For example, before the MACICO project, the only interoperability between public protec-tion and disaster relief (PPDR) actors from different countries was achieved by putting two handsets together with duct tape. Another example is that, in France, there was no connection between the networks of the two national police agencies. The MACICO project develops a concept for interworking of security organizations in their daily activity. It allows for easily setting up communication channels linking the radio networks that do not use the same technology.

The overall impression gained from the international MACICO project is good. The main objective to provide full interoperability between different TETRA and Tetrapol networks has been achieved. With the achieved technical solutions, the following networks can be connected: TETRA-TETRA, TETRA-Tetrapol, Tetrapol-Tetrapol. This comes at the right time, as there is currently increasing pressure from the governments that this cooperation happens. An important aspect is also that the MACICO solution allows migration from an older to a more recent solution, without interrupting the services. This opens new opportunities, for example, in the promising transition to the 4G/LTE technology.

The research area of the MACICO project was interoperability at all levels:

1. ICT technology used in the field of PPDR,
2. services that apply PMR and broadband technology,
3. service providers and PMR operators, and
4. operational procedures of PPDR actors.

The MACICO project was an industrial-driven project with a good mix of industries with high potential impact. The partners mentioned that five new products were developed and five products were improved and will be commercialized soon. The main technology innovation of the whole international consortium was a mobile device that allows setting up connectivity between Tetrapol and TETRA systems, which

can link different intervention teams in the operational field within minutes. Within the Finnish consortium members, the main technical innovations were TETRA-TETRA ISI phase 2 and the 4Com router solution for secure and reliable multi-channel communication by implementing the Distributed Systems intercommunication Protocol (DSiP).

With regard to voice communications and short messages, the international consortium provides the architecture and the technology to implement the following use cases:

1. Inter-network communication, referring to communication between terminals from two different networks, where each terminal is under the coverage of its own network;
2. Overlapping networks, referring to communication between terminals from two different networks, where each terminal is under the coverage of its network but can communicate to all the other terminals;
3. Coverage expansion, addressing the challenge that a terminal from one network can operate in the visited network with the same services as if it were under the coverage of its network of origin and
4. Migration, referring to inter-network communication with terminal mobility (Handover from one network to the other).

The only above-mentioned use case that was not fully demonstrated within the MACICO project was the migration use case. The main technical goal was reached: voice and short messages for Tetra(pol)-Tetra(pol) are operational and correspond to the use-case description. What did not fully transpire in demonstrations was how the discussions with the user groups were materialized in requirements for the project and for exploitation.

Much research exists from the field of mobile broadband for PPDR, cf. section 2.2. The MACICO project presents a concept of redundant and secure data communica-tion network systems in a multi-organizational environment, where PPDR, critical infrastructure protection and military actors, can operate in parallel. The MACICO project proposes a new fully decentralized architecture with optimized critical communication channels (Rajamäki, Rathod, & Holmström, 2013). Here, network actors and elements are identified and authenticated by establishing a physical connection. This concept also recommends a group-level, user-authorization mechanism for each participating organization. The decentralized architecture concept uses the Distributed Systems intercommunication Protocol (DSiP). The concept is highly fault-tolerant in routine as well as crisis operations. The software-based approach is independent of heterogeneous data communication technologies, IP networks, and telecommunication operator services. The solution enables the building of an effective and lasting cyber-secure data network for the multi-organizational environment. Being a fully decentralized concept, networks of individual member organizations will be virtually autonomous and unlikely to upset each other, allowing smooth message and information exchange to enable interoperability.

The nature of secure and reliable critical communication depends on the serving actors. Consider a scenario where an electricity transmission system operator detects a problem in the main power grid, and the load and power plant must be disconnected in milliseconds. This exacting requirement demands proprietary communication channels. Most other PPDR, critical infrastructure protection, and military users can rely on the adequacy of regular telecom operators' latency, but not on the performance of a single operator. Mission and safe critical communications should use communication channels distributed in parallel, because it must be fail-safe and unbreakable (Rajamäki et al., 2013).

From an investment point of view, the technical solution must withstand time and not 'paint itself into a corner.' The exceptional circumstances that should be taken into account include that the telecom operator may not always be there or that critical data should move, even though the IP-network is not available. Cooperation amongst various actors is becoming more valuable due to the aforementioned reasons. Organizations may have different operational statuses, but the communication solution should support all of them in their mutual and internal communication without suppressing any cooperation. The customer should have freedom of choice, being the 'master' of his/her application. This cannot be assigned to any telecom operator or vendor because situations change constantly. The selected communications architecture should bend to the needs, not vice versa (Rajamäki et al., 2013).

The nature of a crisis event affects the usable media. During a panic event, public cellular technology is useless. The public cellular data becomes highly loaded even during minor events with a large crowd, but dispersed communication may get through. In the case of an oil disaster, within a large geographic area, cellular technology is operative, and interoperability is required. TETRA works in all circumstances, but its data capacity is limited. TEDS will bring some improvement; however, it may fall short regarding future needs. Satellite communication can be considered pretty advantageous. A comprehensive answer can be found with parallel use of several communications networks, and DSiP realizes this demand. Furthermore, it is possible to interconnect any device or network segment using any media in DSiP: IPv4, IPv6 or non-IP supported in DSiP. Moreover,

a redundant and secure form of communication is supported. DSiP may be regarded as a multi-point to multi-point mesh-structured VPN network with good control over priority, security, and reliability. Applications and devices will see the multiple connections as a single connection channel, thus eliminating the modification of any application or device (Rajamäki et al., 2013).

At Laurea, MACICO's main application areas emphasize the continuum of Laurea's persevering research and development. The application area *resilient systems and infrastructures* (see section 7.4) is a straight continuum of the RIESCA project [Rescuing of Intelligence and Electronic Security Core Applications, 2007-2010, cf. (Pirinen & Rajamäki, 2010)]. The application areas *multinational tracking systems* (see section 6.5) and *law enforcement authorities' cross-border operations* (see section 6.4) go on with the research of the SATERISK project [Risks of Satellite-based tracking, 2008-2011, cf. (Rajamäki, Pirinen, & Knuuttila, 2012)]. The application area *unmanned aircraft systems as tools for co-operation between authorities* (see section 6.2) has synergy with the AIRBEAM project (AIRBorne information for Emergency situation Awareness and Monitoring, 2011-2015, cf. http://airbeam.eu/project/). The application area *mobile platform security* (see section 7.1.2) studies how the applications and services developed for emergency response vehicles within the MOBI project (Mobile Object Bus Interaction, 2010-2013 cf. (Tikanmäki, Rajamäki, & Pirinen, 2014) could be interconnected to other systems and services.

The business relevance becomes clear from the need for interoperability between different PMR technologies that must allow, in the future, that cooperation between different emergency organizations is possible. The coming months and years will decide how this materializes. However, the MACICO project has highlighted a con-scious that the public protection and disaster relief actors (firemen and police, among others) do not like to share their resources (including their networks), and there is work ahead to convince them to adopt this new way of working; for example, further discussions would be needed to ensure data interoperability. To solve this challenge, "trust building" should be the main research and development area in the future.

Traditionally good cooperation between different authorities in Finland enables development for the whole PPDR sector. The supportive atmosphere enables productive co-operation between universities, authorities, and companies. Finland has evidence of success in developing ICT systems: development of public mobile networks, the first nationwide TETRA network, and the POKE field command system. The national target, stated in Finland's cyber security strategy, is to become a leading nation in cyber security by 2016 (Finland's cyber security strategy.2013). DIGILE is going to start its strategic research agenda (SRA) for cyber trust (Ahokangas et al., 2014). Its main breakthrough target is to return privacy and trust in the digital world and to gain a global competitive edge in security-related business. The trust building among PPDR actors should start in Finland as a sub-task or a parallel research agenda of DIGILE's SRA.

9.2 Business Models of Public Safety Cross-border Communications

Tapio Savunen

The business models of public safety cross-border communication services are much more complex than the models of public safety services within one country. This goes for several aspects: the number of contracting parties, the estimation of additional value created, and the cost-sharing model. All three of these aspects are briefly discussed here.

In a typical business model of a public safety communication service, the key contracting parties are user organizations (e.g. police, rescue, and border guard), a communications service provider ("PMR Operator"), and a governmental organization that is in charge of allocating the funding for the investments. The last one is usually the Ministry of the Interior. The governance of the public safety service provider is usually agreed between the user organizations and the Ministry of the Interior.

In an arrangement where more than one country is involved, the number of contract-ing parties is easily doubled. When an agreement between two or more countries is in question, an inter-governmental agreement is needed. Issues like share of responsibilities, liabilities, and the distribution of costs of the cross-border operations need to be solved and agreed upon in the context of the inter-governmental agreement.

When the set-up between the countries is symmetric, the benefits, liabilities, and costs are evenly distributed between them. Then, also, the business model is symmetric. Both parties have the evenly distributed roles of a service provider and a service consumer. However, if the situation between the countries is asymmetric, that is, one country benefits more from the cross-border operations than the other, the starting point is more complex. One of the countries is more in the role of the service provider and the other one in the role of the service consumer.

The assessment of the value in Public Safety cross-border operations depends on the original objectives of the arrangement. If the objective is to share the resources in the border area in every-day operations, the measurable cost savings

are the basis of the value assessment. For example, if the number of police officers can be reduced by enabling them to operate on both sides of the borderline, the value of the arrangement is fairly easy to measure. However, if there is an agreement which enables the allocation of resources from both sides of the borderline in an exceptional situation, for example a major accident, the valuation is more complex. In such a case, the additional value provided by the cross-border operations cannot be calculated by the number of saved resources, but the socio-economic benefits to society and the wider economy need to be evaluated. What is the value to the Public Safety users and other key stakeholders, such as the public at large? The question is about the value of the society's safety and hence challenging to measure.

The share of the costs between the countries depends on the symmetry of the roles. If the benefits are distributed equally between the parties, the agreement can be that both parties defray their own costs, and no monetary transactions take place be-tween the countries. In the case of asymmetric roles, the country being in the role of the service provider may want to have compensation for the resources used. Another option is to estimate the value delivered to the other country and agree on the service price based on that. When the agreement takes place between the governments of the countries, naturally the aspects are manifold and the definition of the price is not so straightforward.

To summarize, the elements of the business models of public safety cross-border communication services are various, and there are many different options. Hence, the number of potential models is also large.

9.3 Future Research Needs

Heikki Riippa

The market on TETRA and Tetrapol is dominated by Airbus Defence and Space and Motorola, who both have a 40% market share of each. It is the pressure of the gov-ernments and this kind of project that help to make interoperability happen and that standardization is progressing. The MACICO consortium should take advantage of the strong position of Airbus Defence and Space in standardization to further influence ISI-related aspects and use the cooperation with system vendors to include public safety aspects in the 4G/LTE standards.

As a continuum of the MACICO project, the following two topic proposals would be presented to be included in the EU's HORIZON 2020 framework program for research and innovations.

Proposal one: End-User-driven next generation PPDR Mobile Broadband Service Concept - Interoperability between organizations and nations

Specific challenge: Law Enforcement Agencies (LEA´s) are building effective field command and control systems with mandatory mobile applications. These mobile systems need a reliable broadband solution that does not depend on public mobile services. A cost-efficient roadmap and implementation of next generation public safety (PS) radio systems/services is needed, taking the best of existing (TETRA, Tetrapol) services and their capability for evolution into the context of broadband commercial, mobile virtual network operator and dedicated public safety broadband networks. Optimization of the total cost of ownership of public safety radio services and applications is needed, utilizing also commercial mobile markets and terminals. Seamless evolution of current PMR services (TETRA, Tetrapol) is the goal, without any disruption in their use and flexible extension to utilize broadband radio access and intelligent commercial and dedicate mobile terminals. European harmonization of the Public Safety mobile service roadmap provides a sufficient market for competitive offering, providing the PS customers' choice and cost efficiency. EU-harmonized utilization of commercial market offerings also provides the base line for interoperability, utilizing international commercial cellular communications interoperability.

Scope: Focus on existing and emerging public safety mobile voice and data services, starting with the currently used TETRA and Tetrapol voice services, extended by existing and developing mobile data services in PPDR field operations, and further migrating to multimedia (video) services, which are based entirely on broadband mobile access. Commercial cellular and legacy PMR radio networks and services, and also terminals, will provide the baseline of the pilot, while the focus of project development is on key Public Safety voice and data services, e.g. law enforcement and rescue applications that are not available in the commercial offerings or not compliant to the requirements of public safety use cases.

Expected impact: A carefully analyzed, cost-efficient roadmap and pilot case for PPDR's to utilize dedicated broadband mobile networks technology is developing very rapidly. As a result, the harmonized solution will provide interoperability of the networks and mobile broadband services at all levels, nationally and interna-tionally EU-wide. Also, critical points of the interoperability issues will be analyzed, verifying in practice LEA's and Rescue services applications, integrated terminal devices (like ANPR) to fit to the end-users' needs found by best practices cooperation. By selected pilot implementations, there is a possibility to verify the real

costs and functional problems to help with standardization and harmonization efforts.

Proposal two: Mobile Service Platform for PPDR vehicles - ICT and technology integration and architecture to secure effective field operations

Specific challenge: A modern PPDR vehicle is a complicated combination of technology, and it has to survive in different conditions and situations depending on the status of field operations. Different types of technology must be integrated to achieve a reliable and flexible solution for PPDR officers' mobile workspace on the field. European PPDR organizations are using Mobile Communication Applications and other peripherals (ANPR, Fingerprint readers, Video Streaming) in their mobile units (cars, boats, bikes, etc.). These mobile connections are mainly based on IP. Technical solutions vary among MS PPDR organizations, and are mostly tailored using unique national solutions. There is no common approach to build the mobile service platform on cars and other mobile units. There is also a need for services launched from PPDR vehicles (e.g., controlling and finding priorities for traffic lights). At the same time, PPDR organizations are building Command & Control systems, which are using advanced mobile applications. These solutions are becoming mandatory when providing PPDR field-operation services in the future. These solutions seem to be built on a case-by-case basis, by tailoring without any common architectural approach. There is also a possibility to find new innovations on services which can be triggered from PPDR vehicles (e.g., launching a green wave to traffic lights along driving routes). Meanwhile PPDR organizations are searching/developing a dedicated mobile broadband solution (frequencies & technology) in Europe. The basic decisions for frequency allocation will probably be made in 2015. There is a need to develop a standard mobile platform as a part of a mobile broadband technical concept for PPDR organizations. This kind of innovation/integration/piloting project needs partners from several user organizations, car & other vehicle industries, the telecommunication industry, the ICT and PPDR peripheral industry (routers, cameras, alcometers, fingerprint readers, etc.).

Scope: To find common de facto standards for architecture and technology in PPDR mobile units, tense co-operation between Users, the ICT industry, and the car Industry is required. Also, research to find standards for PPDR mobile technology is needed. Innovation should be created using user interfaces, ergonomics, installations and demonstrations of real PPDR mobile environment. Testing different types of user interfaces is also essential. The developed solutions must be modular and flexible and also (if possible) be based on off-the-shelf technology. The project should concentrate on technical architecture and user interfaces used on PPDR mobile units (vehicles etc.). The main scope is to find a cost-effective mobile ICT service platform for PPDR vehicles. The common solutions for broadband technology and infrastructure should be left outside of the project, and be clarified in other projects.

Expected impact: To create (1) a de facto standard for PPDR mobile unit architecture, with all the necessary layers (hardware, software, user interfaces), accepted by user organizations and e.g., the car industry; (2) common specifications for PPDR vehicle mobile communication architecture platform; (3) pilot installations and tests. The developed solutions should enable efficient use of resources on the field and increase the possibilities to use digital services transparently in processes beginning in the field. Also, new innovations on user interfaces, technology implementations, and services are expected. With standardization, the PPDR mobile communication architecture and co-operation with car and vehicle industries will decrease the implementation costs of the desired technology.

9.4 Developing Ties by Improving Communication Channels Between Public and Private Actors in Securing Societies

Juha Knuuttila

Telecom industries are competing from quarter to quarter by launching new 4G/LTE generation products, services, and business models to replace older ones. The mountains of abandoned – also relatively new – handsets keep piling up.

In police work, they are still using the unchanged TETRA basic technologies, eventually complemented with TEDS and other updates, and sometimes even using the same handsets throughout the quarter of the centennial.

Quantative Development: Widening the Client Circle of TETRA to Semi-Public, Semi-Private, and Private Areas

In the growing telecom markets, new systems continue to penetrate the world, which drives the market. Subscribers are counted in the billions. The number of po-licemen (and other law enforcement officers and search and rescue staff, too), on the contrary, is diminishing, and in terms of potential LEA end-users respectively, TETRA markets are not growing. The maximum numbers of TETRA network users in the biggest cities are counted in the tens of thousands.

At the same time, the number of private guards – and businesses like Securitas, G4S and ISS – continue to grow (Kerttula, 2010, 51); they are not seen or welcomed as new customers

for TETRA. On the other hand, they do not see TETRA´s existing pricing schemes as part of their lucrative business either.

How does the bridging of TETRA and LTE take place? The answer is very simply in the hands of the policeman: he or she may use a TETRA phone for taking a task and an LTE smart phone to accomplish it. A TETRA phone is provided by his/her employer, which may be the case with the LTE phone as well.

If a policeman has to carry out a duty, where making an international telephone call is required, a smart phone will be used. The roaming system of TETRA ISI is in the early stages of making, which was the case of the commercial network roaming during the first quarters of mobile telephony 25 years – a policeman´s quarter - ago.

One can ask whether PMR operators and vendors have been too close to customers like police for too long in the environment of stagnating budgets (Bower & Christensen, 2010). At the same time, private security businesses and semi-public fire-fighting and semi-private search and rescue organizations have continued to grow. Stagnating budgets of existing end-users do not allow more investments in the TETRA networks´ capacity building in order to market for new end users for security and healthcare areas, which are at least from ten to twenty times larger than the traditional PPDR client area. Is there a way of breaking the circle caused by stagnating budgets by finding new business models by attaching LTE services on top of TETRA services?

Qualitative Development 1: A Boost from LTE to TETRA?

Tony Gray (2014) nutshells the business relation of TETRA and LTE very nicely in an interview:

"Can commercial networks with added public-safety features adequately serve the PPDR market?
Gray: As usual, it comes down to resources and investments being the limiting factors. PPDR users have become used to expecting, from existing TETRA services, highly resilient, available and reliable service with virtually ubiquitous geographic coverage and guaranteed capacity, particularly in times of crisis. Any and all these metrics are challenging, to say the least, for commercial networks to deliver against, because by their very nature, they represent best efforts service, dimensioned to provide optimal return on investment for primarily consumer applications."

In other words, LTE will not be disrupting technology regarding TETRA (ct. to Bower & Christensen, 2010). It takes only a severe thunderstorm to understand this. Well protected TETRA networks survive them, while public radio broadcasting and public cellular networks suffer service breaks. The task is to bridge services between TETRA and LTE where the USA´s FirstNet shows one way to go as cited below.

Qualitative Development 2: TETRA in Fire, the Air and by Sea?

There are new frontiers to be conquered in remote sensing areas, which require feasibility studies on where TETRA support is needed. In some countries, indoor TETRA availability is becoming a standard in public buildings and places. Automated sprinkler systems now report to buildings' electricity control room about functioning sprinklers. Can these systems be empowered with TETRA in order to help fire fighters by connecting sprinkler reporting to fire fighters´ control and command system?

There are plans on how to drive Remotely Piloted Aircraft System (RPAS) by using TETRA commands, which may be an untested powerful option for cases where natural hazards, like earthquakes, cause overload in other networks. How should portable TETRA systems be combined with maritime awareness, and search and rescue systems (cf. to Hajo et Al., 2011)?

There are other remote sensing areas, like networking of CCTV systems, enhanced with artificial intelligence pattern recognition, where big savings can be achieved in the control and command room end.

Business Model Development: Go West!

The birth of the TETRA/TETRAPOL standard is twisted with the release of certain radio spectrums, free from occupation of the U.S. military in Europe. In these arrangements, it became difficult for European vendors to compete with TETRA technology in the USA´s law enforcement communication markets, which are still heavily dependent on analog radio systems.

In the USA, 911-emergency calls and related services have become a field of competence between telecom operators, due to the applied business model. A certain turn-over percentage is to be put on the maintenance and development of 911 services for the public, which is a marketing issue.

Work done under a powerful NCC Committee has made it possible for FirstNet by using a nationwide spectrum license, where FirstNet will provide a single platform for daily public safety communications. When natural disasters, threats to our nation's security, or other emergencies occur anywhere in the country, FirstNet will enable local, state, regional, and national emergency responders to communicate at the direction of the incident commander.

FirstNet will be built to public safety-grade standards, using Long-Term Evolution (LTE) wireless technology, the most advanced available today. FirstNet will deliver greater coverage, capacity, connectivity, cybersecurity, and resiliency than the current multiplicity of diverse public safety wireless systems. Police, firefighters, and emergency medical service personnel will still rely on their land mobile radio (LMR) networks for mission-critical voice, with FirstNet providing high-speed data, supplemental commercial grade voice, and eventually mission-critical LTE voice. First-Net also will support the integration of LMR networks, even after LTE voice is provided.

Created by the Middle Class Tax Relief and Job Creation Act, signed Feb. 22, 2012, FirstNet is funded by the law and projected proceeds from 2014 spectrum auctions. The network is overseen by a Board, including individuals from public safety: current and former local, state, and federal officials, and wireless experts. FirstNet is an independent entity within the U.S. Department of Commerce, National Telecommunications, and Information Administration (FirstNet, 2014),

In comparison to these developments in the USA, Europeans are stuck in their national and intra-national bureaucratic silos, where everybody is defending their diminishing budgets. The most cynical experts say it will take World War III and a new U.S. occupation of Europe to establish the spectrum lee-way needed for enhanced TETRA/LTE services. Nevertheless, there are now compromised pan-European proposals on the table, by the LEA community, but without the uniform support of telecom businesses. Leadership a la FCC is needed in Europe – and billions of euros!

While waiting for a crisis to occur, in order to get political decision making to move ahead, let us concentrate on working step by step on projects like those proposed in previous chapter 9.3 and widening the multitude of business models described in chapter 9.2.

Finland could play a role here, but overcoming of existing silos and clusters, whether security or ITC or healthcare, with their "administratification" is needed: "... a constant awareness of the dilemmas and of the possibilities of the actual institutional practices and visions of the future is needed. Neither is sufficient by itself" (Miettinen, 2002, 148-149; cf. also Kanter, 2010).

The most important dilemma is this: How can we make better transparent value propositions for the real end users, the citizens, in terms of safety and security?

References

Ahokangas, M., Arkko, V., Aura, T., Erkinheimo, P., Evesti, A., Frantti, T., . . . Vepsäläinen, P. (2014). *Strategic research agenda for cyber trust DIGILE*.

Bower, J., & Christensen, C. (2010). Disruptive Technologies: Catching the Wave. *Harvard Business Review on Business Model Innovation*, originally published in 1995, Boston: Harvard Business School Publishing Corporation, 2010.

Gray,T. (2014), A Chat with Broadband Group, *RadioResource International*, Quarter 2 2014.

Finland's cyber security strategy. (2013). Retrieved from http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy

FirstNet (2014) Retrieved from http://www.ntia.doc.gov/page/about-firstnet

Hajo, E., Jones, J., Meyer, F., Mahoney, A., Druckenmiller, M., Rohith, M., & Kambhamettu, C. (2011). Environmental Security in Arctic Ice-Covered Seas: From Strategy to Tactics of Hazard Identificatiob and Emercency Response, *Marine Technology Society Journal* , Vol. 45, Nr. 3, May/June 2011.

Kanter, R. (2010). From Spare Change to Real Change: The Social Sector as Beta Site for Business Innovation, *Harvard Business Review on Business Model Innovation*, originally published in 1999, Boston: Harvard Business School Publishing Corporation, 2010.

Kerttula, T. (2010). *Vartijat ja järjestyksenvalvojat julkisen vallan käyttäjinä*, Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut.

Pirinen, R., & Rajamäki, J. (Eds.). (2010). *Integrative student-centred research and development work: Rescuing of intelligence and electronic security core applications (RIESCA)*. Vantaa: Laurea publications.

Rajamäki, J., Pirinen, R., & Knuuttila, J. (Eds.). (2012). *SATERISK - risks of satellite-based tracking: Sample of evidence series*. Vantaa: Laurea-University of Applied Sci-ences, Leppävaara Unit.

Rajamäki, J., Rathod, P., & Holmström, J. (2013). Decentralized fully redundant cyber secure governmental communications concept. *Intelligence and Security Informatics Conference (EISIC)*, 2013 European, 176-181. doi:10.1109/EISIC.2013.39

Tikanmäki, I., Rajamäki, J., & Pirinen, R. (Eds.). (2014). *Mobile object bus interaction - designing future emergency vehicles*. Vantaa: Laurea.

LIST OF PUBLICATIONS

Doctoral Thesis

Rajamäki, J. (2014). *Studies of Satellite-Based Tracking Systems for Improving Law Enforcement. Comprising Investigation Data, Digital Evidence and Monitoring of Legality*. Doctoral Thesis. Jyväskylä: University of Jyväskylä.

Journals

Aho, J., & Rajamäki, J. (2013). How to improve safety of school environment: A case study of safe school in Finland. *Urban Planning and Design Research*, 1 (21), 19-24.

Aro, M. & Rajamäki, J. (2014). Multi-agency cooperation in cross-border operations in the field of public protection and disaster relief. *International Journal of Education and Information Technologies*, 8, 244-251.

Kämppi, P., Tyni, J., & Rajamäki, J. (2014). Gathering end-user requirements for the MACICO public safety communications project. *International Journal of Communications*, 8, 21-28.

Rajamäki, J. (2014). Software intensive GNSS-based tracking systems for improving law enforcement. *WSEAS Transactions on System and Control*, 9, 629-639.

Rajamäki, J., Ahokas, J., & Rathod, P. (2013). A redundant communications solution for critical infrastructure protection and SCADA systems. *International Journal of Communications*, 1 (1), 109-117.

Rajamäki, J., Knuuttila, J., Suni, O., Silanen, H., Tuomola, A., & Meros, P. (2014). How to empower policemen and their vehicles: A multiple case study analysis of seven public safety related ICT projects. *International Journal of Systems Applications, Engineering & Development*, 8, 238-249.

Rajamäki, J., & Rathod, P. (2014). How standardized utility cloud services and service-oriented architecture benefits in public protection and disaster relief ? *International Journal of Computers and Communications*, 8, 86-93.

Rajamäki, J., Rathod, P., & Kämppi, P. (2014). A redundant tracking system for public safety and emergency response: Reporting past research, present findings and future directions. *International Journal of Systems Applications, Engineering & Development*, 8, 76-83.

Rajamäki, J., & Viitanen, J. (2014). Near border information exchange procedures for law enforcement authorities. *International Journal of Systems Applications, Engineering & Development*, 8, 2015-2020.

Tikanmäki, I., Tuohimaa, T., & Ruoslahti, H. (2012). Developing a service innovation utilizing remotely piloted aircraft system (RPAS). *International Journal of Systems Applications, Engineering & Development*, 6 (4), 279-287.

Peer-reviewed conference papers

Drouglazet, L., Rajamäki, J., Tyni, J., & Aro, M. (2014). Multi-agency cooperation in cross-border operations (MACICO) project. *8th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14)*, 129-136.

Jokinen, E., Rajamäki, J., Karppinen, K., Tarkkanen, L. & Tiainen, S. (2014). Learning within research, development and innovation projects. Case: MACICO project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy.*

Kämppi, P., Aro, M., & Rajamäki, J. (2014). End-user requirements for multi-agency cooperation in cross-border operations (MACICO) project. *8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST'14)*, 183-190.

Kämppi, P., Rajamäki, J., Kervinen, I., & Saijonmaa, J. (2014). Use cases and technical solutions for cross border operation pilot. *8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14)*, 37-42.

Kämppi, P., Tyni, J., & Rajamäki, J. (2014). Use cases of the multi-agency cooperation in cross-border operations (MACICO) project. *8th International Conference in Circuits, Systems, Signal Processing and Communications (CSST'14)*, 209-212.

Rajamäki, J. (2012). Redundant multichannel public safety communications network for public protection and disaster relief (PPDR) organizations. *3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE'12)*, 56-61.

Rajamäki, J. (2012). Cross-border satellite-based tracking: Needs, approach, benefits and competition. *Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS)*, 1-8. doi:10.1109/UPINLBS.2012.6409747

Rajamäki, J. (2014). Challenges to a smooth-running data security audits. case: A Finnish national security auditing criteria KATAKRI. *Joint Intelligence and Security Informatics Conference*, 240-243.

Rajamäki, J. (2014). Externally funded research, development and innovation projects as learning environments. Case: the MOBI project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy*.

Rajamäki, J. (2014). The MOBI project: Common mobile digital services for all public protection and disaster relief (PPDR) vehicles. In J. Music (Ed.), *Recent advances in computer engineering, communications and information technology*, WSEAS Press, 120-125.

Rajamäki, J., Daifi, M., Töyrylä, T., Alanko, M., Kiiski, P., Isohanhi, J., Kivelä, M., Viuhko, M., Nevalainen, J., Kuikka, H., & Tarkka, J. (2014). A multinational research project as a platform for multi-discipline learning environment. Three cases as a part of the MACICO project. *17th International Conference on Interactive Collaborative Learning and 42nd International Conference on Engineering Pedagogy*.

Rajamäki, J., & Rajamäki, M. (2013). National security auditing criteria, KATAKRI: Leading auditor training and auditing process. *12th European Conference on Information Warfare and Security*, 217-223.

Rajamäki, J., & Rathod, P. (2013). Leveraging benefits of standardized utility and cloud computing with service-oriented architecture in public protection and disaster relief. In S. Lopes (Ed.), *Recent advances in computer engineering series*, vol. 16, WSEAS Press, 74-80.

Rajamäki, J., Rathod, P., Ahlgren, A., Aho, J., Takari, M., & Ahlgren, S. (2012). Resilience of cyber-physical system: A case study of safe school environment. *European Intelligence and Security Informatics Conference (EISIC)*, 285-285. doi:10.1109/EISIC.2012.10

Rajamäki J., Rathod P., & Holmström J. (2013). Decentralized fully redundant cyber secure governmental communications concept. *European Intelligence and Security Informatics Conference (EISIC)*, 176-181. doi: 10.1109/EISIC.2013.39

Rajamäki, J., & Ruohomäki, P. (2013). Multi-agency cooperation in cross-border operations: Information exchange between law enforcement authorities. *International Congress of Engineering and Informatics*, 271-279.

Tikanmäki, I., & Rajamäki, J. (2012). Exploiting security, safety and situational related services by using remotely piloted aircrafts. *3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE'12)*, 50-55.

Tikanmäki, I., & Tuohimaa, T. (2011). How real time picture and situational awareness can be improved by using unmanned aircraft systems (UAS)? *Recent Researches in Communications, Electrical & Computer Engineering*, WSEAS Press, 28-33.

Tuohimaa, T., & Tikanmäki, I. S. (2011). The strategic management challenges of developing unmanned aerial vehicles in public safety organizations. *Recent Researches in Communications, Electrical & Computer Engineering*, WSEAS Press, 34-39.

Conference presentations and submitted papers

Kämppi, P. (2014). MACICO project: Proposal for TETRA-TETRAPOL interoperability solution. *Public Safety Communications Europe Conference*, Gothenburg, Sweden.

Rajamäki, J. (2014). Plenary lecture 3. Multi-agency cooperation in cross-border operations. *8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14)*, Playa de las Americas, Spain.

Rajamäki, J. (2015). Cyber security education as a tool for trust-building in cross-border public protection and disaster relief operations. *IEEE Global Engineering Education Conference*, Tallinn, Estonia.

Rajamäki, J. (2014). Information security policy development and implementation piggybacking onto Finnish national security auditing criteria KATAKRI. *5th European Conference of Computer Science*, Geneva, Switzerland.

Simola, J. & Rajamäki, J. (2014). Using a Real-time Video to Allocate Public Protection and Disaster Relief Resources in Rescue Service Process. Case: Natural Disaster in the Viksu 2014 Young Firefighters Camp. *5th European Conference on Computer Science*, Geneva, Switzerland.

Master's thesis

Laitinen, O. (2013). Yrityksen turvallisuuspolitiikan laatiminen.

Pullinen, M. (2012). Kriittisten tietojärjestelmien suojaaminen kyberuhilta.

Rajamäki, M. (2011). Pätevyysmalli turva-auditointikoulutukselle: Tapaustutkimus Laurean auditoinnin johtaminen-opintojaksosta.

Ruohomäki, P. (2012). Public key infrastructure operations model.

Tuohimaa, T. (2014). Studies of unmanned aircraft systems from the perspective of operational use.

Thesis

Aaltonen, H. (2014). Simulated natural disaster in Viksu 2014 Young Firefighters' Camp.

Assinen T., Kemppainen J. (2014). Emergency medical service actions in simulated multi-casualty situation. Case: Viksu 2014.

Harvio, V. (2014). Use of real-time video in rescue operations – Current state and future prospect.

Iiskola, S. (2014).Can Viksu 2014 Young Firefighters' Camp's present security and prepar-edness plans respond to accidents and disturbances caused by people?

Jääskeläinen, V. (2014). Monologista dialogiksi—Katakri-pääauditoijakoulutuksen kehittäminen.

Kimiläinen, M. (2011). Yritys X: N henkilöstöturvallisuuden ja fyysisen turvallisuuden esiauditointi kansallisella turvallisuusauditointikriteeristöllä.

Kojo, J. (2013). Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla.

Leppänen, R. (2014). Evaluation of situational operation view for field operation leading.

Martiskainen, M. (2012). Sisäinen turvallisuusauditointi aikuiskoulutusoppilaitoksessa.

AUTHORS

Surname	First name	Position in Laurea	Position in project
Aaltonen	Harri	Student	
Ahlgren	Anu	Graduate student	
Ahlgren	Sami	Graduate student	
Aho	Johanna	Graduate student	
Alanko	Minna	Graduate student	
Aro	Mari	Project worker	Researcher
Assinen	Taneli	Student	Thesis worker
Daifi	Mourad	Graduate student	
Drouglazet	Laurent		Coordinator of Celtic MACICO
Harvio	Viktor	Student	Thesis worker
Holmström	John		Board member
Iiskola	Samu	Student	Thesis worker
Isohanni	Juhana	Graduate student	
Jokinen	Esa	Graduate student	Masters' thesis worker
Jääskeläinen	Ville	Student	Thesis worker
Kemppainen	Janne	Student	Thesis worker
Kervinen	Ilkka		Partner representative (Airbus Defence & Space)
Kiiski	Petrus	Graduate student	
Kimiläinen	Mikko	Student	Thesis worker
Kivelä	Mia	Graduate student	
Knuuttila	Juha	Principal lecturer	
Kojo	Jussi	Student	Thesis worker
Kuikka	Heidi	Graduate student	
Kämppi	Pasi	Project Manager	Researcher
Laitinen	Olli	Graduate student	Thesis worker
Leppänen	Riku	Intern	Thesis worker

Martiskainen	Mona-Kristiina	Student	Thesis worker
Meros	Päivi	Graduate student	
Nevalainen	Jenni	Graduate student	
Pirinen	Rauno	Principal lecturer	Researcher
Pullinen	Mika	Graduate student	Thesis worker
Rajamäki	Jyri	Principal lecturer	Scientific Director
Rajamäki	Merja	Graduate student	Thesis worker
Rathod	Paresh	Senior lecturer	Researcher
Riippa	Heikki		End-user representative (National Police Board)
Roisko	Ville	Project worker	Researcher
Ruohomäki	Petteri	Graduate student	Thesis worker
Ruoslahti	Harri	Senior lecturer	Researcher
Saijonmaa	Jaakko		Board member
Savunen	Tapio		Partner representative (Airbus Defence & Space)
Silanen	Henna-Riitta	Graduate student	
Simola	Jussi	Graduate student	
Suni	Outi	Graduate student	
Takari	Mari	Graduate student	
Tarkka	Jaana	Graduate student	
Tarkkanen	Laura	Project Manager	
Tiainen	Seija	Senior lecturer	Project Manager
Tikanmäki	Ilkka	Project Manager	Researcher
Tuohimaa	Tuomo	Graduate student	Thesis worker
Tuomola	Antti	Graduate student	
Tyni	Jaakko	Chief R&D Officer	Researcher
Töyrylä	Tomi	Graduate student	
Viitanen	Jouni	Lecturer	Researcher
Viuhko	Marko	Graduate student	

Laurea Julkaisut | Laurea Publications

LAUREA
AMMATTIKORKEAKOULU

Pasi Kämppi, Jyri Rajamäki,
Saija Tiainen & Riku Leppänen (eds.)

MACICO

Multi-Agency Cooperation In Cross-border Operations

Samples of Evidence Series: Volume 4

Cooperation between Public Protection and Disaster Relief actors across a border is a difficult task today, because the teams on both sides of the border cannot communicate with each other. One of the reasons is that their communication systems cannot be linked easily. Other challenges are related with heterogeneous operational procedures, heterogeneous services and the lack of trust between cooperating parties. The MACICO project presents a concept for interworking of security organizations in their daily activity that guarantees communications reliability, integrity and security.

Tekes

Celtic-Plus
Smart Connected World