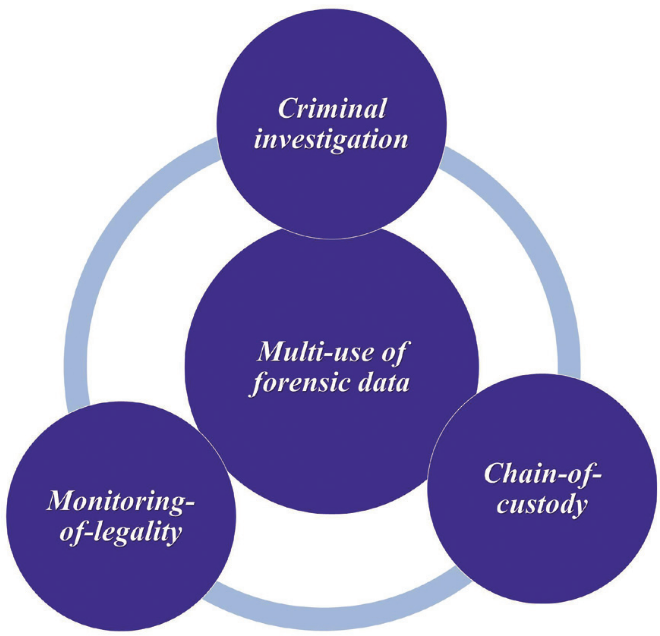
JYVÄSKYLÄ STUDIES IN COMPUTING
192

Jyri Rajamäki

Studies of Satellite-Based Tracking Systems for Improving Law Enforcement

Comprising Investigation Data, Digital Evidence and Monitoring of Legality



JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 192

Jyri Rajamäki

Studies of Satellite-Based Tracking Systems for Improving Law Enforcement

Comprising Investigation Data, Digital Evidence and Monitoring of Legality

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 3
syyskuun 6. päivänä 2014 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, Auditorium 3, on September 6, 2014 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2014

Studies of Satellite-Based Tracking Systems for Improving Law Enforcement

Comprising Investigation Data, Digital Evidence and Monitoring of Legality

JYVÄSKYLÄ STUDIES IN COMPUTING 192

Jyri Rajamäki

Studies of Satellite-Based Tracking Systems for Improving Law Enforcement

Comprising Investigation Data, Digital Evidence and Monitoring of Legality

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2014

Editors
Timo Männikkö
Department of Mathematical Information Technology, University of Jyväskylä
Pekka Olsbo, Ville Korkiakangas
Publishing Unit, University Library of Jyväskylä

URN:ISBN:978-951-39-5789-6
ISBN 978-951-39-5789-6 (PDF)

ISBN 978-951-39-5788-9 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2014

ABSTRACT

Rajamäki, Jyri
Studies of satellite-based tracking systems for improving law enforcement: Comprising investigation data, digital evidence and monitoring of legality
Jyväskylä: University of Jyväskylä, 2014, 166 p. (+included articles)
(Jyväskylä Studies in Computing
ISSN 1456-5390; 192)
ISBN 978-951-39-5788-9 (nid.)
ISBN 978-951-39-5789-6 (PDF)
Finnish summary
Diss.

Law enforcement agencies (LEAs) constantly seeks new technological recording, retrieving and monitoring solutions that would facilitate their combat against organized 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.

Keywords: chain-of-custody, crime investigation, global navigation satellite system, law enforcement, monitoring-of-legality, tracking

Author's address *Jyri Rajamäki*
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Supervisors *Prof. Pekka Neittaanmäki*
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Prof. Timo Hämäläinen
Department of Mathematical Information Technology
University of Jyväskylä
Finland

Reviewers *Prof. Jarmo Ahonen*
School of Computing
University of Eastern Finland
Finland

Prof. Rauno Kuusisto
Technical Research Centre
Finnish Defence Forces
Finland

Opponent *Prof. Dipankar Dasputa*
Dept. of Computer Science
University of Memphis
U.S.A.

ACKNOWLEDGEMENTS

I would like to express my gratitude to many people who have made this effort possible. First of all I want to express my sincere gratitude to my supervisors Professor Pekka Neittaanmäki and Professor Timo Hämäläinen. Both of them have provided valuable comments and advices that have helped throughout the project. I have been fortunate to have Professor Jarmo Ahonen and Professor Rauno Kuusisto as the reviewers of my dissertation. I'm grateful for the time and effort they have invested in the evaluation of my dissertation. I would like to thank both gentlemen for their constructive comments and recommendations for finalizing this thesis. I give my sincerest gratitude to Professor Dipankar Dasputa at University of Memphis for kindly agreeing to act as the opponent of this dissertation.

I have had the pleasure to work with talented researchers and Laurea's students in the research projects RIESCA, SATERISK, MOBI and MACICO that make this dissertation possible. Especially I thank MBA Jouni Viitanen who has had multiple roles during my doctoral studies and he has offered his precious time and insight through-out the course of the study. Jouni, having a long experience of developing and utilizing law enforcement technologies, was the main initiator of the SATERISK project during his studies in Laurea University of Applied Sciences. When he acted as a senior lecturer and project manager at Laurea, I had an opportunity to co-authored many articles with him, and these sessions had a key role in the initiation and progress of my research task. After returning to his daily work as an innovative police officer, Jouni has been the link between my research and practice.

I am also very grateful to all my colleagues at Laurea University of Applied Sciences. My warmest thanks go to Dr. Rauno Pirinen and Lic. Sc. Juha Knuuttila, a good and most helpful friend: these gentlemen have not only facilitated the present work, but also supported me in improving as a decent researcher. Thanks are also due to the co-authors of the included articles John Holmström, Pasi Kämppi, Paresh Rathod and Laurea's master's students.

For the financial support for this thesis and related work, I would like to thank the Finnish Funding Agency for Technology and Innovation (Tekes) and Laurea University of Applied Sciences.

My final thanks go to my friends and family, especially my grandchildren Minttu and Jami, who contributed to this journey by dragging me away from scientific work ever so often. And finally, my warmest and dearest thanks to my wife Merja; you have offered me a lot of comfort. Thank you for giving me your sincere support.

Paltamo, August 2014
Jyri Rajamäki

GLOSSARY

2G/3G/4G	Second/Third/Fourth-Generation
ABC	Automated Border Check
ACPO	Association of Chief Police Officers
AI	Artificial Intelligence
AIS	Automatic Identification System
BCP	border crossing points
BFC	Blue Force Tracking
BGAN	Broadband Global Area Network
C3I	Communications, Command and Control, and the Intelligence
CALM	Communications Access for Land Mobiles
CAN	Controller Area Network
CAST	Centre for Applied Science and Technology
CCR	Control and Command Room
CCTV	Closed-circuit television
CEN	European Committee for Standardization
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISE	Common Information Sharing Environment
CMA	Coercive Measures Act
CoS	Cost of Service
CSR	Case Study Research
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DNP	Distributed Network Protocol
DoS	Denial of Service
DSiP	Distributed Systems intercommunication Protocol
DSR	Design Science Research
EA	Enterprise Architecture
EC	European Commission
EDA	European Defense Agency
EES	Entry/Exit System
EISIC	European Intelligence and Security Informatics Conference
EMS	Emergency Medical Services
ENISA	European Network and Information Security Agency
ENLETS	European Network of Law Enforcement Technology Services
EPE	Europol Platform of Experts
ERV	Emergency Response Vehicle
ESM	Enterprise Service Management
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROSUR	European border surveillance system
FBCB2	Force XXI Battle Command Brigade and Below
FMS	Future Monitoring System

FR	First Responder
GEO	Geostationary
GIS	Geographic Information System
GLONASS	Globalnaja navigatsionnaja sputnikovaja sistema
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HMI	Human-Machine Interfaces
IaaS	Infrastructure as a service
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
II	Information Infrastructure
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPsec	IP Secure Architecture
IPv4, IPv6	Internet Protocol version 4, Internet Protocol version 6
IRL	Integration Readiness Level
ISI	Inter-System Interface
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITS	Intelligent Transport Systems
ITSM	Information Technology Service Management
ITU	International Telecommunications Union
KIISE	Korean Institute of Information Scientists and Engineers
KPI	Key Performance Indicators
LAN	Local Area Networks
LCC	Life Cycle Cost
LCD	liquid-crystal display
LE	Law Enforcement
LEA	Law Enforcement Agency, Law Enforcement Authority
LEO	Low Earth Orbit
LEWP	Law Enforcement Working Party
LTE	Long Term Evolution
M2M	Machine-to-Machine
MAV	Micro Air Vehicles
MIL	Military
ML	Machine Learning
MOBI	Mobile Object Bus Interaction
MPTCP	Multi-Path TCP-stack
NASA	National Aeronautics and Space Administration
NFPA	National Fire Protection Association

NIEM	National Information Exchange Model
Ni-MH	Nickel-Metal Hydride
NMEA	National Marine Electronics Association
NSA	National Safety Agency
OBSVA	One Box Single Vehicle Architecture
OLA	Operational Level Agreement
OSI	Open Systems Interconnection
OSSTMM	Open Source Security Testing Methodology
PA	Police Act
PMR	Professional Mobile Radio
PoC	Proof of Concept
PPDR	Public Protection and Disaster Relief
PPP	Public-Private Partnership
PS	Provisioning Server
PSC	Public Safety Communications
QoS	Quality of Service
RACI	Responsible, Accountable, Consulted, Consulted
ROI	Return On Investment
RTP	Registered Traveller Programme
RTT	Round Trip Time
RTU	Remote Terminal Unit
SaaS	Software as a Service
SALPA	Salaiset Pakkokeinot
SCADA	Supervisory Control And Data Acquisition
SDS	Short Data Services
SE	Systems Engineering
SEPA	Single Euro Payment Area
SHA	Secure Hash Algorithms
SIS	Software-Intensive Systems
SLA	Service Level Agreements
SME	Small and Medium Enterprise
SMS	Short Message Service
SOA	Service Oriented Architecture
SoI	System of Interest
SoSE	System of Systems Engineering
SOTA	State Of The Art
SRL	System Readiness Level
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCCA	TETRA + Critical Communications Association
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio
TFTP	Terrorist Finance Tracking Program
TMSI	Temporary Mobile Subscriber Identity
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicles

UMTS	Universal Mobile Telecommunications System
UNIFI	Universities Finland
VfM	Value for Money
VHF	Very High Frequency
VIRVE	Viranomaisverkko
VPN	Virtual Private Networks
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WSEAS	World Scientific and Engineering Academy and Society

LIST OF FIGURES

FIGURE 1 Applied research methodology: Embedded multiple-CSR in DSR framework 27
FIGURE 2 Scopes of empirical R&D projects 35
FIGURE 3 Software-intensive systems layers 41
FIGURE 4 Four-tier access control model 47
FIGURE 5 Components of a satellite-based tracking system 57
FIGURE 6 Model for identifying technical threats of satellite-based tracking 59
FIGURE 7 Miniaturizing levels in tracking sensor development 64
FIGURE 8 Simultaneous utilization of parallel communication channels 68
FIGURE 9 Key market drivers and restraints of first responders' communications, command and control and intelligence market 74
FIGURE 10 ITIL V3 – Service lifecycle 82
FIGURE 11 Selective sourcing 86
FIGURE 12 Supplier offerings vs. in-house capability sourcing 87
FIGURE 13 Summary of literature review from SIS point of view 89
FIGURE 14 Operational environment 91
FIGURE 15 System for transparent surveillance 95
FIGURE 16 Idea behind the reference architecture 103
FIGURE 17 Blueprint of DSiP network solution 114
FIGURE 18 Multi-user DSiP network solution 116
FIGURE 19 Four standardization layers of ERVs 120
FIGURE 20 Selective sourcing, RACI matrixes, SLA's and ESM at the different phases of service strategy 130
FIGURE 21 SIS model for law enforcement tracking systems 134
FIGURE 22 Multi-use of law enforcement sensor data 135
FIGURE 23 Finnish ERV-related R&D projects 166

LIST OF TABLES

TABLE 1 Units of analysis of case studies 34
TABLE 2 Design science research tasks of this study 34
TABLE 3 Data categories of empirical R&D projects 36
TABLE 4 Research data 36
TABLE 5 Generic SE life-cycle stages 39
TABLE 6 Design rules for dynamic complexity in the design for IIs 42
TABLE 7 Public safety organizations and functions 44
TABLE 8 Technical vulnerabilities in satellite-based tracking systems . 60
TABLE 9 RACI example 83
TABLE 10 Stakeholders and their needs/benefits/applications 139

CONTENTS

ABSTRACT
ACKNOWLEDGEMENTS
GLOSSARY
LIST OF FIGURES
LIST OF TABLES
CONTENTS
LIST OF INCLUDED ARTICLES
PUBLICATION FORUMS
AUTHOR'S CONTRIBUTIONS
OTHER PUBLICATIONS AND PUBLIC PRESENTATIONS

1 INTRODUCTION 21
1.1 Background and research environment 21
1.1.1 EU's secure societies challenges research 22
1.2 Objectives and scope 23
1.2.1 The coherent whole of the study 23
1.2.2 Research questions 25
1.3 Research approach 26
1.3.1 Applied DSR and Service Design methodology 28
1.3.2 Applied CSR methodology 29
1.3.3 Design of case study research 30
1.4 Research process and dissertation structure 32
1.4.1 Empirical data sources 35
1.4.2 Dissertation structure 36

2 THEORETICAL FRAMEWORK 37
2.1 Designing of socio-digital systems 38
2.1.1 Systems engineering 38
2.1.2 Designing software-intensive systems 40
2.1.3 Design principles for information infrastructures 41
2.2 Law enforcement 44
2.2.1 Overview of public safety functions 44
2.2.2 Border protection and LEAs' cross-border operations 46
2.2.3 Law enforcement technology services 48
2.2.4 ENLETS 49
2.2.5 Coercive measures and technical tracking 51
2.2.6 Monitoring-of-legality 52
2.2.7 Emergency response vehicles 52
2.3 GNSS-based tracking systems 56
2.3.1 Risks of commercial GNSS 58
2.3.2 GNSS technology for law enforcement 61
2.3.3 Sensors for tracking non-cooperative targets 62

2.3.4 Enabling technologies for GNSS sensors 63
2.4 Communication systems 65
2.4.1 Technical threats to mobile communications 67
2.4.2 Multichannel communications 68
2.4.3 Cyber-security 70
2.4.4 Interoperability and the multi-organizational environment 71
2.4.5 Communication concept of the Finnish government 72
2.5 Command & control and intelligence 73
2.5.1 Remote operations and monitoring 74
2.5.2 Surveillance: security or an invasion of privacy 75
2.5.3 Digital forensics 78
2.5.4 Digital evidence 80
2.6 IT service governance 82
2.6.1 ITIL—continuous service improvement 82
2.6.1.1 RACI model 82
2.6.2 Enterprise service management 84
2.6.3 Utility based computing 85
2.6.4 Selective sourcing 86
2.6.5 SLA based management 87
2.7 Conclusions of the theoretical framework 88

3 RESEARCH CONTRIBUTIONS 90
3.1 Operational environment 90
3.1.1 Cross-border operations 92
3.1.2 Secure mobile communications 92
3.2 Social acceptance of technical surveillance 93
3.2.1 Transparency of surveillance 93
3.2.2 New solution for transparent and efficient surveillance 94
3.2.3 Discussion of Study II 96
3.3 LEAs' legal digital evidence gathering 97
3.3.1 Requirements for the monitoring system 98
3.3.2 Possibilities of new digital services for crime prevention 99
3.3.3 Legislative and political view 100
3.3.4 Discussion of Study III 101
3.4 The reference architecture and stakeholders' needs 102
3.4.1 Reference architecture 103
3.4.1.1 GNSS sensors 103
3.4.1.2 Future Monitoring System (FMS) 103
3.4.1.3 Data flow and communication channels 105
3.4.2 Stakeholder needs 106
3.4.2.1 Citizens 106
3.4.2.2 Targets 106
3.4.2.3 Authorities 107
3.4.2.4 Manufacturers and service providers 108
3.4.2.5 Policy makers, legislators and funding agencies 108

3.4.3 Discussion of Study IV ... 109
3.5 Cyber-secure communications ... 110
3.5.1 Distributed Systems intercommunication Protocol—DSiP .. 111
3.5.2 Quality of service and cyber-secure communications ... 112
3.5.3 Key elements and functionalities of DSiP ... 113
3.5.4 Discussion of Study V ... 116
3.6 Mobile digital services for law enforcement ... 117
3.6.1 Why mobile digital services for border protection? ... 118
3.6.2 Emergency response vehicles and their standardization aspects ... 119
3.6.3 Discussion of Study VI ... 121
3.7 Designing the future emergency response vehicle ... 122
3.7.1 End-user and market needs ... 123
3.7.2 Solution approach ... 124
3.7.3 Communications layer ... 125
3.7.4 Service platform and digital services ... 126
3.7.5 Discussion of Study VII ... 127
3.8 IT service governance model for PPDR organizations ... 129
3.8.1 Benefits of the new framework ... 131
3.8.2 Discussion of Study VIII ... 132
3.9 Cross-case conclusions ... 132
3.9.1 Understanding satellite-based tracking systems for law enforcement ... 132
3.9.2 Model for future law enforcement intelligence system ... 134

4 DISCUSSION ... 136
4.1 Additions to the knowledge base ... 136
4.2 Applications in the appropriate environment ... 139
4.3 Audit of the study ... 140
4.3.1 Design science research quality ... 141
4.3.2 Validity and reliability of case study research ... 141
4.3.2.1 Construct Validity ... 142
4.3.2.2 Internal Validity ... 142
4.3.2.3 External Validity ... 143
4.3.2.4 Reliability ... 144
4.4 Recommendations for future research ... 144

YHTEENVETO (FINNISH SUMMARY) ... 147

REFERENCES ... 149

APPENDIX A: RESEARCH AND DEVELOPMENT PROJECTS ... 163

INCLUDED ARTICLES

LIST OF INCLUDED ARTICLES

[PI] Jyri Rajamäki and Pasi Kämppi. Mobile Communications Challenges to Cross-border Tracking Operations Carried out by Law Enforcement Authorities. *International Conference on Information Networking (ICOIN)*, 2013, 560-565.

[PII] Jyri Rajamäki, Jutta Tervahartiala, Sofia Tervola, Sari Johansson, Leila Ovaska and Paresh Rathod. How transparency improves the control of law enforcement authorities' activities?" *The European Intelligence and Security Informatics Conference (EISIC)*, 2012, 14-21.

[PIII] Jyri Rajamäki & Juha Knuuttila. Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement. *The European Intelligence and Security Informatics Conference (EISIC)*, 2013, 198-203.

[PIV] Jyri Rajamäki. Satellite based tracking systems for better law enforcement: a systems engineering exploratory research via a multiple case study analysis. *WSEAS Transactions on Systems and Control.* [In review]

[PV] Jyri Rajamäki, Paresh Rathod & John Holmström. Decentralized Fully Redundant Cyber Secure Governmental Communications Concept. *The European Intelligence and Security Informatics Conference (EISIC)*, 2013, 176-181.

[PVI] Jyri Rajamäki. Mobile Digital Services for Border Protection: Standardization of Emergency Response Vehicles. *The European Intelligence and Security Informatics Conference (EISIC)*, 2013, 256-261.

[PVII] Jyri Rajamäki. The MOBI Project: Designing the Future Emergency Service Vehicle. *IEEE Vehicular Technology Magazine*, vol.8, no.2, June 2013, 92-99.

[PVIII] Jyri Rajamäki and Markus Vuorinen. Multi-supplier integration management for public protection and disaster relief (PPDR) organizations. *International Conference on International Conference on Information Networking (ICOIN)*, 2013, 499-504.

PUBLICATION FORUMS

All eight publications have been quality-classified by the Publication Forum initiative of the Universities Finland UNIFI. PII, PIII, PV and PVI were reviewed by the IEEE Computer Society. PI and PVIII were reviewed by the Korean Institute of Information Scientists and Engineers (KIISE) and the IEEE Computer Society. PIV is in the review process of the WSEAS Transactions on Control and Systems. PVII was reviewed by the IEEE Vehicular Technology Society.

AUTHOR'S CONTRIBUTIONS

This section gives the author's contribution to the content of the included publications. I was the main author of all the eight publications.

PI was written jointly with Pasi Kämppi. Mr. Kämppi studied technical vulnerabilities of satellite-based tracking, as discussed in Chapters III and IV of the paper. I contributed the rest, assembled it and presented the paper at the International Conference on Information Networking (ICOIN), January 28–30, 2013, Bangkok, Thailand. My contribution to the publication was 60%.

PII was written jointly with my master's students Jutta Tervahartiala, Sofia Tervola, Sari Johansson and Leila Ovaska, and my colleague Paresh Rathod. I presented the idea behind PII for the first time at the "Security in Futures – Security in Change" conference, June 3–4, 2010, in Turku, Finland [1]. The student authors wrote part of the literature review and conducted other of the polls presented in Chapter IV. Mr. Rathod provide comments and editing. Ms. Tervahartiala, Ms. Tervola and Ms. Johansson presented the paper PII at the Intelligence and Security Informatics Conference, August 22–24, 2012, in Odense, Denmark. My contribution to the publication was 60%.

PIII was written jointly with Juha Knuuttila. Lic. Sc. Knuuttila gave valuable comments, especially from legislative and political perspective. He also presented the paper at the Intelligence and Security Informatics Conference, August 12-14, 2013, in Uppsala, Sweden. My contribution to the publication was 80%.

PV was written jointly with John Holmström and Paresh Rathod. PV is based on my Plenary lecture "Decentralized cyber secure public safety communications and information management systems for a multi organizational environment" at the 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12), April 18–20, 2012, in Rovaniemi, Finland. Mr. Holmström gave technical details about DSiP protocol and helped create the figures. Mr. Rathod gave comments, helped edit and presented the paper PV at the Intelligence and Security Informatics Conference, August 12–14, 2013, in Uppsala, Sweden. My contribution to the publication was 60%.

PVIII was written jointly with my student Markus Vuorinen. I supervised his master's thesis on IT governance models for private companies. I analyzed his thesis' content from public organizations' point of view and edited the paper. Mr. Vuorinen presented the paper at the International Conference on Information Networking (ICOIN), January 28–30, 2013, in Bangkok, Thailand. My contribution to the publication was 50%.

---

1 Jouni Viitanen, Pasi Patama, Juha Knuuttila, Jyri Rajamäki and Harri Ruoslahti, "Towards transparent authority of power in law enforcement: Is there a choice for Big Brother" presentation slides available at: http://www.futuresconference.fi/2010/presentations/ws4-Viitanen_Patama_Knuuttila_Rajamaki_Ruoslahti.pdf

OTHER PUBLICATIONS AND PUBLIC PRESENTATIONS

The author has also contributed to several other studies that touch on the topic of this thesis. The results of these studies were presented and published in the following conferences and publications:

Invited plenary lectures

Rajamäki, J. 2014. Multi-Agency Cooperation in Cross-border Operations. *The 8th International Conference on Circuits, Systems, Signal and Telecommunications (CSST '14).*

Rajamäki, J. 2013. Future Emergency Vehicles' ICT Services. *The 2nd International Conference on Information Technology and Computer Networks (ITCN '13).*

Rajamäki, J. 2012. Decentralized cyber secure public safety communications and information management systems for a multi organizational environment. *The 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE'12).*

Rajamäki, J. 2011. Vulnerabilities in Satellite-Based Tracking Systems. *The 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11).*

Books

Rajamäki, J., Pirinen, R. & Knuuttila, J. (Eds.) 2012. SATERISK - Risks of Satellite-Based Tracking: Sample of Evidence Series. Vantaa: Laurea-University of Applied Sciences, Leppävaara Unit.

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.

Tikanmäki, I., Rajamäki, J. & Pirinen, R. (Eds.) 2014. MOBI - Mobile object buss interaction: Sample of Evidence Series. Vantaa: Laurea-University of Applied Sciences, Leppävaara Unit.

Peer-reviewed scientific articles

Rajamaki, J. 2012. Cross-border satellite-based tracking: Needs, Approach, Benefits and Competition. *Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS)*, 1-8.

Rajamäki, J. & Viitanen, J. 2013. Law enforcement authorities' special requirements for GNSS. *Proceedings of the 6th GNSS Vulnerabilities and Solutions Conference* , 135-146.

Rajamäki, J., Rathod, P. & Kämppi, P. 2013. Hybrid Multi-channel and Redundant Tracking System in Emergency Response. *Recent Advances in Computer Science and Networking*, 177-182.

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*. Vol. 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.* Vol.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* Vol.8, 76-83.

Rajamäki, J., Timonen, T., Nevalainen, J., Uusipaavalniemi, H., Töyrylä, T. & Arte, E. 2014. Human-machine Interactions in Future Police Vehicles: Applying Speech User Interface and RFID Technology. *International Journal of Systems Applications, Engineering & Development*. Vol.8, 163-170.

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.

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.* Vol.8, 244-251.

Happonen, M., Viitanen, J., Kokkonen, P., Ojala, J. & Rajamäki, J. 2009. Jamming detection in the future navigation and tracking systems. *Proc. 16th Saint Petersburg International Conference of Integrated Navigation Systems*, 314-317.

Holmström, J., Rajamäki, J. & Hult, T. 2011. The future solution and technologies of public safety communications–DSiP traffic engineering solution for secure multichannel communication. *International Journal of Communication.* Issue 3, Vol.5, 155-122.

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

Lehto, J., Rajamäki, J. & Rathod, P. 2012. Cloud computing with SOA approach as part of the disaster recovery and response in Finland. *International Journal of Computers and Communications* 6 (1), 175-182.

Pirinen, R., Rajamäki, J. & Aunimo, L. 2008. Rescuing of Intelligence and Electronic Security Core Applications (RIESCA). *WSEAS Transactions on Systems* 7 (10), 1080-1091.

Tuohimaa, T., Tikanmäki, I., Rajamäki, J., Viitanen, J., Patama, P., Knuuttila, J. & Ruoslahti, H. 2011. Is Big Brother Watching You? *International Journal of Systems Engineering, Applications and Development* 5 (5), 602-609.

Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. 2010a. Near border procedures for tracking information. *WSEAS Transactions on Systems* 9 (3), 223-232.

Viitanen, J., Patama, P., Rajamäki, J., Knuuttila, J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. 2012a. How to create oversight in intelligence surveillance. *Proceedings of the 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications* (ELECTROSCIENCE'11), 52-56.

1 INTRODUCTION

1.1 Background and research environment

Broadly speaking, law enforcement (LE) refers to any order to enforce the law in an organized manner. LE has two main goals. First, it seeks to prevent the occurrence of a crime that will do damage to another human being or to society as a whole. Second, it will see that suspected criminals are tried in a manner that is in compliance with local laws. Various LE officials will also assign some form of punishment or imprisonment that is considered equitable for the type of crime committed, while also seeking the rehabilitation of criminals when and as possible. Critical infrastructure consists of the assets, systems, and networks, whether physical or virtual, so vital to the society that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. LE is a critical infrastructure for nation's economy, security and health. Law enforcement agencies/authorities (LEAs) continue to develop and acquire joint systems and deliver needed capabilities to enforce the law. With an objective to improve and mature the information acquisition process, LEAs need new and creative methodologies to procure these technically complex systems.

With the emergence of an international warehouse of crime, organized crime is a real threat in Europe. International terrorism has also evolved into a more threatening problem. There is a strong relationship between public fear of terrorism, and the willingness of the public to give more rights to the authorities for increased security (Elvy 2011). Data protection laws do not always offer sufficient protection against threats stemming from the use of new technologies and modes. The importance of security increased dramatically due to fear caused by terrorist attacks. The cutting-edge security measures in use now have not been properly debated nor have their social implications been studied. The most efficient security practices are often regarded as threats to privacy, and civilians are afraid of being suspect. It is common to think that more security means less privacy and more privacy means less security. Such feelings of insecurity lead a majority of citizens to give up their privacy in order to obtain more security (Coudert 2010). Informational control requires a high level of transparency regarding data gathering and information processing (Wood et al. 2006). In investigations of criminal networks, there are four common problem sources: resources, amount of information, information complexity, and information sharing (Petersen & Wiil 2011). On the other hand, law enforcement authorities are constantly seeking new technological recording, retrieving and monitoring solutions to facilitate their combat against criminal organizations. To help LEAs' struggle against criminals, the European Union is backed by anti-terrorism legislation (Terrorist Offences Act 2005) that requires telecommunication operators to preserve phone data and Internet logs for a minimum of six months . In 2014, the European Court of Justice ruled that this Act violated the privacy rights of individuals.

A satellite-based tracking sensor calculates its own position and sends this information for post-processing via a mobile telecommunications infrastructure. Some new sensors support various systems — such as NAVSTAR Global Positioning System (GPS), Globalnaja navigatsionnaja sputnikovaja sistema (GLONASS), Beidou/Compass, Galileo and Iridium — so that several techniques may be used simultaneously to guarantee better positioning accuracy and availability (Rajamäki, Rathod & Kämppi 2014). Satellite-based tracking is used in many applications, such as in logistics, fleet management, road tolls and traffic signal management. Also, LEAs are using these systems, for example, for tracking their own troops in the field as well as tracking suspects and drug lots.

Organized crime is aware that LEAs are gathering information about them, their actions and their whereabouts. Criminals have learned to detect a car tailing them in traffic. For that reason, satellite-based tracking is a good tool for LEAs: a small sensor installed under the car is harder to detect than a tailing car. Unfortunately, criminals are learning; they have learned to check their vehicles and use other countermeasures. Therefore, LEAs needs better tracking sensors that are resilient to these countermeasures (Rajamäki & Viitanen 2013).

1.1.1 EU's secure societies challenges research

The European Commission has announced Horizon 2020, an €80 billion program for investment in research and innovation. Horizon 2020 brings together all EU research and innovation funding under a single program. It focuses on turning scientific breakthroughs into innovative products and services that provide business opportunities and change people's lives for the better (European Commission 2011).

For the EU's secure societies challenges, the research priorities of Horizon 2020 are about protecting European citizens, society and economy, assets, infrastructures and services, while not forgetting prosperity, political stability and well-being. In 2013, organized crime and mobile organized crime groups were considered to be some of the biggest challenges for EU internal security to address (European Commission 2013a). One of the key research areas in the secure societies theme of Horizon 2020 is to fight against crime and terrorism. For example, the research topic FCT-05-2014 concerns itself with novel monitoring systems and miniaturized sensors that improve LEAs' evidence- gathering abilities:

> Investigations on the activities of criminal organizations usually require Law Enforcement Agencies (LEAs) to use electronic equipment for legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way, while keeping for both the sensors part and the monitoring station all the legal, integrity and chain-of-custody requirements that will enable the presentation of evidences obtained this way at the Courts of Justice.
>
> Requirements for this equipment are very different from those offered by available commercial devices. Depending on the operation, the periods of time that these electronic devices have to work can range from days to months or in real time. Access to the device could be limited or impossible. Secure remote operation over radio channel (or other type of communication channel, including GSM networks) should be possible. Other requirement may apply like small size for easy concealment, low power consumption for extended time life, robustness and self-protection in addition to strong authentication mechanisms for operators and protection of the communication channels.[2]

1.2 Objectives and scope

The scope of this study is to collect together the research results from four different research projects with regard to the tracking of non-cooperative targets by LEAs, to understand the phenomena and to make suggestions on how to improve European law enforcement.

1.2.1 The coherent whole of the study

The first article, "Mobile communication challenges to cross-border tracking operations carried out by law enforcement authorities," presents the operational environment in which LEAs use tracking systems and the major challenges they face: (1) tracking sensors: commercial sensors do not fulfill the needs of LEAs; (2) cross-border operations: criminal activities have become internationalized, but LEAs are national organizations; (3) secure mobile communications: this is becoming increasingly important in all operations; (4) digital evidence: surveillance data should fulfill chain-of-custody requirements and (5) transparency: it enables societal acceptance and monitoring-of-legality. The article also discusses the second and third challenges.

The second article, "How transparency improves the control of law enforcement authorities' activities?" presents the idea behind the reference architecture of future satellite-based tracking systems for better law enforcement. Then, the second article goes through the fifth challenge: how transparency improves the social acceptance and monitoring-of-legality. This is a fairly topical

2 FCT-05-2014 [online] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/ h2020/topics/1105-fct-05-2014.html

issue at the moment; see for example the following excerpts from the leading Finnish newspaper:

> The operations of the drug enforcement division of the Helsinki Police Department have not been monitored properly, Helsingin Sanomat reports citing over 70 official sources. A former member of the division, for example, views that the division is allowed additional leeway due to its effectiveness. In addition, several sources claim that the division turns a blind eye to crimes committed by its informants. [3]

> A bribery investigation has fuelled persistent rumours about methods of the Helsinki drug squad. CHIEF of the Helsinki Police Department Jukka Riikonen has dismissed claims by Helsingin Sanomat that the operations of the department's drug squad are monitored insufficiently. "Operations of the Helsinki Police Department, including the operations of the drug squad, are in compliance with guidelines and regulations, and endure any third-party judicial review," Riikonen emphasised to the daily on Tuesday afternoon. He also pointed out that no grounds for reprimand were found when the squad was last subjected to a standard review last year. Similarly, the Office of the Prosecutor General says that thus far no reason to suspect that the police command has neglected its supervisory duties has surfaced in the ongoing investigation into Jari Aarnio, the chief of the drug squad. Citing over 70 informed sources, Helsingin Sanomat suggested earlier that the practices of the drug squad, especially regarding informants, are dubious. Several sources interviewed by the daily claimed, for example, that the squad has turned a blind eye to crimes committed by its informants. A high-ranking police officer, in turn, viewed that the command has never been able to monitor the activities of the squad. Similar claims have also emerged previously but have been shrugged off by the Helsinki Police Department as jealousy within the police organisation. Meanwhile, STT believes Aarnio's close relationship with a high-ranking member of the outlaw gang United Brotherhood was discussed on an official level already six years ago – at least at the Office of the Prosecutor General and the Ministry of the Interior's Police Department. Yet, Mikko Paatero, the National Police Commissioner, has said that he was surprised to learn about the relationship. Information obtained from the Trade Register indicates that Trevoc, the surveillance equipment manufacturer embroiled in the probe into Aarnio, is partially owned by a company founded by the gang member's sister. Aarnio was detained on Friday on suspicion of, for example, accepting bribes from Trevoc. The company has supplied surveillance equipment to at least the Helsinki Police Department, the Finnish Customs, the Ministry for Foreign Affairs and the Finnish Security Intelligence Service.[4]

The third article, "Law enforcement authorities' legal digital evidence gathering: legal, integrity and chain-of-custody requirement," researches the fourth challenge: how the digital surveillance data LEAs collect could be valid in the court. Proposals for better law enforcement should ensure that the new technologies must be such that they can be upheld in the courts of justice.

The fourth article, "Satellite based tracking systems for better law enforcement: a systems engineering exploratory research via a multiple case study analysis," reviews the current commercial or "homemade" types of tracking sensors and systems and their communication channels for law enforcement field operations. It explores new technologies that have not yet been applied in

---

3 Daily: Helsinki drug squad not monitored properly, *Helsinki Times*, 19 Nov 2013. http://www.helsinkitimes.fi/finland/finland-news/domestic/8419-daily-helsinki-drug-squad-not-monitored-properly.html

4 Chief of Helsinki Police denies leeway claims, *Helsinki Times*, 21 Nov 2013. http://www.helsinkitimes.fi/finland/finland-news/domestic/8430-chief-of-helsinki-police-denies-leeway-claims.html

tracking non-cooperative targets. It presents the reference architecture for a better tracking system. It also examines the needs of stakeholders of tracking sensors of a new type, a monitoring station and their associated communication channels in the field, taking into account the societal acceptance of the proposed solutions.

The fifth article, "Decentralized fully redundant cyber secure governmental communications concept," continues to research the third challenge. It also explains how to integrate the needed communication systems of LE sensors with other telecommunication systems.

The sixth article, "Mobile digital services for border protection: standardization of emergency response vehicles," focuses on law enforcement in the field of border protection. It demonstrates how the digital services that LEAs need, such as monitoring by sensors, could be brought to the field via their emergency response vehicles (ERVs). It shows the need to integrate the sensor-monitoring systems with the existing systems and presents the "OSI reference model"[5] for LE vehicles.

The seventh article, "The MOBI project: designing the future emergency service vehicle," widens the ERV concept presented in the sixth article to include first responders (FRs) other than just LEAs. This "out-of-the-silos" thinking enables new business models for public protection and disaster relief (PPDR) organizations with their equipment and service providers. PPDR organizations will also promote innovation and competition between equipment providers in terms of provision of user functionality, interoperability and services to actively support delivery of front line services. The article also presents the demo vehicle employed within the study and the lessons learned from it.

The eighth article, "Multi-supply integration management for public protection and disaster relief (PPDR) organizations," researches how PPDR organizations, such as LEAs, should choose their service delivery models for new digital services, such as tracking systems.

1.2.2 Research questions

The dissertation includes one main research question, which is additionally focused by eight expanded and iterative research questions in eight studies in which the research questions of each study produced more detailed insight into the main research question. In this dissertation, the main research question is:

> RQ: How can new types of satellite-based tracking sensors, mobile monitoring stations and their associated communication channels for law enforcement (LE) operations be understood and designed, taking into account the chain-of-custody and monitoring-of-legality requirements?

The eight expanded and iterative research questions are:

---

5 The Open System Interconnecting model (OSI) is a conceptual model that characterizes and standardizes the Internet functions of a communication system by partitioning it into abstraction layers.

RQ1: How can the operational environment be understood and categorized, where law enforcement authorities (LEAs) use tracking equipment for legal recording, retrieving and monitoring of criminal activities?

RQ2: How can LEAs' monitoring-of-legality actions and social acceptance of the use of tracking equipment be improved?

RQ3: How can investigation data also be used as digital evidence in the courts of justice?

RQ4: How can the state-of-the-art (SOTA) reference architecture for a new LE tracking system be designed, and how can its main stakeholders and their needs be understood and categorized?

RQ5: How can global cyber-secure communication channels be created for LEAs and their sensors, taking into account interoperability with existing systems and economic issues?

RQ6: How can the digital services (e.g. mobile monitoring of sensors) LEAs need be effectively brought to the field, taking into account interoperability of systems and economic issues?

RQ7: How can LEAs' core services be guaranteed with significantly reduced budgets?

RQ8: How can LEAs manage the multi-supply environment of their new ICT systems?

1.3 Research approach

This section presents the research approach and methodology of the dissertation. The research approach is based on a combination of the science of designing software-intensive systems (SIS) with systems thinking and a generic label of information infrastructures (IIs). Systems engineering (SE) has a long history within the development of critical systems. We can find examples demonstrating the use of effective engineering and engineering management as well-defined processes, as either well applied or as poorly applied (Kinzig 2010). Throughout the many decades over which systems engineering emerged as a discipline, many practices, methods, heuristics and tools were developed, documented, and applied (Kinzig 2010). The challenges of building large-scale SIS are unique and very different from the challenges of building large physical systems (Brady 2000, Hevner & Chatterjee 2010). A satellite-based tracking system for law enforcement is a complex system of systems. It consists of different socio-digital systems, such as public safety functions, law enforcement technology services, satellite-based tracking systems, communication systems and command, control and monitoring systems. All these systems have many stakeholders with different requirements. One stream of research that has addressed the challenges of realizing complex socio-digital systems as new types of IT artifacts is the II literature (Hanseth & Lyytinen 2010, Monteiro & Hanseth 1996, Star & Ruhleder 1996, Edwards et al. 2009, Hanseth 2002).

The chosen research approach is the design science research framework of Hevner et al. (2004) supplemented by embedded multiple-case study analysis, as shown in Figure 1.

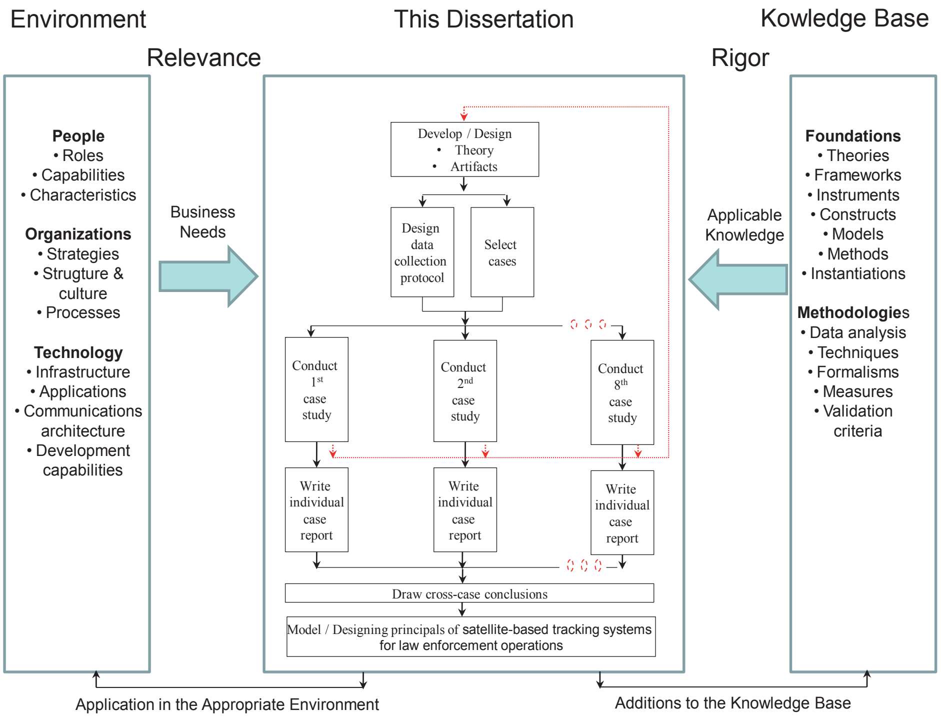


FIGURE 1 Applied research methodology: Embedded multiple-CSR in DSR framework

For this study, the combination of design science research (DSR) and case study research (CSR) was the rational choice as the research approach. The main research question here is: **How** can new types of satellite-based tracking sensors, mobile monitoring stations and their associated communication channels for law enforcement (LE) operations be understood and *designed,* taking into account the chain-of-custody and monitoring-of-legality requirements? Considering the setting of this study, the case study analysis approach seemed suitable for providing answers to our research questions on "how" (Yin 2009, Benbasat, Goldstein & Mead 1987). In this research setting, the focus is on understanding (= CSR part) critical systems as a basis for designing (= DSR part) new software-intensive artifacts.

1.3.1 Applied DSR and Service Design methodology

Design science research (DSR) traces its roots to pragmatism and the sciences of the artificial (Simon 1978, Haack 1976). For the pragmatist, truth and utility are indistinguishable as truth lies in utility. Thus, for DSR, the relevance is evaluated by the utility provided to the organization and developers. Thus DSR must pass both the tests of science and practice (Markus, Majchrzak & Gasser 2002). The Information Systems Framework (Hevner et al. 2004) presents a conceptual framework for understanding, executing, and evaluating information systems (IS) research that combines the behavioral science and design science paradigms. Different terms have been used to describe this mode of research, including Design Science and Design Research (Hevner et al. 2004). DSR consists of activities concerned with the construction and evaluation of technological artifacts to meet organizational needs as well as the development of their associated theories. Hevner and Chatterjee (2010) define DSR as follows:

> Design science research is a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem.

One set of guidelines for conducting and evaluating DSR is the seven criteria (Hevner et al. 2004) that are summarized in the following:

1. Design as an artifact: Design research must produce a viable artifact in the form of a construct, a model, a method or an instantiation.
2. Object: The object of design research is to develop technology-based solutions for important and relevant business problems.
3. Via execution: The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation plans.
4. Research contributions: Effective design research must provide clear and verifiable contributions in the areas of the design artifact, design foundations and/or design methodologies.
5. Research rigor: Design research relies on the application of rigorous methods in both the construction and evaluation of the design artifact.
6. Design as a search process: The search for an effective artifact requires utilizing the available means to reach desired ends while satisfying laws in the problem environment.
7. Communication of research: Design research must be presented effectively to both technology-oriented as well as management-oriented audiences.

DSR must necessarily make a dual contribution to epistemic and practical utility. Any piece of research must add to existing theory in order to make a worthwhile scientific contribution and the research should assist in solving the practical problems of practitioners, specifically problems that are either current or anticipated. DSR consists of activities concerned with the construction and evaluation of technology artifacts to meet organizational needs as well as the development of their associated theories. In brief, behavioral science is concerned with theories that explain human or organizational behavior, while DSR is concerned with creating new and innovative artifacts (Hevner et al. 2004).

The earliest contributions of Service Design from the perspective of the marketing and management disciplines are connected to Shostack's (1982) article "How to Design a Service." It describes the integrated design of material components, namely products and immaterial components services. A design process can be documented and codified using a "service blueprint" to map the sequence of events in a service and its essential functions in an objective and explicit manner. Effective service marketing requires the recognition of the complex combination of products and services that make up a simple service (Shostack 1982). The review "Services as Subject Matter for Design" further articulates Shostack's work and presents methods of service design (Mager 2004). The Service Design Network was launched by Köln International School of Design in 2004. Currently, the international service design network (from the perspective of marketing and management) extends to service designers around the world, professional service design agencies and educational institutions such as Laurea University of Applied Sciences. The Service Design of IS action is mainly based on the ITIL v.3 (The Information Technology Infrastructure Library 2007), and it describes Service Design's principles, processes, technology-related activities, tools, implementation and risks.

1.3.2 Applied CSR methodology

According to Gerring (2007), the term "case" connotes a spatially delimited phenomenon, as a unit, observed at a single point in time or over a period of time. Gerring continues, claiming that the case comprises the type of phenomenon that an inference attempts to explain (cf. Yin 1994). In this dissertation, each individual case provides a single observation or multiple ones within case observations and evidence (Miles & Huberman 1994, Yin 2009, Gerring 2007).

According to Yin (2009), case study research brings an understanding of a complex issue or object, and can extend experience or add strength to what is already known through previous research (cf. Miles & Huberman 1994). Case studies emphasize detailed contextual analysis of a limited number of events or conditions and their relationships when the relevant behavior cannot be manipulated (Yin 2009). As the setting of study, according to a continuum of methodological work, a case study is a strategy for doing research that involves an empirical investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence (Yin 1994, Miles & Huberman 1994, Eisenhardt 1989, Yin 2009). Yin (2009) defines the scope of a case study as follows:

> A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident.

According to Yin (2009), this technical definition includes the logic of design that distinguishes case studies from other research methods (see also (Eisenhardt 1989, George & Bennett 2005, Gerring 2007, Laine, Bamberg & Jokinen 2007, Miles & Huberman 1994, Stake 1995). According to Yin (2009), the case study inquiry: (1) copes with the technically distinctive situation in which there will be many more variables of interest than data points; (2) relies on multiple sources of evidence, with data needing to converge in a triangulation fashion; and (3) benefits from the prior development of theoretical propositions to guide data collection and analysis.

There are four types of triangulation in evaluations: the triangulation of data sources as data triangulation, that among different evaluators as investigator triangulation, that of perspectives on the same data set as cal triangulation and methods as methodological triangulation (Campbell & Fiske 1959, George & Bennett 2005, Lincoln & Guba 1985, Robson 2002, Stake 1995, Yin 2009).

Robson (2002) interprets case studies in the context of social research. Its issue concerns what kinds of generalizations are possible from the case and how this might be done. It is focused on a phenomenon in context, typically in situations where the boundary between the phenomenon and its context is not clear, and is undertaken using multiple methods, appropriate data collection and triangulation.

According to Eisenhardt (1989), CSR can be defined as a research strategy which focuses on understanding the dynamics present within single settings. CSR is then said to be suitable for research seeking to answer "how" and "why" questions (Yin 1994 and 2009). Yin (2009) continues that the "how" and "why" questions in case studies have a distinct advantage when asked about a contemporary set of events, over which the investigator has little or no control.

Robson (2002) states that a case study is a well-established research strategy where focus is on a case which is interpreted widely to include the study of an individual, a group, a setting, an organization and so forth in its own right. Robson (2002) continues and remarks that case studies opt for analytic rather than statistical generalization, which means that they develop a theory which can help researchers understand other similar cases, phenomena or situation.

According to Gerring (2007), a case study is an intensive study of a single case for the purpose of understanding a larger class of similar units and its synonyms are: single-unit study, single-case study and within-case study. Gerring (2007) continues that cross-case study refers to a large-sample study where the sample consists of multiple cases representing the same units that comprise the central inference.

1.3.3 Design of case study research

Yin (2004) identifies five components of research design for case studies: (1) the questions of the study; (2) its propositions, if any; (3) its unit(s) of analysis; (4) the logic linking the data to the propositions; and (5) the criteria for interpreting the findings. According to Gerring (2007), a case study research design may also refer to a work that includes several case studies —for example comparative-historic analysis or comparative method. Yin (2009) emphasizes that the unit of analysis defines what the case is and that the main unit of analysis is likely to be at the level being addressed by the main study question, which is followed by linking the data to propositions and the criteria for interpreting the findings.

Yin (2009) states that multiple-case studies should follow replication logic and selected cases should serve in a manner similar to multiple experiments. Yin (2009) presents the replication approach to multiple-case studies.

The interior part of Figure 1 shows how CSR is applied in this research. The initial step in designing CSR consists of theory development, and the next steps are case selection and definition of specific measures in the design and data collection process. Each individual case study consists of a whole study, and then conclusions of each case are considered to be the replication by other individual cases. Both the individual case and the multiple-result should be the focus of a summary report. For each individual case, the report should indicate how and why a particular result is demonstrated. Across cases, the report should present the extent of replication logic, including certain and contrasting results (Yin, 2009).

Yin (2009) notes that the simplest multiple-case design would be the selection of two or more cases that are believed to be literal replications; a more complicated multiple-case design would result from the number and types of theoretical replications. He suggests five to six or more replications for a higher degree of certainty.

According to Yin, the general characteristics of research designs serve as a background for considering four types of specific designs for case study: (1) single-case (single unit of analysis —holistic), (2) single-case (multiple units of analysis —embedded), (3) multiple-case (single unit of analysis —holistic) and (4) multiple-case (multiple units of analysis—embedded). For him, single cases are a common design for doing case studies, especially under certain conditions where the case represents: (1) a critical test of existing theory; (2) a rare or unique circumstance or (3) a representative or typical case, or where the case serves (1) revelatory or (2) longitudinal purposes. He maintains that a single case study should follow sampling logic.

In Figure 1, the dashed-line feedback represents a discovery situation, where one of the cases does not suit the original multiple-case study design. Such a discovery implies a need to reconsider the original theoretical propositions. At this point, redesign should take place before proceeding further, and in this view the replication approach represents a way of generalizing that uses a type of test called falsification or refutation, which is the possibility that a theory or hypothesis may be proven wrong or falsified (Popper 2009).

According to Yin (2009), doing case study research is a linear but iterative process, and it includes six phases: (1) plan, (2) design, (3) prepare, (4) collect, (5) analyze and (6) share. He emphasizes that case studies are the preferred method when: (1) "how" and "why" questions are being posed, (2) the investigator has little control over events and (3) the focus is on a contemporary phenomenon within a real-life context. Phase 1 includes the identification of the research question or other rationale for doing case study, deciding to use the case study method over other methods and understanding its strengths and limitations. The challenge of a case study approach is that there will be many more variables of interest than data points, in which case multiple sources of evidence should be used, with the data needing to converge in a triangulation (Robson 2002, Stake 1995). Phase 2 includes activities such as defining the unit of analysis and likely case(s) to be studied; developing and articulating theory (e.g., what is being studied and what is to be learnt, propositions and issues underlying the anticipated study); identifying the case study design (e.g., single, multiple, holistic or embedded) and finally defining and designing procedures to maintain the case study quality (e.g., construct validity, internal validity, external validity and reliability) (Yin 2009). Phase 3 consists of the skills the investigator should have to conduct a case study and covers the preparation and training for the specific case study, including procedures for protecting human subjects, the development of a case study protocol, the screening of candidate cases that are to be part of case study and conducting a pilot case study (Yin 2009). In Phase 4, according to Yin (2009), the case study evidence may come from six sources: documents, archival records, interviews, direct observation, participant-observation, and physical artifacts. Phase 5, according to Miles and Huberman (1994) and Yin (2009), consists of examining, categorizing, tabulating, testing or otherwise recombining evidence to draw empirically based conclusions. Yin (2009) states that every case study should follow a general analytic strategy, whether such a strategy is based on (a) theoretical propositions, (b) case descriptions, (c) using both quantitative and qualitative data or (d) rival explanation. According to Yin (2009), the use of a strategy is necessary for the reduction of potential analytic difficulties and for the definition of priorities as to what to analyze and why. In addition, Yin refers to these five analyzing techniques for case studies: (I) pattern matching, (II) explanation building, (III) time series analysis, (IV) logic models and (V) cross-case synthesis. A persistent challenge is to produce high-quality analyses, which require attending to all the evidence collected, displaying and presenting the evidence separate from any interpretations and considering alternative interpretations (Corbin & Strauss 2008, Miles & Huberman 1994, Robson 2002, Stake 1995, Walsham 2006, Yin 2009). Phase 6 consists of reporting the case study, which means bringing its results and findings to closure (Yin 2009). Regardless of the form of the report, similar steps underlie the case study composition: identifying the audience for the report, developing its compositional structure, and having drafts reviewed by others (Stake 1995, Walsham 2006, Locke, Spirduso & Silverman 2007).

1.4 Research process and dissertation structure

The research is carried out by combining design science research with embedded multiple-case study. The initial step in designing the research consists of theory development. In this research the idea behind the developed theory consists of systems thinking design, principles of information infrastructures (IIs) and a science of design for software-intensive systems. Systems thinking binds the foundations, theories and representations of systems science together with the hard, soft and pragmatic methods of systems practice and can be used for improving law enforcement. A system of systems context may involve interplay between multiple socio-digital systems, including many different technologies. The design theory of II tackles the dynamic complexity in the design for IIs, defined as a shared, open, heterogeneous and evolving socio-digital systems of IT capabilities (Hanseth & Lyytinen 2010). The intention of my research is to implement systems science, systems engineering and II & SIS theories, specifically the five design principles proposed by Hanseth and Lyytinen (2010), for improving law enforcement by combining different socio-technical and socio-digital systems and functions (such as criminal investigation, chain-of-custody and monitoring-of-legality) into the same system of software-intensive systems.

Eight cases were selected to comply with Yin's (2009) five general characteristics for case study: (1) the case study must be significant, (2) the case study must be complete, (3) the case study must consider alternative perspectives, (4) the case study must display sufficient evidence and (5) the case study must be composed in an engaging manner. Yin (2009) clarifies that if the case study is likely to be one in which the individual case or cases are unusual and of general public interest, it is advisable if the underlying issues are nationally important. A sense of completeness permeates the way of studying so that the phenomenon is completely investigated and explicit attention is given to its context. The consideration of rival propositions and the analysis of the evidence in terms of rivals are valuable, and a case study is one that judiciously and effectively presents the most relevant evidence.

Before entering the case study analysis, it is necessary to define what the "case" is in this study. Yin (2009) indicates that the selection of an appropriate unit of analysis arises from accurately specified research questions. Table 1 shows the specific units of analysis of this embedded multiple-case study analysis. It also presents the special points of view in terms of how the unit(s) of analysis is explored in each study.

The objective of embedded multiple-case study analysis is to provide understanding and background information for designing new software-intensive systems. In parallel with the case studies, design science research studies are also carried out. Table 2 shows the DSR parts of the studies. Service design methodology is also applied in Study VIII.

TABLE 1 Units of analysis of case studies

Study	Units of analysis			Special points of view
	Sensors	Communications	Command, control &intelligence	
Study I	X	X	X	Operational environment
Study II			X	Monitoring-of-legality; Social acceptance
Study III			X	Investigation data; Digital evidence; Chain-of-custody requirements
Study IV	X	X	X	Enabling technologies; Stakeholders; Stakeholders' needs
Study V		X	X	Communication channels; Interoperability of systems
Study VI		X	X	Provision of digital LE services to field; Mobile monitoring stations; Interoperability of systems; Economic issues
Study VII		X	X	Guaranteeing of LEAs' core services; Economic issues
Study VIII	X	X	X	Management of ICT systems; Multi-supply environment

TABLE 2 Design science research tasks of this study

Study	Artifacts
Study I	Risk analysis model, categories of operational environment challenges
Study II	Concept for transparent surveillance
Study III	Concept for comprising criminal investigations and chain-of-custody requirements
Study IV	Reference architecture for GNSS-based tracking system for LEAs; categories of stakeholders
Study V	Concept for cyber-secure governmental communications
Study VI	"OSI reference model" for LE vehicles
Study VII	ERV concept for all PPRD actors; demo vehicle
Study VIII	Service delivery models for new digital services that PPDR actors need
Cross-case conclusions	System of software-intensive systems' model for law enforcement; PoC model for multi-use of surveillance data

1.4.1 Empirical data sources

The author acted as the national coordinator and scientific supervisor of four public safety related research and development (R&D) projects between October 2007 and May 2014 (RIESCA, SATERISK, MOBI and MACICO). Figure 2 illustrates the subject of the dissertation and how these four R&D projects are connected to the topic. The results and data gathered during these R&D projects have been the main source of evidence for this dissertation. Table 3 analyzes the data categories of these R&D projects from the point of view of this dissertation. Appendix A contains short descriptions of these four R&D projects.

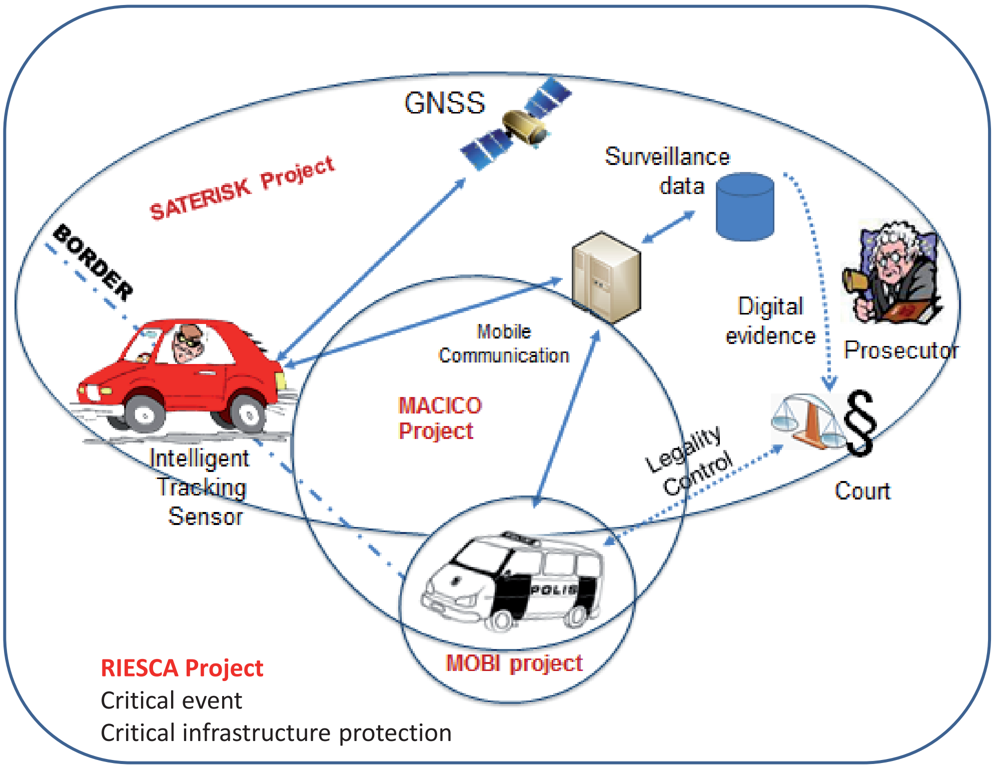


FIGURE 2 Scopes of empirical R&D projects

The data collection of this continuum of eight studies is cumulative, and it was systematically used for qualitative analysis (Corbin & Strauss 2008) between October 2007 and May 2014. Yin (2009) lists the following major sources of evidence for case studies: documents, archival records, interviews, direct observations, participant observations, and physical artifacts. The four R&D projects utilized all these sources of evidence. The main sources of evidence of the case studies of this dissertation have been the documents processed within the four R&D projects. The documents included six themes: (1) books [n = 4] (Pirinen & Rajamäki 2010, Viikari 2011, Rajamäki, Pirinen & Knuuttila 2012), (2) scientific research articles [n = 115], (3) theses made at the Laurea University of Applied (LUAS) Sciences [n = 54], (4) unpublished project reports and practical works of LUAS' students [n = 29], (5) data on project board meetings [n = 30] and (6) data on project workshops and seminars [n = 37]. Table 4 illustrates how these items are divided within the four projects.

TABLE 3 Data categories of empirical R&D projects

Project	Contents
RIESCA	Critical infrastructure (e.g., GNSS, PSC, mobile communications, LEAs' information systems) protection; Critical events (e.g., criminal investigation, pursuit of criminals); Operational environment; Interoperability of systems; Economic issues
SATERISK	GNSS; Tracking sensors; Chain-of-custody requirements; Social acceptance; Monitoring-of-legality; Interoperability of systems; Economic issues
MOBI	Digital services; Mobile monitoring stations; Interoperability of systems; Economic issues
MACICO	Communication channels; Interoperability of systems; Economic issues

TABLE 4 Research data

Project	Data themes							
		Research articles		Theses				
	Books	Journal articles	Conference papers	Master's	Bachelor's	Project reports	Board meetings	Seminars
RIESCA	1	3	8	10	-	9	10	17
SATERISK	2	6	18	5	4	12	5	11
MOBI	1	12	28	8	22	6	9	4
MACICO	-	29	11	1	4	2	6	5
Total	**4**	**50**	**65**	**24**	**30**	**29**	**30**	**37**

1.4.2 Dissertation structure

This dissertation comprises four chapters followed by eight original research publications. This introduction is followed by the presentation, in Chapter 2, of the theoretical foundation of the study. Chapter 3 presents the main research contributions of each of the eight empirical studies as well as cross-case conclusions. Chapter 4 describes the long-term theoretical and practical implications of the research, the quality perspectives and the recommendations for future research.

2 THEORETICAL FRAMEWORK

A GNSS-based tracking system for law enforcement is a complex system of systems. It consists of different socio-digital software-intensive systems, such as law enforcement, GNSS-based tracking systems, communication systems, and command, control and monitoring systems. For improving law enforcement, different functions are also needed, such as criminal investigation, chain-of-custody and monitoring-of-legality. All these systems and sub-systems have many stakeholders with different requirements. IT service governance within these systems needs special attention.

As the theoretical foundation of this study, the systems engineering (SE) based approach, accompanied by software-intensive systems (SIS) and information infrastructure (II) theories, to designing new GNSS-based tracking systems for improved law enforcement is proposed. According to (Hevner & Chatterjee 2010), a system can be defined generally as a collection of elements that work together to form a coherent whole, and software-intensive systems (SIS) are systems in which some, but not necessarily all, of the component elements are realized in software. Hanseth (2002) defines the difference of system and infrastructure as following:

> Our concept of system should not be replaced by that of infrastructure. Rather the infrastructure concept is needed in addition to that of system. The notion of system and the planning and control oriented strategies associated with it will still be useful - and even required - in the development of new components that are going to be included into infrastructures. But the concept of infrastructure and its associated development strategies will redefine those of systems. Systems have to be seen as part of larger infrastructures and the strategies for developing them have to be implemented within the context of strategies for developing the infrastructures the systems are becoming parts of.

SE has a long history within the development of critical systems and examples demonstrating the use of effective engineering and engineering management can be found. These include well or poorly applied but well-defined processes (Kinzig 2010). Throughout the many decades over which SE has emerged as a discipline, many practices, methods, heuristics and tools have been developed, documented, and applied (Kinzig 2010). SE is a systematic approach to find means for achieving previously defined goals. It works well in developing 'hard' technical systems. However, SE has shortages in respect to 'soft' systems of human actions, in which the research goals are always a part of the conundrum. In this dissertation, SE is accompanied by SIS and II theories in order to taking into account the socio-digital infrastructures, platforms, application and IT capabilities that cannot be truly 'designed' in a traditional sense as in traditional approaches a designer assumes control over the design space (Edwards et al. 2009).

2.1 Designing of socio-digital systems

2.1.1 Systems engineering

Systems thinking binds the foundations, theories and representations of systems science together with the hard, soft and pragmatic methods of systems practice. In systems praxis, there is a constant interplay between theories and practice, with theory informing practice and outcomes from practice informing theory. Systems thinking is the on-going activity of assessing and appreciating the system context, and guiding appropriate adaptation, throughout the praxis cycle (Pyster & Olwell 2013).

Integrative Systems Science has a very wide scope. Systems Theory represents a significant theoretical background for any professional undertaking within the branch of GNSS-based tracking. Many methods exist to elaborate this kind of theory. For engineering purposes, such as tracking systems, the classical approach, called General Theory of Systems, is usually accepted as the most beneficial theoretical background.

Systems engineering (SE) is an interdisciplinary field of engineering that focuses on how to design and manage complex engineering projects over their life-cycles (Pyster & Olwell 2013). SE ensures that all aspects of the system are considered and integrated into a whole and that the system satisfies the needs of its customers, users and other stakeholders. SE as a technical and technical management process is widely used, such as in the military sector. SE results in delivered products and systems that exhibit the best balance between cost and performance (Kinzig 2010). The process must operate efficiently with desired mission-level capabilities, establish system-level requirements, allocate these down to the lowest level of the design, and ensure validation and verification of performance while meeting the cost and schedule constraints (Kinzig 2010). Some key elements of SE include the principles and concepts that characterize the system, which comprise an interacting combination of system elements to accomplish defined objectives. The system interacts with its environment, including other systems, users and the natural environment. The system elements that comprise the system include hardware, software, people, information, techniques, facilities, services and other support elements (Pyster & Olwell 2013). Sauser et al. (2006) present the concept of a system readiness level (SRL), which incorporates the technology readiness level (TRL) scale used by the National Aeronautics and Space Administration (NASA) since the 1980s. They also introduce the concept of an integration readiness level (IRL) to dynamically calculate an SRL index (Sauser et al. 2006).

Every man-made system has a life-cycle. Table 5 lists seven generic SE life-cycle stages and their purposes. The INCOSE SE Handbook (Haskins et al. 2011) states:

> The purpose in defining the system life cycle is to establish a framework for meeting the stakeholders' needs in an orderly and efficient manner. This is usually done by defining life-cycle stages and using decision gates to determine readiness to move from one stage to the next.

TABLE 5 Generic SE life-cycle stages

Life-cycle stage	Purpose
Exploratory research	Identify stakeholders' needs. Explore ideas and technologies.
Concept	Refine stakeholders' needs. Explore feasible concepts. Propose viable solutions.
Development	Refine system requirements. Create solution descriptions. Build system. Verify and validate system.
Production	Produce system. Inspect and verify.
Utilization	Operate system to satisfy users' needs.
Support	Provide sustained system capability.
Retirement	Store, archive or dispose of the system.

SOURCE: Modified from Haskins et al. (2011)

A new project (system-of-interest, SoI) typically begins with an exploratory research stage. This starts before any formal definition of the SoI is developed. According to Robson (2002), the purpose of exploratory research is to search conjectures and hypotheses to be selected as targets for future research. Robson (2002) continues that the purpose of exploratory enquiry may also be to find out what is happening, particularly in little-understood situations. Yin (2009) notes that an exploratory case would cover the issue or problem being explored, the methods of exploration, the findings from the exploration, and the conclusions with suggestions for future research. According to the International Council on Systems Engineering (INCOSE) (Haskins et al. 2011), the exploratory research stage in SE includes the identification of stakeholders' needs and exploration of ideas and technologies available. If the stakeholder needs are not properly understood, any system carries the risk of being built to solve the wrong problems. The first step in the exploratory research phase is to identify all stakeholders and their needs. The main tasks of this phase are to establish the feasibility of meeting the stakeholder requirements and explore technology readiness. This process should be carried out iteratively, and stakeholder needs and requirements should be revisited as new information becomes available (Pyster & Olwell 2013).

Classical structural contingency theory suggests that organizational effectiveness is dependent upon the organization's ability to adjust or adapt to the environment, and that there is a need for congruency between the environment and structure (Drazin & Van de Ven, Andrew H 1985, RW.ERROR - Unable to find reference:234, Betts 2011, Lawrence, Lorsch & Garrison 1967). Most environments include multiple systems and systems of systems. System of systems engineering (SoSE) is applied in merging the operations of multiple enterprises in order to provide some new form of service. When responding to the challenges of tracking non-cooperative targets, SoSE should be initiated in the form of a request for service in order to meet a complex situation that has come up. SoSE involves accelerated engineering of the system created to respond to the situation.

2.1.2 Designing software-intensive systems

Theory of complex systems traces its roots to the 60s when Herbert A. Simon wrote his book "Science of the Artificial" (Simon 1978). Fulfillment of purpose involves the relationship between the artifact, its environment and a purpose or goal. Alternatively, it can be viewed as the interaction of an inner environment (internal mechanism), an outer environment (conditions for goal attainment) and the interface between the two. According to Hevner and Chatterjee (2010), the real nature of the artifact is the interface. Both the inner and outer environments are abstracted away. The science of artificial complex systems should focus on the interface, the same way design focuses on the "functioning." According to Hevner and Chatterjee (2010), a general theory of complex systems must refer to a theory of hierarchy, and the near-decomposability property simplifies both the behavior of a complex system and its description.

Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how software-intensive systems (SIS) are conceptualized, built and evaluated. According to Hevner and Chatterjee (2010), manual methods of software and systems engineering must be replaced by computational automation that will transform the field into a true scientific and engineering discipline. They also argue that the vision of science of design research for SIS must achieve the following essential objectives:

> • Intellectual amplification: Research must extend the human capabilities (cognitive and social) of designers to imagine and realize large-scale, complex software-intensive systems.
>
> • Span of control: Research must revolutionize techniques for the management and control of complex software-intensive systems through development, operations, and adaptation.
>
> • Value generation: Research must create value and have broad impacts for human society via the science and engineering of complex software-intensive systems and technologies.

Figure 3 illustrates the three layers of SIS: (1) the platform layer, (2) the software layer, and (3) the human layer. In addition, the two critical interfaces are shown.

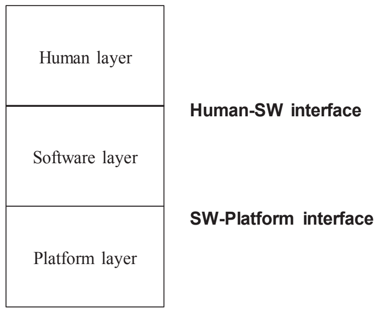


FIGURE 3 Software-intensive systems layers

SIS design entails many important decisions, such as the design and allocation of system behaviors (e.g., functions, actions) and system qualities (e.g., performance, security, reliability) to the different layers (Hevner & Chatterjee 2010). A particular system activity could be realized in hardware (platform), via, for example, a service call (software), by human behavior (human) or by some combination of activities across all three layers, and a performance requirement (e.g., response time) for an SIS transaction could be divided and allocated as performance requirements in each of the layers (Hevner & Chatterjee 2010). Nearly all future SIS will be connected to environmental resources and other systems via network connections, and these connections lead to complex systems-of-systems architectures to provide behaviors and qualities (Hevner & Chatterjee 2010). There will be identifiable networks across all three SIS layers: physical networks support the transmission of digital and analog data among system platforms, software networks provide the middleware layers and protocols that transform the transmitted data into information that is shared among the information processing systems, and social networks provide a means of interaction and community among the human participants of the complex system (Fiadeiro 2007).

2.1.3 Design principles for information infrastructures

The II literature has addressed the challenges of realizing large-scale technological systems (Hanseth & Lyytinen 2010, Monteiro & Hanseth 1996, Star & Ruhleder 1996, Edwards et al. 2009). Large-scale information systems are not stand-alone entities but rather are integrated with other information systems and communication technologies as well as with other technical and non-technical elements. This approach is relevant for analyzing the domain of satellite-based tracking systems for improving law enforcement.

Hanseth and Lyytinen (2010) have synthesized their study's insights into a normative design theory for IIs, distinguishing between two generic challenges:

(1) The ''bootstrap problem'' addresses the establishment of a novel II. Since an II gains much of its value from its large and diverse user base and components, the fact that initially the user community is non-existent or small precludes the fact that the infrastructure can offer these benefits. (2) The ''adaptability problem'' relates to the further growth and expansion of an II where unforeseen demands, opportunities, and barriers may arise. Table 6 presents Hanseth's and Lyytinen's 19 design rules that they have inferred from the Complex Adaptive Systems (CAS) theory (Holland 1996).

TABLE 6 Design rules for dynamic complexity in the design for IIs

Design problem	Element of CAS	Design principles	Design rules
(1) Bootstrap problem Design goal: Generate attractors that bootstrap the installed base	Create an IT capability that can become an attractor for the system growth.	1. Design initially for direct usefulness.	DR1. Target IT capability to a small group DR2. Make IT capability directly useful without the installed base DR3. Make the IT capability simple to use and implement DR4. Design for one-to-many IT capabilities in contrast to all-to-all capabilities.
	Avoid dependency on other II components that deflect away from the existing attractors Use installed base as to build additional attractors by increasing positive network externalities	2. Build upon existing installed bases	DR5. Design first IT capabilities in ways that do not require designing and implementing new support infrastructures DR6. Deploy existing transport infrastructures DR7. Build gateways to existing service and application infrastructures DR8. Use bandwagons associated with other IIs
	Exclude alternative attractors by persuasive tactics Offer additional positive network externalities by expanding learning in the user community	3. Expand installed base by persuasive tactics to gain momentum	DR9. 'Users before functionality' – grow the user base always before adding new functionality DR10. Enhance any IT capability within the II only when needed DR11. Build and align incentives so that users have real motivation to use the IT capabilities within the II in new ways DR12. Develop support communities and flexible governance strategies for feedback and

			learning
(2) Adaptability problem Design Goal: Make the system maximally adaptive and variety generating as to avoid technology traps	Build capabilities that enable growth based on experience and learning Use abstraction and gateways to separate II components by making them loosely coupled	4. Make the IT capability as simple as possible	DR13. Make the II as simple as possible in terms of its technical and social complexity by reducing connections and governance cost DR14. Promote partly overlapping IT capabilities instead of all-inclusive ones.
	Design IT capabilities and their combinations in ways that allow II growth Use evolutionary strategies in the evolution of II that allow independent incremental change in separate components Draw upon II designs that enable maximal variations at different components of the II	5. Modularize the II	DR15. Divide II recursively always into transportation, support and application infrastructures while designing the II DR16. Use gateways between standard versions DR17. Use gateways between layers DR18. Build gateways between infrastructures DR19. Develop transition strategies in parallel with gateways

SOURCE: Hanseth & Lyytinen (2010)

Aanestad and Jensen (2011) have studied IIs in healthcare. According to them, large-scale and long-term stakeholder mobilization is a core challenge when realizing nationwide information infrastructures for public organizations. They continue that the implementation strategy of such IIs must deal with the multiple stakeholders and be able to mobilize and coordinate them. A modular implementation strategy, made possible by appropriate modularity of the solution, allows the implementation to be organized in a way that does not require widespread and long-term commitment from stakeholders initially. Aanestad and Jensen (2011) argue that "solutions that provide immediate use value by offering generic solutions to perceived practical problems, balance the stakeholders' costs and benefits, and solve a problem with minimal external dependencies, can avoid some of the dilemmas often associated with large-scale IIs." Their research illustrates the dangers of introducing requirements that are too high for stakeholder mobilization, and the notions of stable intermediary forms and modular transition strategies may help decision-makers to pursue other avenues when planning large-scale implementation projects (Aanestad & Jensen 2011).

2.2 Law enforcement

2.2.1 Overview of public safety functions

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[6]. 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 7 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 are also certified first responders.

TABLE 7 Public safety organizations and functions

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

6 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).

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.
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	Transport police is a specialized police agency responsible for the law enforcement and protection of transportation ways like railroad, highways and others.	Law enforcement
Railway Transport Police	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
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	Airport enforcement authority is responsible for protecting airports, passengers and aircrafts from crime.	Law enforcement
Port Security	Port enforcement authority is responsible for protecting port and maritime harbor facilities.	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.

SOURCE: Baldini (2010)

Law enforcement is concerned with the prevention of crimes, and discovering and punishing persons who violate the rules and norms governing the society. Although the term may encompass entities such as courts and prisons, it is most frequently applied to those who directly engage in patrols or surveillance to dissuade and discover criminal activity and to those who investigate crimes and apprehend offenders. A law enforcement authority (LEA) is a national police, customs or other authority that is authorized by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. According to Baldini (2010), law enforcement includes, for example, the following sub-functions:

- Tour of duty to identify and intervene in cases of offence to criminal law. This is also called patrolling.
- Criminal investigation.
- Customs verifications, which are responsible for monitoring people and goods entering a country or to detect offences against customs laws (this function is also shared by border security).
- Law enforcement in the transportation domain to identify law offences on the transportation infrastructures like roads, air, railways and sea.
- Custody and transportation of criminal convicts.

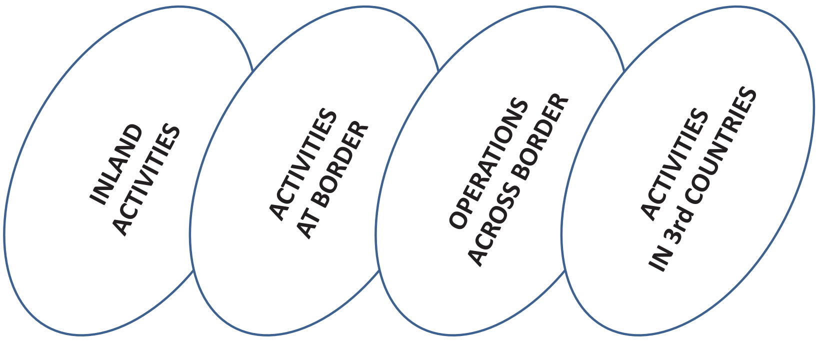
2.2.2 Border protection and LEAs' cross-border operations

Traditionally border protection consists of border troops and security checkpoints. Border troops include many border patrol agents in vehicles (cars, snowmobiles, helicopters, etc.) or on foot to patrol areas searching for intruders. Once intruders are detected, the patrol agents must switch tasks and attempt to arrest the intruders (Patrascu 2007). The Border Guard uses both permanent and temporary security checkpoints, where all vehicle traffic is stopped in order to detect and apprehend illegal aliens, drugs and other illegal activities. Permanent checkpoints are generally located on international roads, while temporary checkpoints are located on smaller arterial and rural streets (Patrascu 2007). Each border troop watches and controls a specific section of the border (Sun et al. 2011).

Traditional border protection systems endure intense human interaction. Recently, new high-tech devices (unmanned aerial vehicles, unattended ground sensors, surveillance towers equipped with camera sensors, etc.) have been put into operation. However, any single technique encounters inextricable problems (high false alarm rate, line-of-sight-constraints, etc.) (Sun et al. 2011).

The main target of EU border security is to safeguard European values and interests, 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 et al. 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.



SOURCE: modified from Laitinen (2011)

FIGURE 4 Four-tier access control model

Figure 4 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.

Organized crime is a real threat in Europe with the emergence of international warehouses of crime. Criminal organizations are multinational, but LEAs are national organizations. The use of advanced technologies, such as in Customs, has become increasingly important when the aim is to ensure unobstructed commercial traffic and, at the same time, make efforts to stop illegal traffic. Effective international cooperation is necessary for ensuring effective logistics, and the cooperation should also cover the technical standards used. Finnish Customs joined the SATERISK research project in 2009. Accordingly, the SATERISK project supported operative cooperation between Customs and other authorities while creating business opportunities for security companies (Erling 2012). Hopefully, these opportunities can be efficiently utilized in the future.

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 (Viitanen et al. 2010a).

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 (Viitanen et al. 2010a, Rajamäki & Viitanen 2014).

2.2.3 Law enforcement technology services

In the last two decades, modern technologies have become an indispensable part of our lives. Technologies facilitate our daily lives, and nowadays it is not even possible to imagine that we can manage without them. Unfortunately, technologies facilitate the daily lives not only of upstanding citizens, but of the organized criminals, as well. Regrettably, organized crime often has more opportunities to use the technological achievements than do LEAs (Padding 2013). However, in order to improve their evidence-gathering abilities, LEAs are constantly seeking new technological recording, information retrieval and monitoring solutions that will facilitate their combat against criminal organizations. The criminals' countermeasure activities, such as electronic counter-surveillance, jamming and constant changes in behavior to prevent eavesdropping or physical surveillance, are continuously increasing (Rajamäki & Viitanen 2013). The pressure to find new intelligent technologies, which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive, is emerging and is a high-priority task. Respecting the accountability and integrity requirements and smooth utilization of data in different phases of chains-of-custody is of utmost importance. In the current situation, the chain-of-custody is difficult to maintain due to different stand-alone techniques that are connected to different monitoring systems. This makes the LEA work very labor-intensive, so the use of new state-of-the-art technologies should enable the optimization of the use of human resources (Tuohimaa et al. 2011, Viitanen et al. 2010b).

When LEAs are working in order to prevent and investigate crimes, some of the operations affect the privacy of citizens. Video surveillance, audio surveillance and technical tracking are among those activities (Viitanen et al. 2012). As early as 2006, BBC News listed some of the possible means for surveillance and tracking: CCTV cameras, automatic number plate recognition, radio frequency ID tags in shops, mobile phone triangulation, store loyalty cards, credit card transactions, satellites, the electoral roll, national health service patients records, personal video recorders, phone-tapping, bugs and hidden cameras, worker call monitoring and cookies.[7] Only LEAs can legally use the information from all these sources. In addition to using gathered data, LEAs share information with other authorities. European integration has increased transport of illegal goods and criminals. Therefore, transmitting, tracking and other status information between nations and different organizations is becoming everyday business. For example, LEAs are using more tracking technology than ever before. The systems are network-based (GSM&TCP/IP), and they can transmit information basically anywhere. These days, technical tracking is used in even nominal cases (Rajamäki, Pirinen & Knuuttila 2012, Rajamäki 2012).

2.2.4 ENLETS

In order to effectively fight organized crime, the EU must keep up with the development of technology. The EU should use all the benefits of the modern technologies in order to fight against criminal activities and promote cooperation among the EU Member States. In order to implement the desired goals, 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. The main goal of this sub-group is to strengthen police activities and cooperation and increase the use of modern technologies in the process of exchanging information, knowledge or experience. Another goal of ENLETS is to develop a common single platform for the delegates of the EU Member States for information exchange. One contact person in every EU member coun-

---

7 BBC news story, "How we are being watched?," BBC London, Feb. 2006. [Online]. Available: http://news.bbc.co.uk/2/hi/uk_news/6110866.stm

try will be responsible for collecting information on technological needs and for presenting those needs to ENLETS. This platform is necessary for the experts in the LEAs in order to share the news about the technology market and advice on the use of technologies in the daily life of any officer. The primary goal is to use one common platform of ENLETS, which would be available for every EU member country, and in this way to avoid duplications of different systems that have already been used by some EU member countries. It is not a secret that technologies are quite expensive. For that reason, ENLETS is also trying to find possible financial solutions in regards to the implementation of technologies in the field of law enforcement (Council of the European Union 2012, Padding 2013).

According to Padding (2013), the new vision and mission for ENLETS are:

> Vision: The European Network of Law Enforcement Technology Services will be the leading European platform that strengthens police cooperation and bridges the gap between the users and providers of law enforcement technology.
>
> Mission: ENLETS supports front line policing and the fight against serious and organised crime by gathering user requirements, scanning and raising awareness of new technology and best practices, benchmarking and giving advice. It is active in joint initiatives, sharing information and networking between law enforcement agencies, industry and research organisations. It is a point of contact to access European law enforcement technical organisations.

According to Padding (2013), ENLETS realizes its mission by co-operating on three levels: (1) the sharing of best practices, (2) the co-creation of new technology services and (3) research. Padding continues that the sharing of best practices, which enables "quick wins" on the Europol Platform of Experts (EPE), is the most important task and priority of ENLETS. Examples of shared best practices include: automatic number plate recognition, IT systems (open source and signals), tools for cross-border surveillance and remote stopping of vehicles. The next step of ENLETS' technology scope is co-creation based on missing requirements within best practices (Padding 2013). This step includes sharing (inter)national projects, such as biometrics, fraud identification and covert surveillance multisensory tools (e.g., high-quality long-distance listening tools with chain-of-custody and privacy enhanced technology) (Padding 2013). These technology developments should be based on operational priorities with a short-to-market approach (1–2 years) and with industry being the developer (Padding 2013). According to Padding (2013), the third level of ENLETS' technology scope is the needed research that is not always in line with requirements. This is mainly carried out by the core group members of ENLETS, which include The Netherlands, The United Kingdom, Finland, Belgium, Poland and the EU's presidency country. ENLETS' role is to feed end-users' needs to EU research programs, such as Horizon 2020. The new funding instruments '*pre operational validation*' and '*pre commercial procurement*' are good initiatives in Horizon 2020 (Padding 2013).

2.2.5 Coercive measures and technical tracking

The surveillance technologies and methods used by LEAs are one of the most regulated areas in society. A safe and reliable system is needed, mainly because the majority of people are particularly concerned about the unseen and what they also think is uncontrolled and excessive surveillance. Fortunately, LEAs can legally obtain information from all kinds of sources. Unfortunately, large-scale technological infrastructures are prone to large-scale problems. We read in newspapers and on the web, watch on TV and hear on the radio, news about some or other occurrence of data leakage. Occasionally there are allegations about LEAs' abusing surveillance. Because the cases and materials are mostly confidential and hence not publicly available to use as counter arguments, LEAs cannot prove that they are not abusing their powers. LEAs argue that what is invisible to outsiders and under the police's control must be proportionate; otherwise, it would never have been accepted (Viitanen et al. 2012).

The Finnish Coercive Measures Act (CMA) defines the methods and measures that pre-trial investigation authorities are entitled to use to interfere with human rights protected by law. According to CMA, the technical tracking means the tracking of a vehicle or goods with a radio transmitter or other such device or mechanism attached to the vehicle or the goods. On the other hand, according to the Finnish Police Act (PA), technical tracking means the tracking of the movements of a vehicle or goods. Within the SATERISK project, the legislation in force regarding technical tracking as a part of technical surveillance has been clarified. The legislation is disordered and difficult to understand. It includes numerous partial reforms and references to other laws, and as a whole it is hard to manage. What makes it especially troublesome is the difficulty of drawing the line between the coercive measures that are prescribed in CMA and used in pre-trial investigations and the measures that are prescribed in PA and used for information gathering purposes in the crime prevention phase (Ojala 2010).

When the officers in charge of an investigation are dealing with technical tracking as a covert measure, they should take into consideration the following: The sections of law regarding technical tracking, human rights, general principles of police duties such as the principle of proportionality and professional ethics. According to the evaluation of the functioning of legality control concerning covert coercive measures and especially technical tracking, the quality of monitoring-of-legality in Finland is good. However, the external monitoring-of-legality regarding technical tracking is quite insignificant. This reflects the internal control of the police, which is also on a very small scale (Ojala 2010). With regard to the use of technical tracking, very little scientific research information is available. There is only a small amount of literature available on the evaluation of various methods of application. It is very difficult to find any description or legal rules on this item. Further, there are no comments available from the Parliamentary Ombudsman or Deputy Ombudsman nor legally valid decisions of the Supreme Court or Court of Appeal regarding technical tracking (Ojala 2010).

In Finland, a reform of legislation is in progress. The new Coercive Measures Act was signed in July 2011, and it came into effect in January 2014. The new CMA undermines the possibilities of the police to carry out efficient pre-trial investigations. At the same, time it increases the amount of work for officers in charge of investigations. It also relates particularly to the execution of the technical tracking of vehicles and to the use of extraneous information obtained by covert coercive measures and concerning an offence other than that for which the investigation is carried out (Rajamäki & Viitanen 2013).

2.2.6 Monitoring-of-legality

In Finland, the LEAs' monitoring-of-legality of actions means:

> Under the Constitution, the law must be strictly observed in all public activity. In accordance with section 68 of the Constitution, each ministry, within its purview, is responsible for the appropriate functioning of administration. The principle that the administration is subject to the law also requires that the legality of actions of the authorities is monitored.
>
> In the Ministry of the Interior's branch of government, the primary goal of internal monitoring of legality is to promote the performance of the duties imposed on the branch as well as to maintain and strengthen the trust of citizens in the legality of our actions. Monitoring of legality aims to prevent possible mistakes but also to reveal wrongful or unlawful conduct and process such matters in an appropriate way. [8]

In Finland, the oversight of the police's coercive measures is based on the file system SALPA (the Finnish acronym for an electronic database system used by the Finnish Security Intelligence Service and the National Bureau of Investigation) (Niemi & de Godzinsky 2009). The SALPA system provides guidance on how to make applications and notifications in the right manner. The question then is: Can this system alone be a sufficient legality control system if the information that police officers write down is not based on actual log files? These non-transparent systems might be handicaps to LEAs (Viitanen et al. 2010a).

2.2.7 Emergency response vehicles

Emergency response vehicles (ERVs) used by police, customs and frontier guards, as well as fire, rescue and emergency medical services, are increasingly dependent on technology, especially ICT systems (Rajamäki et al. 2014b, Rajamäki et al. 2014a). In the past decade, an increasing number of new technical devices and systems have been installed in these vehicles, and it is necessary to ensure that information and the "on-demand" services provided by these technologies are delivered reliably and securely through one or more of the recently developed wireless architectures. There are, however, serious challenges to overcome. As the number of ICT systems has increased, the number of user in-

8 Ministry of the Interior. http://www.intermin.fi/en/ministry/monitoring_of_legality

terfaces of ERVs has increased considerably. This has resulted in functionality problems; for example, the space for airbags to function has decreased. Also, technical problems with regard to electric supply and cabling arrangements have occurred. In addition, the documentation of applied solutions is not always adequate. Another issue is that the longed-for standardization in the field has not taken place. This may be due to the large variety of equipment suppliers or because the annual delivery amount of ERVs is so low that standardization has not been given priority by experts in the field. However, some standardization projects are on-going.

The European Standard series EN 1846-x for "Firefighting and rescue service vehicles" currently has three parts: Part 1: Nomenclature and designation, Part 2: Common requirements—Safety and performance and Part 3: Permanently installed equipment—Safety and performance. The National Fire Protection Association (NFPA) is an international non-profit organization that has a mission to reduce the worldwide burden of fire and other hazards regarding quality of life by providing and advocating consensus codes and standards, research, training and education. NFPA is responsible for 300 codes and standards designed to minimize the risk and effects of fire by establishing criteria for building, processing, designing, servicing, and installing fire-fighting facilities in the US and other countries. NFPA has two ERV-related standards: NFPA 414, "Standard for aircraft rescue and fire-fighting vehicles" and NFPA 1071-11, "Standard for emergency vehicle technician professional qualifications."

The Ministry of Health and Long-Term Care of Ontario, Canada, has standardized the minimum acceptable requirements for land ambulances for use by an operator of a land ambulance service. This 126-page standard specifies all construction and design details, including voice radio installation requirements. However, the standard has no information regarding data communications, field command systems and interoperability between different PPRD responders. [9]

The Association of Chief Police Officers (ACPO) Intelligent Transport Systems (ITS) Working Group identifies and works to incorporate emerging technologies to benefit the police services of the UK. ACPO ITS leads a public–private partnership to develop the One Box Single Vehicle Architecture (OBSVA) [10] and Driver and Vehicle Data Management [11] concept and functional requirements for police, with on-going work to develop products showing how the data can be utilized to better manage the police vehicles and drivers proac-

---

9 Ministry of Health and Long-Term Care, Ontario Provincial Land Ambulance & Emergency Response Vehicle Standard, Version 5.0, September 28, 2012. Available at: http://www.ambulance-transition.com/pdf_documents/standards_land_amb_emergency_response_vehicle_standard.pdf

10 Home Office Centre for Applied Science and Technology, One Box Single Vehicle Architecture Criteria, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/115688/cast3911.pdf

11 Home Office Centre for Applied Science and Technology. (2012). One box: Driver and vehicle data management system criteria. Available: http://www.homeoffice.gov.uk/publications/science/cast/crime-prev-community-safety/cast2812?view=Binary

tively. This work is one aspect of police vehicle standardization, increasing functionality and driving down cost to deliver a cost-effective approach to police transport fitment and procurement into the future. The concept ensures that the equipment adheres to the standard and is fit for its purpose and functionality, creating a technology platform for the future. The OBSVA criteria aim to facilitate the development and installation of effective and safe emergency service equipment in vehicles. The OBSVA criteria are owned and maintained by the Home Office Centre for Applied Science and Technology (CAST). The OBSVA criteria suggest standardization and the harmonization of technologies as a way to ensure effective emergency services in the future with significantly reduced budgets. They outline the standards of the future fitment of LEA vehicles. Their aim is to provide a safe and efficient working environment for officers. This equipment fit should deliver better usability and cost-efficiencies and provide a link to the standardization of all types of LEA vehicles currently in use. The OBSVA criteria introduce, for instance, requirements and specifications for controls, switches and interfaces. For example, the criteria suggest that a LEA vehicle should have a graphical user interface with touchscreen capability. They also provide guidelines on how voice activation or hands-free operations should be utilized in a police vehicle. In addition, the OBSVA criteria introduce specific instructions on how different equipment should be fitted in a LEA vehicle in order to maximize work safety and to avoid driver distraction as much as possible.

Project54 is a modular system that integrates in-car based electronic systems, software and user interfaces (Pelhe et al. 2004). It also allows officers to access the in-car system using handheld devices. There is a main executable application and individual applications that control in-car electronic devices or provide other services. The devices are controlled by integrated software components running on an embedded computer. The integrated software components also implement an integrated user interface. The system allows the officer to have control over all the electronic devices, either through a touchscreen or through a voice interface. The Project54 system aims to improve the ability of LEA to collect and interpret data, and exchange data between mobile units. It also aims to increase the functionality of ERVs, increase the information available to officers in the field, and to facilitate communication between mobile units. The increased effectiveness and improved safety of the officers are also important aspects. In 2009, the system was in use in over 1,000 LEA vehicles in New Hampshire. [12]

Feniex Olympus 16X software is compatible with any PC system. A two-user customizable interface features memory button functionality. This software and hardware combination allows a user to control all ERV electronics with the click of a mouse, keyboard stroke or finger touch of a digital button. The user interface set-up allows each officer to customize, configure, label and position their own digital buttons as well as their three main programmable

---

12 A.L Kun, Project54 Introduction, UNH Consolidated Advanced Technologies Laboratory (CATlab). Available: http://www.catlab.sr.unh.edu/overview/introduction/

memory buttons. The system also includes a three-switch face plate, which serves as a fail-safe option in the event of a computer crash. Each button controls one of the programmable memory buttons. There is an optional touchscreen add-on. The touchscreen mounts inside the vehicle console and allows the user to control all vehicle electronics. [13]

The Rockwell Collins iForce™ is an integrated ERV solution that can be tailored to meet specific requirements. At the heart of the system is a Linux-based, high-assurance computer that allows users to control all vehicle electronics through a single integrated system. iForce™ offers three ways to control all electronics: a color touchscreen display, a hand controller and voice activation capability. As a result, much of the electronic hardware is removed from the front of the vehicle, creating a much safer and more efficient work environment for the officers. iForce™ integrates stand-alone vehicle electronics into a command and control system that improves functionality, communications, ergonomics and safety. iForce™ allows officers to cross-band with other FRs at an accident, emergency or crime scene. iForce™ integrates radio, video and computer functions into one system that enhances an officer's on-site communications, control and security needs while ensuring public safety. [14]

The National Information Exchange Model (NIEM), which aligns with user-driven requirements engineered for interoperability, is a community-driven, government-wide, standards-based approach for exchanging information. [15] NIEMS is widely used in the US and internationally. It is a consistent starting point, including a data model, governance, training, tools and technical support services. Its active community assists users in adopting a standards-based approach to exchanging data.

The National Safety Agency (NSA) of Australia has integrated technology into police patrol vehicles and command vehicles. A new police patrol vehicle concept provides benefits to jurisdictions seeking to use technology to improve their law enforcement capability. NSA's police patrol vehicle has been designed to allow greater functionality whilst reducing clutter inside the cabin. The technology integrated into the vehicle enables more work to be undertaken in the field. Overall, the technology and purpose-built interior increase the officers' safety as well as their operational effectiveness. A key feature is a liquid-crystal display (LCD) touchscreen embedded into the dash of the vehicle; all of the equipment included in the car is operated through this touchscreen. The level of technology integration in the vehicle provides superior surveillance capability. This includes automatic number plate recognition cameras, night vision cameras, speed detection equipment and biometric devices. A key risk of installing this technology is vehicle battery drain. This has been overcome with the development of a power management system that enables a range of equipment to function without impacting the vehicle battery. NSA's command vehicle project

---

13 Feniex Product Catalog 2012, Available: http://corepublicsafety.com/catalogs/Feniex2012catalog.pdf

14 Rockawell Collins – Home. Available: http://www.rockwellcollins.com

15 NIEM – National Information Exchange Model. Available: https://www.niem.gov/Pages/default.aspx

will create a mobile command center able to operate in remote locations for extended periods of time. The high level of connectivity in the vehicle enables communication between a central base and the personnel in the field. Active repeaters fitted to the vehicle boost signal strength, supporting communications in the most remote areas. The vehicle is fitted with solar panels to ensure power is constantly generated, so the equipment will operate without being constrained by the vehicle's battery capacity. Power management systems also aid in extending the length of time the equipment is operational in the vehicle without impacting battery charge. The vehicle is fitted ready for deployment reducing response time when there is an incident. [16]

2.3 GNSS-based tracking systems

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 everyone. 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 October 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.

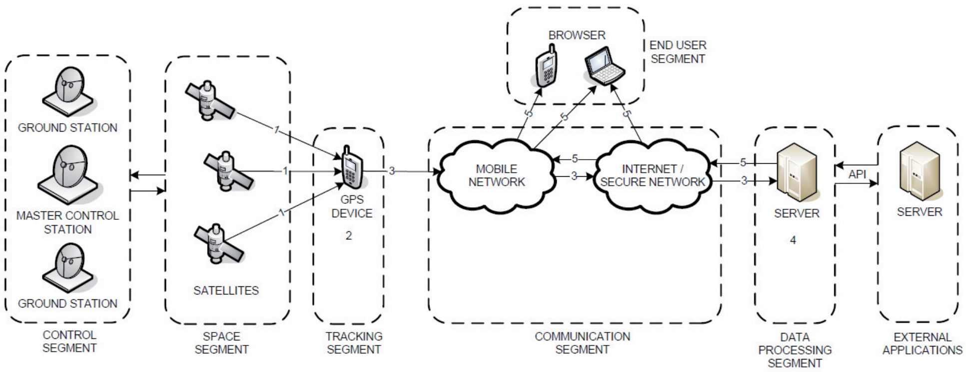
In general, the GNSS receiver compares the time a signal was transmitted by a satellite with the time it was received. The time difference, along with the location of the satellites, allows the receiver to determine the user location. Signals from a minimum of four different satellites are required to determine the three-dimensional position. The receiver usually consists of an antenna assem-

16 National Safety Agency [Online]. Available: http://www.nsaaust.com/

bly, 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 Colorado Springs; five remote monitor stations which are located in Hawaii, Ascension Island, Diego Garcia, Kwajalein and Colorado Springs; three ground antennas, which are located at Ascension Island, Diego Garcia and Kwajalein and a Pre-Launch Compatibility Station, which can also function as a ground antenna, located at Cape Canaveral (O'Brien & Griffin 2007).

A GPSS-based tracking system combines navigation and telecommunications technologies. The system is relatively complicated, and it consists of many technical segments, including 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 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), as shown in Figure 5. The system is complex and vulnerable to many kinds of cyber-attacks (Kämppi, Rajamäki & Guinness 2009).



SOURCE: modified from Kämppi and Guinness (2010)

FIGURE 5 Components of a satellite-based tracking system

Tracking devices have become inexpensive; the coverage of the mobile network has grown, and developments in personal gadgetry have enabled the expansion of GNSS-based tracking applications. Satellites and wireless information form a fast-growing part of our daily lives. This view is confirmed in the literature, and many commentators point out that satellites are to be identified as a part of critical infrastructure (Rajamäki, Pirinen & Knuuttila 2012).

In the future, the public sector may utilize the tracking of motor vehicles for road-tolling. The British Automobile Association is aiming to launch a new insurance policy that uses satellite navigation technology to track driver performance: speed, braking severity, cornering and the types of roads used (Lee

2012). The approach is seen as being likely to become commonplace by the Association of British Insurers, but the Association for British Drivers is slightly worried (Lee 2012).

2.3.1 Risks of commercial GNSS

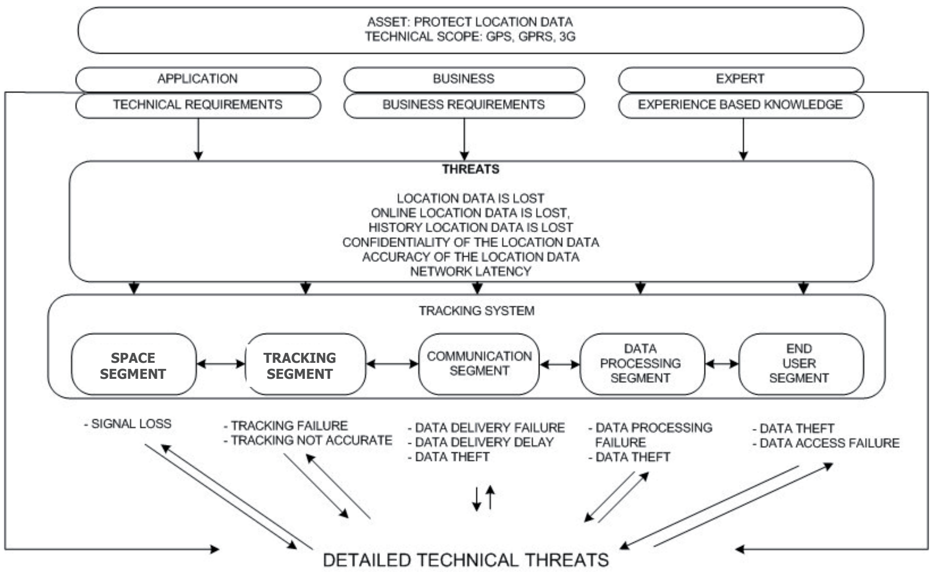
The benefits of GNSS-based tracking applications are regularly promoted. However, the risks and misuses are too often ignored. A GNSS-based tracking system is complex, and there are many vulnerabilities and threats at different technical levels of the system. The SATERISK project has enhanced the understanding of the potential risks, and it has provided valuable tools to avoid potential threats. Most probably, new risks will emerge in the future in the field of GNSS-based tracking. It is important to continue international cooperation and investigations to recognize the most severe and topical risks. This is an important issue especially with regard to cross-border tracking (Rajamäki 2012). This section deals with the potential technical risks in the field of satellite-based tracking systems: how to recognize and identify risks and what the countermeasures are that can be used to avoid them.

Lack of a satellite signal is still the most common risk in GNSS-based tracking. While becoming more popular, man-made interference and misuse for criminal purposes have become more common. Unrecognized risks can paralyze critical business applications, such as cash in transit, fleet management and road tolls, and they can be fatal for mission-critical applications, such as major LEA operations. For that reason, it is important to recognize the risks related to GNSS-based navigation and tracking systems (Kämppi & Guinness 2010).

The end-user segment might be, for example, an office-based Geographic Information System (GIS) for emergency management or a mobile field command system for LEAs. The manner in which GNSS used with GIS is wide and varied, allowing users to determine the way GIS and GNSS are used together to best meet their needs (Rajamäki, Rathod & Kämppi 2013, Rajamäki, Rathod & Kämppi 2014). European LEAs' GNSS-based tracking systems are based on GPS. The US Department of Defense operates the GPS systems, but they cannot guarantee maintenance of global uninterrupted service. If GPS signals were switched off in Europe tomorrow, LEAs efficiency would suffer heavily, and public safety would be jeopardized.

Current GNSS-based tracking systems are complex and open to various kinds of data delivery problems, data losses and cyber-attacks. Most systems are GPS- and GSM-dependent for positioning and communications. They include no cross-over possibilities, and their positioning is not based on parallel satellite systems, known WLAN networks, mobile phone cell location, RF/DF, etc. Also, the systems lack intelligence: They can be commanded, but they do not have the ability of self-reacting and alerting. Furthermore, available commercial products are vulnerable to jamming without jamming detection possibilities, and their power consumption is not always optimized (Rajamäki & Viitanen 2013).

During the SATERISK project, the model shown in Figure 6 for identifying threats related to GNSS-based tracking was created. The identification of threats began by listing well-known technical threats. The whole risk analysis process is reported by Kämppi and Guinness (2010). The asset they chose to investigate was location data. First, they defined the segments of the system, and then they grouped the threats according to the segments in which they occur. They discovered that a single technical threat can be the cause for a higher-level threat. For example, the cause of a tracking failure can be a technical problem in a tracking device. The technical problem is a lower-level threat, and the tracking failure is a higher-level threat. They also noticed that higher-level threats can help to detect lower level threats. A data privacy threat is a higher-level threat, and the technical reason for it is a lower-level threat. Next, they investigated whether a higher-level threat could occur in the other segments of the system. For example, privacy threats can be caused by many technical reasons in many segments. This cycle generated relationships among all threats and segments. When they had sorted all well-known threats, they added operational/business requirements (Kämppi & Guinness 2010). Table 8 summarizes the main threats, grouped by system segments and categories, resulting from this methodology.



SOURCE: modified from Kämppi and Guinness (2010)

FIGURE 6 Model for identifying technical threats of satellite-based tracking

TABLE 8 Technical vulnerabilities in satellite-based tracking systems

System segment	Threats
Control segment	Error in monitoring data, Error in adjustment commands
Space segment	Natural disasters (e.g., solar storms, ash cloud from volcano eruption), Collisions in the orbit, Unintended interface, Intentional interface, Atmospheric conditions, Multipath propagation, Selective availability, Total signal loss
Tracking segment	HW fault, SW fault, Power feed break-down, Clock drift, Signal attenuation, Information security diminution
Communication segment	Capacity, Radio coverage, Roaming, Latency, Information security diminution
Data processing segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution, Database corruption
End-user segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution

The SATERISK project has also extensively studied risks other than technology-based ones of GNSS-based tracking from different points of view. All end-users of tracking devices and systems face some risks when they use tracking; also, being tracked by someone else is a problematic issue. One interesting area is the evaluation of risks from satellite-based tracking in different corporate sectors and for different uses. The risks that are likely associated with satellite-based tracking are caused by financial, political and natural causes. Because of these risks, all the different end-users of satellite-based tracking need to be updated, both technically and mentally. The availability of different services will most likely increase as new service providers come to the growing market in the future. A variety of services is growing, and the customer has to expend more time and effort to determine the best and most reliable alternatives. Keeping one's information up to date is crucial (Guinness, Pitsinki & Penttinen 2012). For example, responsibility issues of international cross-border satellite-based tracking services have been gradually taking shape only recently (Viikari 2011). Private-sector companies use satellite-based tracking systems widely in cross-border traffic for localization of consignments, equipment and vehicles. In the public sector, tracking systems are used for establishing situation awareness and to support the operations of LEAs. In the future, an accurate picture of the situation will also be needed by security and other companies involved in positioning. The SATERISK project has also highlighted the necessity of cooperation between the public and private sectors in terms of the development and use of this technology (Erling 2012).

Morover, risks from legislation, or lack of legislation, have been interesting issues in the SATERISK project. The University of Lapland concentrated on the regulation and legal problem areas, such as privacy protection, information security, state sovereignty and safety and responsibility and liability issues. Their research had a geographical focus: national, the EU and the Schengen Region and Russia. In Viikari's (2011) study, the following four challenges arose: (1) privacy, (2) data security, (3) national security and sovereignty and (4) responsibility issues of positioning and tracking services and products. With respect to the lawfulness, the Laurea University of Applied Sciences gave guidelines for the activities of all users of satellite-based tracking, from authorities (Ojala 2010) to private navigators at sea (Kokkonen 2010). When analyzing risks in satellite-based tracking, we must always know and take into consideration the existing legislation, and the gaps where legislation is missing. International space law does not solve the privacy problems related to positioning activities. There is no specific privacy-oriented satellite-based positioning and tracking regulation in the EU. Only a few states have enacted laws directly related to positioning and tracking; even fewer have legislation about their privacy issues (Viikari 2011).

2.3.2 GNSS technology for law enforcement

GNSS-based sensors and systems are very useful to law enforcement when tracking non-cooperative targets. The technical architecture of GNSS-based tracking systems is composed of different segments, and each of these segments has its own set of risks and threats. Nowadays, law enforcement finds and relies on new uses for GNSS technology to assist in investigating crime and gathering evidence. LEAs need to have forensics technology for investigations and field work. These kinds of technologies include advanced tracking systems that apply GNSS technology to track criminals and vehicles that have been tagged. This allows LEAs to keep track of suspicious activity and can help solve cases. For example, in the US, the Congressional Research Service has reported the following examples (Smith 2011):

> After 11 attacks on women were reported during a six-month period in two Virginia counties, police installed a GPS device on the van owned by a man who lived near the crime scenes. The suspect was a convicted rapist who had served 17 years in prison. By tracking his movements with the device, police were able to intercept him in Falls Church, VA, where he was dragging a woman to a remote area. The series of assaults ceased after his arrest.
>
> Wisconsin police, acting on a tip about a former methamphetamine manufacturer, attached a GPS device to the suspect's car without first obtaining a warrant. Information recorded on the device led them to a large tract of land visited by the suspect. With the consent of the landowner, they searched the property and found paraphernalia used to manufacture methamphetamines. The suspect was subsequently arrested.
>
> Police in New York used evidence acquired from a GPS device (attached without first obtaining a warrant) that had been attached to a burglary suspect's car a year earlier. The device, which monitored the suspect's movement without interruption for more than two months, showed that the suspect had driven by a burglarized

store. This evidence was used to corroborate a witness's testimony that the suspect had been observing the store to determine its vulnerable points.

In California, the Los Angeles Police Department outfitted its cruisers with air guns that can launch GPS-enabled 'darts' at passing cars. Once affixed to a vehicle, police can track it in real time from police headquarters. The air guns are generally used in situations requiring immediate action such as a high-speed chase. [17]

2.3.3 Sensors for tracking non-cooperative targets

With respect to the tracking of non-cooperative targets, LEAs have many problems. The size of the available tracking equipment is too big, which restricts concealment possibilities. Power consumption is too high (maintaining devices during operations brings risks of being exposed, etc.); there is scalability, but low power options mean lower data quality, so alternatives should be found. The systems are GPS- and GSM-dependent for positioning and communications; there are no cross-over possibilities—for example, positioning could be based on using different satellite systems, known WLAN networks, mobile phone cell location, RF/DF, etc. Morover, intelligence is lacking from the systems; they can be commanded, but they do not have the capability of self-reacting and alerting (Rajamäki & Viitanen 2013).

Unintended interferences can be caused by other radio transmitters that are working nearby the frequencies used by the GNSS systems. Also, weakly shielded or faulty electronics can cause interference. All GNSS systems use the same frequency, which could cause interference problems if the systems are not designed properly (Parkinson 2010). GNSS systems operate in the IEEE L frequency band, located from 1 to 2 GHz (ICD 2010) and shared by many telecommunication systems. According to Kaplan & Hegarty (2005), such systems include: aeronautical navigation systems like civilian distance measuring equipment; air traffic control radars; military and government systems for terrestrial communication, navigation and identification; amateur radio communications; telemetry and telecom services for aircraft and missiles; digital audio broadcast and mobile satellite communication systems like Inmarsat and Iridium (Kaplan & Hegarty 2005). Actual radio frequency measurement campaigns have reported that loss-of-lock on the navigational signals can happen to unaided GNSS receivers near radio and TV broadcast transmitters (Klinker & Pietersen 2000). Another recently reported case dealt with telecommunication systems and GNSS interworking. According to Edwards (2011), in the US, LightSquared's 4G mobile communication network may cause interference with GPS signals because it is using almost the same frequency. His simulation results showed that the interference starts at 22.1 km for the aviation receiver and total signal loss occurs at 9.0 km from the transmitter (Edwards 2011).

Furthermore, available commercial products are vulnerable to intentional interference, which can be caused by sending interfering signals on the same

---

[17] A. Smith, "Law enforcement use of global positioning (GPS) devices to monitor motor vehicles: Fourth amendment considerations," Congressional Research Service, Tech. Rep. R41663, 2011/02/28. 2011.

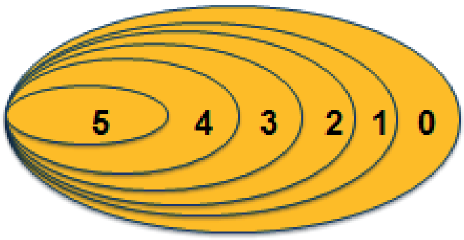
frequency band that the satellite systems are using. Any piece of equipment used for generating interfering signals is called a “jammer”. Multifunctional jammers can generate intentional interference for mobile radio network frequencies as well as for GPS. Prices for portable devices start at around $30, and the effective range is 2–20m—their easy availability and minor cost causing frequent threats. Most of the tracking devices available today have no jamming detection and accept the false signals as real ones because the false ones are stronger and easier to receive (El-Bakry & Mastorakis 2009). The current sensors cannot distinguish jamming from a normal situation where the satellites are not visible to the tracking device. This means that when criminals are using jamming, there is no way for the LEAs to detect whether the disappearance of position information is due a lack of satellite visibility, some malfunction in the equipment or jamming (Rajamäki & Viitanen 2013). Nowadays, LEAs are finding a growing number of this type of jamming equipment in the hands of criminals.

Another way to trick tracking sensors is to use dummy satellites, so-called pseudo-satellites or pseudolites. Instead of jamming, pseudolites imitate satellite signals, and this corrupted satellite data cause wrong positioning for tracking sensors (Happonen et al. 2009). A study by Happonen et al. (2009) offers some perspectives on signal interference and jamming detection. According to the study, jamming may be either intentional or non-intentional. The redeeming feature is that at least GSM jamming is quite easily detectable. The downside is that equipment for short-range jammers can be easily acquired at a low price. For LEAs, it is important to recognize whether the interference is unintentional or intentional. In another study, (Happonen 2010) describes ways to improve tracking sensors and user habits by developing countermeasures to avoid intentional interference.

2.3.4 Enabling technologies for GNSS sensors

The European LEAs can be independent only if their tracking is based on the European GNSS, Galileo. It will allow positions to be determined accurately even in high-rise cities, where buildings obscure signals from today’s satellites. Galileo will offer many signal enhancements making the signals easier to acquire and more resistant to interferences and reflections. European GNSS will deliver more precise and reliable services than the American and Russian systems. By placing satellites in orbits at a greater inclination to the equatorial plane, Galileo will also achieve better coverage at high latitudes, making it particularly suitable for operation over northern Europe, an area not well covered by GPS. A large proportion of equipment now uses GPS and GLONASS satellites together for positioning. Compass and Galileo will be ready in less than 10 years, meaning that by 2020 the number of navigation satellites will be well over 100 (Stigell 2012). The Iridium satellite system can be used as a local navigation system for Polar Regions because it has better coverage at the two poles than that of the GNSSs (Shiyue Fan et al. 2012).

Many companies are developing tracking sensors and miniaturizing them; some are even considering the power consumption. However, most are concentrating only on hardware size. Military devices are very sophisticated, but their power consumption is high because their main purpose is for Blue Force Tracking (tracking own vehicles and people) and not for enemy tracking. This means that availability of power is not a problem: Because tracking sensors are in your possession, it is easy to change batteries or use other power sources from the vehicle. Power consumption also greatly depends on how you use the equipment. Smaller hardware size with no reduction in battery consumption helps only marginally because the actual hardware is usually already smaller than the battery back. Figure 7 shows all relevant miniaturizing levels of tracking sensors.



0 Starting point: sensors and battery now
1 Add: Optimizing the use with AI
2 Add: Better sensor software
3 Add: New battery or other power source technology
4 Add: Lower hardware power consumption
5 Add: Smaller hardware size

SOURCE: modified from Rajamäki & Viitanen (2013)

FIGURE 7 Miniaturizing levels in tracking sensor development

The majority of tracking sensors consume an unreasonable amount of power for long-lasting mobile use. The power consumption of a tracking sensor is not a problem in Blue Force Tracking when vehicles' large batteries and chargers are available. But power consumption is a critical factor if only batteries are available. Most sensors are "stupid," requiring command for almost all tasks. Usually a tracking sensor includes only motion detectors, but if the motion of the sensors stops, the sending of position information also stops until the motion continues. Machine learning (ML) and artificial intelligence (AI) offer many possibilities for developing better tracking sensors. ML is an old branch of AI. As early as the 50s, (Samuel 1959) defined ML as a field of study to provide computers the ability to learn without being explicitly programmed. ML develops algorithms that take as input empirical data, such as that from sensors or databases. The algorithm is designed to (1) identify relationships thought to be features of the underlying mechanism that generated the data and (2) employ these identified patterns to make predictions based on new data. The algorithm acts as a machine learner that studies a portion of the observed data to capture characteristics of interest of the data's unknown underlying probability distribution, and employs the knowledge it has learned to make intelligent decisions based on new input data (Wernick et al. 2010).

In practice, all requisite power of every mobile tracking sensor is stored inside the sensor's own battery, from which it is consumed when needed. Many

GNSS-based tracking sensors are very small and require little power, but their applications are limited by reliance on battery power. The new battery technologies will allow many new tracking applications. New high-power rechargeable battery technologies based on the elements of lithium and sulfur are under development. The combination of these two elements yields a battery system with the highest theoretical gravimetric and volumetric energy densities of any known useful battery couple. It differs from lithium-ion batteries in that its cell voltage is no longer 3.6 V, but rather varies nonlinearly in the range of 2.5–1.7 V during discharge. Lithium-ion batteries are found everywhere from laptop computers and hybrid cars to electric power grids. A limitation of lithium-ion batteries, though, is the amount of power they are able to store. Researchers have identified silicon as a material that can store 10 times more power than conventional technology. However, it swells more than three times its volume when fully charged and then shrinks again during discharge (Roan 2011).

The most common way to recharge batteries is by mains power when the mobile device is not in use. However, energy is everywhere in the environment in the form of thermal energy, light (solar) energy, wind energy and mechanical energy. Unfortunately, the energy from these sources is often found in such minute quantities that it cannot supply adequate power for any viable purpose. Until fairly recently, it wasn't possible to capture such energy in sufficient amounts to perform any useful work, but this situation is about to change. According to the Energy Harvesting Forum [18], energy harvesting is the process of capturing minute amounts of energy from one or more of these naturally occurring energy sources, accumulating it and storing it for later use. According to the Forum, energy-harvesting devices efficiently and effectively capture, accumulate, store, condition and manage this power and supply it in a form that can be used to perform a useful task. Similarly, an energy-harvesting module is an electronic device that can perform all these functions to power a variety of sensor and control circuitry for intermittent duty applications. Scavenging energy from ambient vibrations, wind, heat or light could enable smart tracking sensors to be functional indefinitely.

2.4 Communication systems

As Figure 5 shows, telecommunications technologies have an important role within tracking systems: The communication segment delivers positioning data for post-processing and, further, to end-users. In most cases, the tracking device sends positioning data via mobile networks. The Internet or other networks are used to route positioning data from mobile networks for post processing, and this makes the system globally available. End-users can access their data via multiple different communication networks, as well.

---

[18] Energy Harvesting Forum [online] http://www.energyharvesting.net/

The Global System for Mobile Communications (GSM) is the second-generation mobile communications (2G) standard created by the European Telecommunications Standards Institute (ETSI). The General Packet Radio System (GPRS) is an extension of GSM and offers mobile packet-switched access. The data rate offered is 40-300 kbit/s, and the round-trip time (RTT) is up to a few seconds. GSM enables connectivity in more than 200 countries covering over 80% of the world's population. The Universal Mobile Telecommunications System (UMTS), also called the third-generation mobile communications system (3G), is the successor to GSM. It offers voice, messaging and data services. UMTS' data rate is up to 14 Mbit/s and its RTT is shorter than that of GSM. The radio coverage of UMTS is continually growing and currently covers the most populated areas. Short Message Service (SMS) is the messaging service of GSM and UMTS. It allows users to send and receive text messages on a mobile phone. The maximum length of those messages is 160 characters, and they can be sent globally via different operators. Long Term Evolution (LTE) is a fourth-generation (4G) telecommunication standard. LTE offers a packet-optimized service without native support for voice communication. The data rate offered is up to 300 Mbit/s with low RTT. The first commercial networks were launched in Scandinavia in late 2009.

Worldwide Interoperability for Microwave Access (WiMAX) is based on open 802.16 standards. WiMAX offers a packet-switched service and voice communication is not supported. 802.16m offers pick data rates of 1 Gbit/s for fixed line and 100 Mbit/s for mobile users. In February 2011, WiMAX was deployed in 149 countries and covered 823 million people (WIMAX Forum 2011).

Terrestrial Trunked Radio (TETRA) was developed for professional services, especially for public safety and security like police and fire departments. It gives voice, short data and packet data services. Strong security features and dedicated capacity are essential for professional use. The latest release of TETRA offers data rates up to 500 kbit/s. The Finnish nationwide VIRVE network is based on the TETRA standard. The TETRA Enhanced Data Service (TEDS) standard is a major upgrade from the narrow-band TETRA system to supply professional users with high-speed IP packet data services over wireless mobile channels (Nouri et al. 2006).

Satellite data services are typically provided to users through Geostationary (GEO) satellites, which can offer high data speeds. Most communications satellites use C-band (Comprise), which is a portion of the microwave band ranging from 4 to 8 GHz with a wavelength of around 5 cm. Downlink frequencies (space to earth) are around 4 GHz, and uplink frequencies (earth to space) are around 6 GHz. The band is also used for radar, including weather radar, and Radio LAN in the 5 GHz range. The Broadband Global Area Network (BGAN) is a newer satellite network from the International Mobile Satellite Organization. BGAN will offer transmission speeds of theoretically up to 492 kbps. Actual data rates will be lower, depending on the satellite terminal used. BGAN will offer both voice and data services. It supports both packet-switched services based on IP as well as traditional circuit-switched services. BGAN uses the new series of Inmarsat-4 satellites offering coverage around the whole globe with the exception of the Polar Regions and parts of the Pacific Ocean. Services will be offered to land-based, airborne and maritime users. GEO satellites' communications coverage is at about 70 degrees North / South. In comparison to a GEO satellite orbit with an altitude of 35,786 km, a satellite in a Low Earth Orbit (LEO) of 780 km has an additional free space gain of 19 to 32 dB, depending on the position of the LEO satellite relative to the ground segment (Haddock et al. 2012). According to Frost and Sullivan 2010), Iridium is the only Company that offers coverage over the entire globe. The 66 LEO satellites in the Iridium constellation are cross-linked satellites in space, providing a fully meshed network in space. The approach of networking the satellites together in space as opposed to terrestrial network infrastructure in-between ground earth stations enables the satellites to talk directly to each other in space (Haddock et al. 2012). The system provides critical voice and data services for areas not served by terrestrial communication networks. Although the Iridium data link is slow (2.4 kbps), it suffices for secure tracking services.

2.4.1 Technical threats to mobile communications

This section discusses technical threats that are specific for mobile communications: that is, user plane capacity, latency, radio coverage and roaming.

Mobile communications user plane capacity could be a problem in highly populated areas. The rapidly growing use of mobile Internet stresses mobile networks. Rural areas might have very limited GPRS capacity or there may not be GPRS capacity at all. High amounts of mobility require network signaling capacity. 3G offers higher data rates and more capacity than GSM, but the usage of 3G is increasing due to the real mobile Internet experience that it provides. Networks can run out of capacity in highly populated areas. SMS delivery does not reserve radio network user plane capacity like GPRS or normal speech because SMS is delivered within a signaling channel. However, high amounts of mobility require high network signaling capacity, and SMS capacity is dependent on the operator. Internet capacity depends on access network capacity, core network capacity and current network load.

Latency, the measure of time delay experienced in the system, might be a problem. Round-trip time in GPRS can vary a lot, sometimes being greater than 1000ms. 3G offers much lower RTT than GSM—typically 200–300ms. SMS' delivery time can be down to 10 seconds, depending on the operator and location. If an SMS is not delivered at first try, it will be buffered by the network for resending. On the Internet, delivery time of the data depends on the capacity of the access network as well as the current network load and distance between delivery points.

Although GSM offers wide connectivity, there are areas without GSM radio coverage. Some parts of the US, Canada, South America, Africa, Russia and Australia have their own 2G systems still running today. 3G has good radio coverage in the northern, western and southern parts of Europe. Other parts of the world are currently expanding their networks. There is a lack of unified coverage across the globe with these technologies. The radio coverage of commercial mobile cellular communication networks has huge gaps in remote and sparsely populated areas. Deep valleys and fjords are especially very problematic areas. In addition, these networks are vulnerable to breakdowns during extreme weather conditions, when safety and security systems are needed the most. TETRA networks are quite robust for extreme weather conditions. Although TETRA coverage in Finland is quite extensive, the situation is not same everywhere. With regard to satellite communications, the coverage of geostationary communication satellites is at about 70 degrees North and South; for example, Utsjoki in north Finland is situated at 69°54′25″N. Iridium's crosslinked satellites offer coverage over the entire globe (Frost & Sullivan 2010).

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 or 3G. 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 cooperation 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 was 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.

2.4.2 Multichannel communications

Multichannel communication is a method for simultaneously using several communication paths provided by various telecom operators. Multichannel communication means parallel use of data channels regardless of technology. For end-user applications, all the multiple parallel communication paths should appear as a single uninterruptable path. People can use parallel communications paths simultaneously if they want; they can collect and integrate information coming from different sources, as the left part of Figure 8 illustrates.

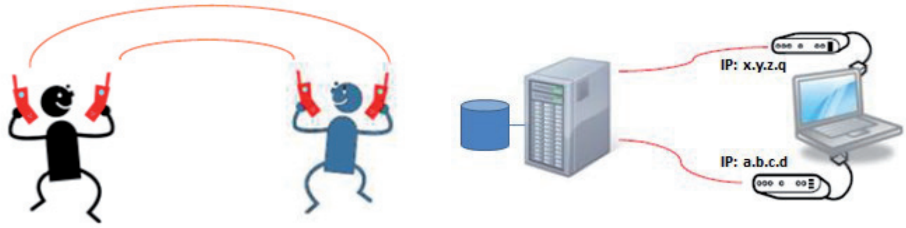


FIGURE 8 Simultaneous utilization of parallel communication channels

However, computers are technically not able to do this, even if they 'wanted' to, because the IP protocol used for data transfer cannot bind a socket over two or more physical connections simultaneously. That is one of the most serious shortcomings in multichannel communication: IP is not 'good' at multi-channeling. On the one hand, creating a multichannel communication solution utilizing the Virtual Private Network (VPN) technique solves some problems, while on the other hand, it ties the solution to the VPN system. The real challenge for us is to overcome the fact that the VPN solution covers only a fraction of the total need.

The IP protocol has poor control of priority, and services should adjust to the physical transfer capacity. For that reason, low capacity lines can transfer only high priority data.

All centralized solutions are vulnerable to many threats, which include denial-of-service (DoS) attacks, system failures, repudiation, spoofing and tampering. Therefore, decentralized modular communication and information management systems should be used; if one part goes down, other part works. Also, turning to the services of a single operator is a risk. Utilizing parallel connections of multiple operators ensures connectivity, minimizes risks and maximizes reliability.

Tracking applications need secure seamless wireless communication solutions with selectable levels of quality-of-service (QoS) and wide coverage areas. Even though publically available wireless services usually provide reasonable coverage under acceptable cost conditions, most of the public providers do not offer any data service with a guaranteed QoS level. The principal improvement of QoS can be arrived at by the selection of the best possible alternatives from the set of currently identified available services, or by applying multiple communications systems in parallel.

The distributed systems intercommunication protocol (DSiP) allows the use of several parallel communication paths simultaneously, handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution (Nordman et al. 2003). Efficient decision processes must be adopted to reach the relevant QoS. The success of such an approach relies on a profound understanding of applied technologies and their performance described by their performance indicators. A DSiP router's QoS option sets the desired order of the network access by desired cost-of-service (CoS) value (Holmström, Rajamäki & Hult 2011).

Especially in remote and sparsely populated areas, parallel use of multiple communication systems increases coverage, but at the same time the size of the device will be larger, which increases power consumption. Small (20x20x3 mm) and low power (consumption in idle mode: <2.6 mA, speech mode: 270 mA average) 2G/3G modems are available.[19] Several TETRA modems supporting simultaneous short data services (SDS) and packet data services can be used to develop a variety of TETRA data solutions, including customized telemetry de-

---

[19] http://www.gsm-modem.de/module-gsm.html

vices, personal digital assistants and tracking devices. Their smallest sizes are about 50x50x5 mm, and current consumption is 1.8 A (4 V). Small satellite modem modules are available: for example, Thuraya has launched a 70x50x10 mm unit designed to fit into other devices. A commercially available tracking system applying the Thuraya Module consumes 3 W during transmission.[20]

2.4.3 Cyber-security

Traditional information assurance has at least five dimensions: availability, authenticity, confidentiality, integrity and non-repudiation. Violating any of these may cause considerable harm. Many articles dealing with the information security of satellite systems have recently been published. For example, (Driessen 2012) describes how the encryption of a satellite telephone system could be cracked in less than one hour. Systems may be the target of cyber terrorism, cybercrime or cyber vandalism. One way to act against such phenomena is to raise awareness of technical risks, even of those risks that may be inherently included in information systems in general.

It is undeniable that the communication of military and security authorities must be secured. Modern critical infrastructures include not only physical components and hardware, but also software, services and intellectual properties. These integrated systems are examples of cyber–physical systems (George 2008). The term 'assurance,' in the context of CI, has many similarities with traditional communications assurance (George 2008). Consider the water supply: Availability is the first requirement, but integrity is an additional concern. Integrity ensures that the supply has not been tampered with or contaminated—in other words, that it remains in its original state. The health care industry must consider availability, integrity, authenticity and non-repudiation. The security needs of CI follow the assurance model of traditional information security (George 2008). By now, some of these challenges are known and are receiving attention from the research community and governmental agencies; for example, the European Network and Information Security Agency (ENISA) is such an organization.

As critical governmental communications become more digitalized, there are significant risks and threats. Traditionally, there are 'conventional' concrete challenges, such as natural phenomena, strikes, disruptions, war and information security problems, which have a fairly stabilized range of means. These conventional challenges are already affecting Quality of Services (QoS). In addition, there are 'new' challenges concerning intertwined risks and threats caused by cyber security problems, changes in ownership of telecommunications infrastructure, globalization of systems and business operations, extensive outsourcing chains and other changes in working structures (Manni 2011). A recent report published by the US government cites a 782% increase in reported breaches of federal agencies security in the last six years (Snyder & Mattingly 2013). A recent study also shows that growing threats of disruptions to operations for

---

[20] http://www.mobility.com.tr/Thuraya

government organizations rely on information sharing amongst their employees, partners, agencies and civilians (Snyder & Mattingly 2013). The mightiest challenge in the current situation remains the protection of CI, especially against the consequences of rapid changes and turning points. Meeting these challenges also assures superior QoS (Manni 2011).

Within the SATERISK project, identifying issues related to information security in satellite-based tracking systems is extensively studied by Kämppi, Rajamäki and Guinness (2009). The study introduces the technical architecture and data flow in GPRS and points out vulnerabilities and unknown issues in information security. The study concludes that applicable security solutions or satellite-based tracking systems are, however, available. Knowing how satellite-based tracking operates is important before considering all possible risk scenarios.

Information security threats include different kinds of threats at different levels. Delivery of an SMS is encrypted only on the radio interface. An SMS is delivered without encryption in operators' core networks and even between different operators' networks. GPRS offers data encryption only on the radio interface, whereas data are delivered without encryption in the core network. 3G information security is built on GSM security, adding many new security features. However, 3G has security problems: for example, the International Mobile Subscriber Identity (IMSI) is sent in clear text when allocating a Temporary Mobile Subscriber Identity (TMSI) to the user. The transmission of the International Mobile Equipment Identity (IMEI) is not protected; hijacking of outgoing/incoming calls in networks with disabled encryption is possible. On the Internet, data are not encrypted as default. Unsecured and sensitive data can therefore be a potential target for hackers and criminals.

In cross-border tracking operations, data are transferred via multiple telecom operators' networks. Normally, data are not encrypted in operators' core networks. Globally there are many different operators with different information security practices, so the end-user cannot rely on data being delivered safely. Data can be protected by establishing secure tunneling between the client and a data processing center or it can be encrypted before sending by using Secure Hash Algorithms (SHA) such as SHA-256, SHA-384 or SHA-512. By secure tunneling, data transfer can be made as secure as the chosen encryption method. The most common tunneling technique is IP Secure Architecture (IPsec).

2.4.4 Interoperability and the multi-organizational environment

In major disasters, not a single PPDR organization can work alone. Hence, cooperation is extremely critical between actors. The working parties should not simply trust and rely on their own resources. Regardless, only a few organizations possess all the required areas of expertise in a large-scale incident or disaster. Information sharing and education at the organizational level is required in order to achieve a working relationship between the actors. This requires actual and operational interoperability between the first-responding organizations—in reality in the field, not only in the form of an official agreement but on a much larger scale (Akella, Tang & McMillin 2010).

PPDR, CIP and MIL actors have multiple similar needs. Lapierre (2011) suggests that similarities in disaster relief operation scenarios include (a) severe disruptions in expected functionalities of critical infrastructures, such as transport, supplies and infrastructures; (b) operations in remote areas without transmission infrastructures; (c) cross-border operations and multinational teams; (d) high demand for interoperability; (e) a lack of remaining infrastructures after a serious disaster; (f) congestion or no use of commercial networks and (g) utilization of both adhoc networks and stable infrastructures. According to Lapierre (2011), similarities in command and control communications involve (1) a desire to obtain information on the operational environment, (2) a need for the decision maker to monitor operation (live feed), (3) a need to examine and issue orders and (4) a desire to assess the progress of the operational environment after an order has been issued.

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 et al. 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. The current situation needs complementary technologies in addition to TETRA. Research suggests that multichannel communications would solve the problem. There is a global demand for safe and secure multichannel communications, and it is expanding day by day.

2.4.5 Communication concept of the Finnish government

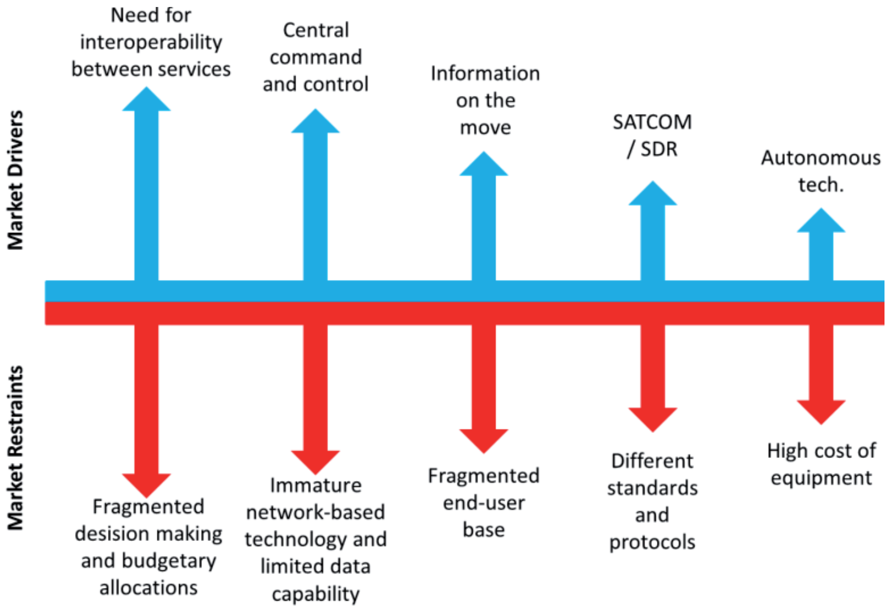
Finland is known globally for its high-tech information society. To meet the requirements of any society characterized as an information society, secure ICT systems that fulfill the prerequisites of businesses, government and citizens are needed. An obvious scenario is to synchronize services with the 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. 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 (Manni 2011, Benson 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).

The Finnish TETRA-based PPDR network VIRVE has been fully operative 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 like 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 are essential in PPDR field operations. 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). According to 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. According to Finnish authorities, the demand for data transmissions has increased many times over in recent times, and, based on their experience, a dedicated PPDR mobile data network is required (Riippa 2011). To serve highly demanding needs, such a future network should be independent of every individual public mobile network technology.

2.5 Command & control and intelligence

Most new digital services for the PPDR sector are supplied via stand-alone systems without built-in interoperability. There is a real lack of a coherent system that would coordinate the various technologies and improves the system's accuracy and usability. According to Frost's and Sullivan's study (Srimoolanathan 2012), the need for interoperability between services is the key market driver with regard to first responders' communications, command and control and the intelligence (C3I) market. The main market restraints are fragmented decision-making and budgetary allocations (Srimoolanathan 2012), as illustrated in Figure 9.



SOURCE: modified from Srimoolanathan (2012)

FIGURE 9 Key market drivers and restraints of first responders' communications, command and control and intelligence market

2.5.1 Remote operations and monitoring

Remote operation means the control and operation of a system or equipment from a remote location. In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. A law enforcement monitoring station is a workstation or place in which sensor information accumulates for end-users who need it. Monitoring systems include information collection, analysis and provision for end-users, which is front-deployed-knowledge. At present, many LEAs are still using point-to-point investigation tools and tracking systems, where the information is transmitted from the sensor to, for example, a laptop of the surveillance team for monitoring. These old-fashioned stand-alone systems create neither watermarks nor log file marks; the system only retrieves the information and stores it locally. For this reason, neither chain-of-custody nor social acceptance by transparency are achieved.

Today, the most important data system for Finnish police field operations is the POKE field command system. It consists of different kinds of maps, including aerial photos, patrol tracking, messaging, activity logs and information sharing. The system has access and enquiry facilities to various databases, and it includes resource management and dispatching as well as reporting applications. POKE has many other features, and various devices, such as fingerprint scanners, could be connected to it (Hätönen 2012). Other field command systems that have been studied within the MOBI project include the MERLOT product family developed by Lociga Ltd. and used in some Finnish regional rescue departments, SAFEcommand developed by EADS Astrium Company and used in rescue services in the United Kingdom and the army-specific Blue Force Tracking technology Force XXI Battle Command Brigade and Below used by the United States Army, the United States Marines Corps and the British Army (Rajamäki, Rathod & Kämppi 2013).

Many LEAs have no case officer resources in their control and command room (CCR) to observe on 24/7-basis the information that the sensors are producing. Some countries have a server-based centralized system based on CCRs with dispatch capabilities. These systems have capabilities to send orders (tasks) and to receive reports. When the number of sensors grows, this procedure becomes problematic. If you are not involved in the case and do not have a deep understanding of the context, it is very difficult to identify what behavior is normal and what is interesting or alarming; hence, important points can go unnoticed.

The end-user is not always the one actually controlling the sensor. In many cases, equipment is planted by technicians and not by the LEAs who are using it. In most cases, the control of the sensor is far from optimal. From the studies carried out within the SATERISK project, we know of many cases where the sharp-end equipment runs flat out and uses its batteries when no one is watching the information in real time and the density of the information is not needed (Rajamäki & Viitanen 2013). It is like running a car on a motorway in the first gear instead of sixth. The existing monitoring systems are developed for case-officers. There is a need to take into thorough consideration the organizational and procedural interoperability—for example, by explaining how the prosecutors and courts can have access to the system and to the evidence.

Essential parts of transparent LEA operations are strong authentication mechanisms and a provisioning system that enables the sensor to work only when it has permission from the central legal audit server. Unfortunately, an open, standardized provisioning system for multimedia covert investigation tools and tracking devices is missing.

2.5.2 Surveillance: security or an invasion of privacy

According to Wood et al. (2006), surveillance is purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection. Purposeful, in this context, means the monitoring has a point that can be justified in terms of a publicly agreed upon goal. Routine means that it happens as we all carry out our daily business. Surveillance is also systematic because it is planned and carried out according to a rational schedule. Finally, surveillance is focused. While some surveillance depends on aggregate data, most of it refers to identifiable persons. Their data are collected, stored, transmitted, retrieved, compared, mined and traded (Wood et al. 2006).

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).

The law enforcement surveillance operation that can be approved by the citizens must be transparent and possible to prove. Authorities can obtain more jurisdiction-based rights if citizens have more trust in the system. In a ubiquitously networked society, it is important that single-sided enforcement changes to multi-directional surveillance and develops transparent authority power. Transparency is needed because the new legislation must meet LEAs' needs even when there is a broad and sound trust base. People must be assured that the LEA is not abusing its power. Today, transparency can be based on technology that firmly supports operations' legal processes (Viitanen et al. 2012b). In Finland, the Act on the Openness of Government Activities upholds the principle of transparency. This means that extended information should be given to a person on the subject in question, including the circumstances under which data were collected and shared, protection measures and the identity of the officer involved in the case. Individuals and communities need to have an opportunity to control the use of the government and public allowances and be supported by the openness of the authorities in the task.

The United States Department of the Treasury initiated the Terrorist Finance Tracking Program (TFTP) after the 2001 terrorist attacks in New York. The objective of TFTP is to identify, track and pursue terrorists and their networks world-wide (U.S. Department of the Treasury 2011). The US Treasury Department issues subpoenas to a company that collects information on financial transactions worldwide: the Society for Worldwide Interbank Financial Telecommunication (SWIFT). The US Government receives information from SWIFT as part of specific terrorism investigations, and it is able to carry out targeted searches of SWIFT's records of in order to track financial transactions that may be linked to terrorist activity. SWIFT data aid in tracing terrorist organizations and their networks. By following the money, the TFTP has enabled the location of terrorists and their financiers and thus helped stop terrorism funding. Lives have been saved, thanks to that program. Access to financial transaction data raises questions about the privacy of citizens. SWIFT is overseen by a committee formed by several central banks, including the US Federal Reserve, the Bank of England and the Bank of Japan. The TFTP ensures it has precise safeguards and protocols regarding privacy. The program is regularly audited by an independent party (U.S. Department of the Treasury 2011).

Various surveys show that concerns about privacy have escalated over the past few decades, at least in the U.S. A great increase in concerns about intrusions into personal life has been noted. People also feel anxious about using computers, and this anxiety seems to be growing. The worry is greatest among people who do not use computers. Citizens are becoming more skeptical regarding allowing government agencies to post public records of personal information on the Internet. The respondents would be more willing to allow posting public records if the agencies had certain privacy guidelines (Robbin 2001).

In Europe, general data protection according to the principle of conservation of information is "kept in a form which allows the identification for as long as is necessary for the purposes for which the data were collected or further processed." Some countries consider three months as sufficient time for the storage of traffic data collected for billing and interconnection payments, while others, such as Romania, require a longer time. Member States' choices reveal a fragmentation with regard to the necessity for the length of the storage period of the traffic data. This concerns the principle of proportionality (Kosta et al. 2012).

Recently, a common agreement was reached at the European level about storage time identification, traffic and location data for law enforcement purposes. Directive 156 is about the retention of data between six months to two years. Directive 157 aims to harmonize the relevant provisions of the Member States concerning their obligations. There is a common recommendation to the electronic communications services or public communications networks to maintain the association of certain identification, traffic and location data that are produced or processed in order to ensure that the information is available for the detection, investigation and prosecution of serious crimes, as defined by each Member State under their national laws. Directive 158 shows that the European Member States have made different choices regarding the storage of identification, traffic and location data for law enforcement choices. The framework for this is provided by the Data Retention Directive (Kosta et al. 2012).

The European Commission has been collating the perceptions, attitudes and views of EU citizens on data protection issues (The Gallup Organization 2008). A wider survey and study was conducted under the title "Data Protection in the European Union: Citizens' perceptions." The survey reflects citizens' general feelings and concerns about data privacy and trust in different types of organizations that hold their personal data. The study also increases awareness of data protection rights and national protection authorities. According to this survey, the threat of international terrorism is an acceptable reason to restrict data protection rights. The opinion of the majority of respondents is in agreement with the notion that it should be possible to monitor passenger flight details (82%), telephone calls (72%) and Internet and credit card usage (75% and 69%, respectively) when the matter is connected with the prevention of terrorism. In this survey, it came to light that there was suspicion about any provisions that would allow authorities to relax data protection laws and, if that was done, it should be within clearly defined limits. Of the respondents, 27%–35% said that only suspects should be monitored, and 14%–21% wanted even stricter safeguards (The Gallup Organization 2008).

According to the same 80% of the respondents trust the police to use their data properly. The respondents reported trusting other public authorities such as associate security (74%), tax authorities (69%) and local authorities (67%). In addition, 66% of the respondents have trust in banks and other financial institutions. The confidence was highest in Finland and Denmark and lowest in Latvia and Lithuania. Age and education played a role in the respondents' trust in specific organizations. Concerning the age of the respondents, there was a pattern that the older the respondents were, the less likely they were to trust any of the listed organizations. Of the 15–24 years-olds, 84% trusted the police to protect their personal data, while only 78% of the over 55 years-olds believed so. Highly-educated respondents had more confidence in data privacy than less-educated respondents (The Gallup Organization 2008).

2.5.3 Digital forensics

Today, computer-based money transactions cover the majority of all money-related transactions, and most of the money around the globe is digital. On the other hand, forensic evidence is mostly based on physical evidence, such as deoxyribonucleic acid (DNA) samples and testimonies. This section deals with state-of-the-art digital evidence. This section discusses, for example, digital forensics, bank transaction techniques and forensics based on bank transactions. This section discusses the investigation methods that are used to resolve economic crime and how bank transactions could be used to help investigating these crimes.

Organizations have the need to collect evidence data on their networks to resolve computer intrusions, fraud, intellectual property theft, sexual harassment and violent crimes. According to Casey (2011), these data are useful to the organizations when they consider legal remedies against criminals who have targeted them. To hold up in court, the data must be trustworthy, which raises expectations about computer security professionals who need to have the training and knowledge to handle the digital evidence properly. According to Casey (2011), this means that corporations and military operations need to respond to and recover from incidents rapidly to minimize losses caused by these incidents. Because of the number of crimes that occur, the computer security professionals need to limit the damage and close each investigation as fast as possible. The rapid development in computer-related crime has created a demand for people who can collect, analyze and interpret digital evidence. Specifically, this involves preservation of digital evidence, extraction of usable information from digital evidence and interpretation of digital evidence to see more clearly the various aspects of an offence. These processes are not always carried out by law enforcement as they are sometimes conducted by corporations and single individuals (Casey 2011).

Computers are often used to provide digital evidence in a case because they contain lots of information. Computers can contain information about devices like Universal Serial Bus (USB) memory sticks, cell phones, digital cameras, and portable hard drives. Evidence is primarily found on computer hard drives, which contain accounts, log files, time stamps, images, and e-mails (Daniel 2011). Cell phones and cell phone service provider records include material for cell phone forensics and are commonly examined due their widespread use. Cell phones contain information like contacts, text messages, images, videos, audio recordings and e-mails. Deleted data from cell phones are possible to recover. According to Casey (2011), the more cell phones become computer-like, the more possible it is to recover deleted pieces of data. Data used as digital evidence consist of numbers that represent information of various kinds, including texts, images, audio and video (Casey 2011).

There are crimes of fraud committed in small businesses, large corporations, government bodies, and in non-profit organizations, for example. Fraud is committed by individuals who take assets from other individuals or organizations. Because these acts are usually covert operations, it is hard for employers to prove how or why they occur. Frauds are investigated and prevented by fraud examiners, who work on cases that involve acts such as bribery and property or monetary theft (Echaore-McDavid & McDavid 2009). According to Manning and CFE (2010), financial statements and tax-records should be obtained in fraud investigations. These records can be analyzed to see what the trends and conditions of the investigated target are. Investigation may be initiated if sales or assets have increased over the previous year. Or perhaps the deposits to the gross receipts reported on tax returns and the financial statements should be compared. Explanations can be sought if inventory, liabilities or assets do not increase (Manning & CFE 2010).

Forensic economists are retained for expert witness services in court. They provide input to the case by giving their professional opinion about the issues being dealt with, usually giving testimony at depositions, trials or other legal hearings (Echaore-McDavid & McDavid 2009). Business entities are examined with audit programs. In these programs, various kinds of evidence relating to economic events and transactions are collected by the examiners. Financial evidence is collected to sort out business entities' financial conditions (Manning & CFE 2010). According to Pickett and Pickett (2002), crime investigation is difficult because the environment has unclear rules and procedures. Fraud investigation might rely on records that are not as precise as required. Therefore, investigation requires accurate records if the underlying trail of transactions crosses through several accounts and records (Pickett & Pickett 2002). Many fraud cases involve threats and crimes committed by organization insiders and are considered for in-house measures only in order to avoid damage to the organization's brand through public exposure.

Business is increasingly being directed towards online services. This brings big risks for consumers who do credit card transactions over the Internet (Manning & CFE 2010). Today's criminals are often cybercrime organizations that use laptops and the Internet rather than guns and masks (BBC News US & Canada 2013). One way to start an economic fraud investigation is to do an analysis of financial statements to determine at-risk accounts and make a detailed examination of them. This can include analysis of bank statements and supporting documentation. Financial statements are reconstructed based on evidence, and actual revenues and expenses might be confirmed. If needed, reports and supporting documentation are issued. In this way, the evidence is sliced into logical pieces (Coenen 2009).

When credit card fraud is investigated, the card holder information submitted is reviewed. This may include the times when charges were incurred on the card. Among other things, the credit card receipts for the transactions are reviewed. This may often be sufficient to prove a fraudulent charge. These types of investigations are unfortunately time-consuming (Fox 2013). Bank statements, cancelled checks and deposit tickets are bank records that are useful financial documents for fraud investigations. Bank records are valuable evidence when tracing the money trail. This kind of documentation comes from independent third parties and is therefore considered very reliable. Bank documentation can be in a hardcopy or digital format, and it provides proof positive of how much was paid or received. The documentation also points to whom the payment was addressed or from whom it was received. This kind of documentation is instrumental in reconstructing the finances and determining where the money went if a company's accounting records have been compromised (Coenen 2009). Large banks have a large number of bank transactions, and analyzing their documents is time-consuming when the money flow is being traced. Multiple transfers between bank accounts can make it hard for investigators to trace the flow of the money. Besides this, the examination of bank records includes additional challenges because it may be hard to identify all active bank accounts if someone suspected of being involved in the fraud has concealed the existence of some accounts. The increased use of technology has made it possible for banks to produce account documentation with a few clicks of a computer mouse. The technology guarantees a higher level of accuracy and reduces manual human labor in identifying the checks (Coenen 2009).

2.5.4 Digital evidence

LEAs have a tendency to create two-level systems and solutions: one level for collecting information from the streets and another for showing evidence in the Courts of Justice (Manning & Van Maanen 1978). It is important to have generally accepted standards of practice and training in digital forensics because they reduce the risk of mishandled evidence and errors in analysis and interpretation. They can also protect innocent individuals from the consequences of false handling of evidence data. The aim of an investigation is to follow the trails that offenders leave during the commission of crime and to tie perpetrators to the victims and crime scenes. Tangible evidence of individuals' involvement tends to be more compelling and reliable than witness' identification of a suspect (Casey 2011). While hacking a computer, attackers leave multiple traces of their presence throughout the environment. This includes file systems, registries, system logs and network-level logs. It is also possible that the attackers have stolen passwords, or there are other elements that could be used to link an individual to an intrusion. The most volatile data should be collected first from the compromised computer. Volatile data, for example CPU registers, are the data that have the highest chance of disappearing or being damage on a running system. But because CPU registers are rarely collected, it is better to collect a memory dump first. This way no contents of memory will be compromised due to any process executed in the system (Casey 2011). While the hardware still contains the evidence data, it is necessary to seize the computer in question. It is the investigator's choice whether to investigate every piece of equipment found or only that which is essential to conserve time, effort and resources and avoid the risk of being sued for disrupting a person's life or business more than necessary. It is also possible that the size of the hardware or its quantity is too large to seize to be feasible (Casey 2011).

Digital evidence can be presented as a written summary, which is called the expert report: a well-rendered text that outlines the digital investigator's findings. An expert report may not contain assumptions or lack foundational evidence; it must contain solid arguments provided with supporting evidence. Assertions should be supported with multiple independent sources of evidence. The report should clearly state the origin of the evidence to help decision-makers interpret the report and to enable another digital investigator to verify results. The important items of digital evidence in a report include figures or attachments that are useful when testifying in court (Casey 2011). An expert report consists of (1) an examination summary, (2) a file system examination, (3) forensic analysis and findings and (4) conclusions (Casey 2011). An examination summary bundles up the critical findings related to the investigation. It is usually in a short form and is intended for decision-makers who have a short time window in which to prepare a decision. The examination summary summarizes the tools used in the examination, the recovery of important data and elimination of irrelevant data. A file system examination covers the file inventory, directories and recovered data that are relevant to the investigation. All the path names, date/time stamps, message digest algorithm values (e.g., MD5 values) and physical sector locations on the disk must be included in the examination. In Forensic Analysis and Findings, the report specifies the location where each item was found. It helps others to verify the results in the future. Photographs, screenshots or printouts of evidence can be included in this section. Conclusion references are the supporting evidence for the case (Casey 2011).

2.6 IT service governance

2.6.1 ITIL – continuous service improvement

The Information Technology Infrastructure Library (ITIL) offers a framework for the delivery of IT services. It is not only a best practice framework but also a philosophy shared by people who work in IT service management (Van Haren Publishing 2007). The fundamental service principle of ITIL is based on the five phases of the IT service life-cycle: Service strategy, Service design, Service transition, Service operation and Continuous service improvement (Van Haren Publishing 2007). Figure 10 illustrates these five phases and their relationships.

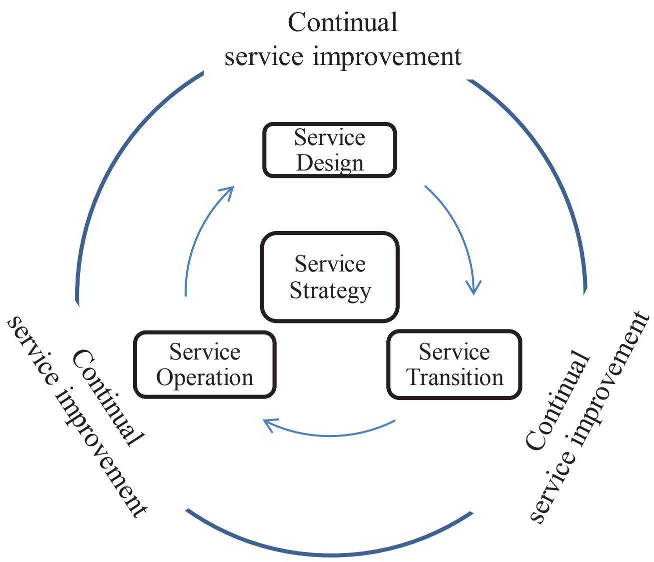


FIGURE 10 ITIL V3 – Service lifecycle

Service strategy is the core axle in the center of the design, transition and operation phases and continuous service improvements including the projects, learning and programs that improve the inner circle's performance and quality (Van Haren Publishing 2007).

2.6.1.1 RACI model

The RACI matrix is used to define roles and responsibilities within organizations. This RACI matrix captures the cross-supplier dependencies, roles and responsibilities of all suppliers in a multi-supplier organization. Following are the definitions of each of the roles: "Responsible" – the party authorized to execute the activity; "Accountable" – the party that owns the "bottom-line" for the activity; "Consulted" – the party involved in providing inputs to the activity and "Informed" – the party informed about the outcome of the activity (Gallivan & Wonseok Oh 1999). Using the RACI matrix to define clear responsibilities between suppliers is the key success factor in a supplier management. In multi-supplier environment, the roles of suppliers might be similar but their responsibilities might differ (Gallivan & Wonseok Oh 1999). Therefore, it is crucial to understand clearly and document the roles between suppliers and customers. Table 9 provides an example describing the different activities in rows and the parties with corresponding roles in columns.

TABLE 9 RACI example

Function R=Responsible, A=Accountable, C=Consulted, I=Informed	Helpdesk (Vendor A)	Infrastructure (Vendor B)
Incident Management Tool/Application Maintenance	I	I
System Monitoring and Alerts		A/R
Application Monitoring and Alerts		C
Incident Logging: Assign Severity, Priority, Application	A/R	I
Incident Escalation	A/R	I
Incident Response	I	A/R (if System)
Incident Closure	A/R	
Permanent Fix/Follow-up Activity	I	I
Applications Incident Reporting: SLA, Root Cause, Permanent Fix		I
Infrastructure Incident Reporting: SLA, Root Cause, Permanent Fix		A/R

SOURCE: (Ramakrishnan & Pro 2008)

In multi-sourcing engagements, suppliers who are individually accountable for their Service Level Agreements (SLA) are not usually accountable to each other. Here the rules provide a framework for collaboration and coordination among the suppliers. A development roadmap involves the creation of supplier dependencies between the suppliers and the determination of gaps in their management. An Operational Level Agreement (OLA) should be created to manage interdependent relationships between different suppliers to describe their responsibilities towards each other (Herz et al. 2011). The process of creating these rules needs to be carried out by a core group that includes authorized supplier representatives and the client organization. The client company's role is important in providing oversight responsibilities for implementation.

Unlike in traditional sourcing where a single supplier is given well-defined work units and is held accountable for them, in multi-sourcing none of the suppliers is accountable for the entire scope of work. Moreover, the rules of public procurement bring their own challenges in the field of PPDR. Distributed accountability makes supplier coordination and collaboration difficult for the client. Supplier governance through effective implementation of the RACI matrix can help the client organization extract the most value from its supplier network.

2.6.2 Enterprise service management

Hewlett-Packard has published an enterprise service management (ESM) framework for organizations to use with multiple suppliers. This framework describes the key points of the benefits and challenges of multi-sourcing (Yates 2012). How can it be determined whether such a framework is required and what the basic measurements for assessing whether the multi-sourcing is effective or not are?

According to Yates (2012), most organizations applying multi-sourcing face continuous challenges, and only very few of them have been able to achieve their expected targets. Multiple governances, processes and different reporting and support tools are killing the benefits derived from multiple suppliers, actually making multi-sourcing less effective than operations with a single supplier, in most of the cases. According to Yates (2012), in order to make multi-sourcing possible and conduct it in a proper manner, four criteria must be met: (1) To transform organization processes, governance and policies to support multi-supplier operations, it is necessary to create an aggressive transformation plan, which usually takes at least two years and incurs an approximately 5% increase in IT operations spending. The transformation plan must be supported by the executives of the organization. (2) Organizations must define why they are considering a multi-supplier scheme. Are the reasons cost savings, service quality, flexibility or something else? These reasons must be tangible and measurable. (3) Organizations must evaluate their current IT practices and assess whether they are mature enough for multi-supplier practices or need further development. (4) Once these organizations have defined the areas and objectives, they should take a phased approach towards the multi-supplier model rather than choose a ‘Big Bang’ approach.

In the ESM model, IT supply and IT demand organizations are separated. The ESM framework provides IT services with a single interface for the users of IT services. Users working in any division or in any country are able to request any service from the corporate service catalogue through this interface. The service providers remain invisible behind the corporate IT ESM framework interface. Ultimately, if the users are satisfied with the service quality provided through multiple suppliers, the model is working fine.

The challenge with the ESM model for IT organizations is to have all suppliers aligned with corporate IT operation, security and architecture policies and practices while still constantly developing them through business demand management. The requirements for the suppliers must be aligned with the policies and services provided to the end-users. If any of the suppliers are not compliant with the organization’s requirements for IT suppliers, it should not be used. Noncompliant service providers make corporate services weak, for example if they can't commit themselves to the tools, SLAs or processes required.

2.6.3 Utility based computing

The traditional outsourcing business is re-emerging and equipped with new business models. The applications are becoming increasingly web-based, which enables the new type of Software as a Service (SaaS) model. Another trend is server virtualization, which is driving capacity-based datacenter usage a bit further; this is known as Infrastructure as a service (IaaS). Tomorrow's IT will be increasingly based on services provided over the network as utility services, comparable to water or electricity services today (Ross & Westerman 2004).

Organizations are moving from outsourcing to cloud sourcing. For the client, it makes a big difference to use a utility-based IT infrastructure, where mailboxes are charged monthly per mailbox, and clients do not have to buy servers, licenses and perform the installations. The cloud services are bringing a revolution to IT that is similar to the industrial revolution brought to manufacturing. The provisioning of services is being consolidated to fewer suppliers, and with automation and large volumes the unit prices are going down (Wardley 2009). The client no longer needs to know the technical details of how much memory the server holds, just the requirements for the service. These requirements are further discussed in Section 2.6.6.

According to Ross and Westerman (2004) , there are risks associated with capitalizing on the potential benefits of utility computing, where client firms will rely more heavily on the technical—and perhaps business process—capabilities of suppliers. This reliance will reshape the risks associated with outsourcing. According to Ross & Westerman (2004), one of the challenging questions behind utility computing concerns the strategic processes that require certain IT services to be available. What happens if a supplier for any reason is not able or willing to provide that service? In the worst case scenario, this can lead to the lack of a particular PPDR service to citizens.

Partly due to the risks and the on-going revolution in utility-based services, we are in a situation where services are delivered in a hybrid mode. The environment consists of both utility-based services and traditional self-maintained and self-developed IT services. To manage IT consisting of various utility, outsourced and insourced services require advanced frameworks for IT governance to be effective. The governance model should be flexible enough to support the service strategy for both utility services and traditional IT services provided by both internal and external organizations. The study by Lehto, Rajamäki and Rathod (2012) examines which cloud-computing deployment model and cloud service model are suitable for PPDR. The study shows that new Enterprise Architecture (EA) will reduce some of the problems that appear when installing the programs locally when they are not intended to work that way.

This EA also covers the use of cloud computing in the PPDR field (Lehto, Rajamäki & Rathod 2012).

2.6.4 Selective sourcing

When organizations outsource only certain parts of their IT environment it is known as selective sourcing or smart sourcing. This can be compared to alternatives in which everything or nothing is outsourced. There is a model by Lacity, Willcocks and Feeny (1966) where the key areas to be kept in-house are defined. While these key-areas provide additional value when held internally by the organization, lesser key areas can be outsourced. This matrix is shown in Figure 11.

		Commodity	*Differentiator*
Contribution of IT activity to business operations	*Critical*	Best source	Insource
	Useful	Outsource	Eliminate or migrate

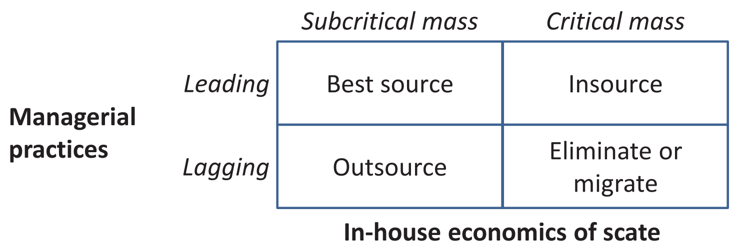
Contribution of IT activity to business operations

SOURCE: modified from Lacity, Willcocks and Feeny (1966)

FIGURE 11 Selective sourcing

Areas that should be kept in-house are critical strategic differentiators, services that are critical to core operations. Nearly always these critical differentiators are tailored applications that other organizations do not have. According to Lacity, Willcocks and Feeny (1966), critical commodities comprise a group that is required to run the operations but that does not provide additional value to them. A type of critical commodity is a system that is used only to fulfill legal requirements. As these could be standard commodity systems that customers are using, usually the best sourcing options for these systems are high-quality suppliers, if available. Useful commodities include standard services such as email or accounting that supports the operations (Lacity, Willcocks & Feeny 1966). This group of services is likely to have lower costs through external suppliers outsourcing through standardization and volume. Standard and often high-volume services can usually be provided most effectively as utility services. The last group of the selective sourcing matrix is useful differentiators. The problem with these is that they are always costly to maintain. They are usually tailor-made and require more management than standard systems. Outsourcing of useful differentiators does not help to bring the costs down. These systems should be migrated or eliminated as they lead to more costs than benefits (Lacity, Willcocks & Feeny 1966).

In some cases, outsourcing rather than insourcing is not as financially justified as one might expect. If the client is large enough, they could have the critical mass to provide the same service as the supplier would. The difference here is that external suppliers are also looking for a profitable margin for themselves. In the case where the client has the critical mass and managerial practices developed, it can be cheaper to insource rather than outsource due to the fact that the internal IT organization doesn't always need to be profitable (Lacity, Willcocks & Feeny 1966). The aspects of volume and management skills are illustrated in Figure 12.



SOURCE: modified from Lacity, Willcocks and Feeny (1966)

FIGURE 12 Supplier offerings vs. in-house capability sourcing

2.6.5 SLA based management

A Service Level Agreement (SLA) is defined as a formal written agreement developed jointly between a client and a supplier that specifies a product or service to be provided at a certain level in order to meet certain objectives. SLA helps to clarify responsibilities, improve communication, reduce conflicts, and build trust between the companies involved (Jahyun Goo & Kichan Nam 2007, Marques, Sauve & Moura 2007).

Service level management requires defined metrics to measure the service. The controlling of service is built on controlling the effectiveness of certain SLAs. As there cannot be hundreds of different SLAs, the SLAs in use must be well defined. There may be numerous performance indicators, usually known as Key Performance Indicators (KPI). The sample performance indicators for any process may include process speed, process volume, errors in process or cost of process. According to Jahyun Goo and Kichan Nam (2007), contractual elements under governance characteristics include a communication plan (documenting communication processes to facilitate consistent knowledge exchange), a measurement charter (specifying the tactical measures of service performance), a conflict arbitration plan (stating the parameters and conduct rules for involving a third party for resolving problems) and an enforcement plan (stating the appropriate incentives and penalties based on performance).

The changing of service levels should be possible during the contract period. The continuous change processes also make the requirements for service levels and quality change regularly. The client should maintain the option to adjust the service levels during the contract period, for example to change the measurement of process time to process quality.

A weak IT service (with little redundancy or with over-utilized resources) has an advantage in having a low running cost but may generate high quality losses in PPDR field operations. A service with much better availability and lower response times will possibly generate better quality PPDR field operations but will usually have much higher running costs. Thus, in both cases, the total financial outlay may be high. It appears that a middle ground can be found that will optimize the costs (Marques, Sauve & Moura 2007). SLA-based management requires that the key deliverables of the supplier as well as the metrics for the service be well defined. Enforcing very high SLA requirements that exceed business requirements could generate very high running costs for the IT service.

2.7 Conclusions of the theoretical framework

The main purpose of Chapter 2 is to provide background information and to develop the theoretical framework for the research questions of this dissertation from the research literature. Figure 13 summarizes the content of the review of the literature, adopting the software-intensive system layers approach from Hevner and Chatterjee (2010). There has been a gigantic shift from a hardware product based economy to one based on software and services. This has also been the fact with regard to law enforcement. For example, the ICT systems of a typical police vehicle already cost about the half that of a new vehicle (Tikanmäki, Rajamäki & Pirinen 2014). From every indication, the growth of the software layer, in size and percentage of the overall systems, will be the future trend. According to Hevner and Chatterjee (2010), the software layer is a makeup of software code, information and control within the context of an application domain. They continue that "the overlaps among these three concepts support varying methods and techniques of understanding and building the software layer of systems. For example, software architectures define structures for integrating the concept of code, information, and control for a particular application domain system."

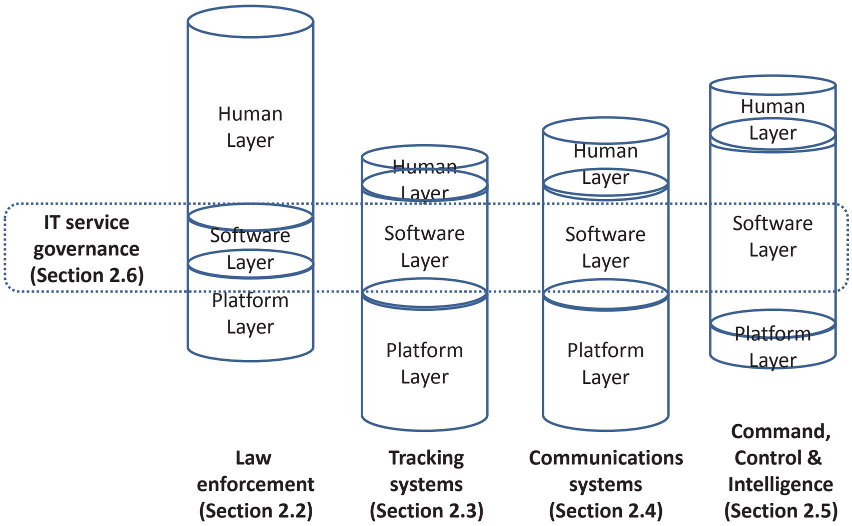


FIGURE 13 Summary of literature review from SIS point of view

According to Hevner and Chatterjee (2010), in the future world of pervasive computing and ubiquitous cyber-physical devices, it will be essential that IT artifacts and the integrated systems containing these artifacts be reliable, adaptable, and sustainable. Design for SIS should draw its foundations from multiple research disciplines and paradigms in order to effectively address a wide range of system challenges. According to Hevner and Chatterjee (2010), the most important intellectual drivers of future science of design in SIS research will be dealing with complexity, composition and control. Hanseth and Lyytinen (2010) adopt the viewpoint of designers: "how to 'cultivate' an installed base and promote its dynamic growth by proposing design rules for II bootstrapping and adaptive growth." Within their design rules, the II designers would have to prefer continuous, local innovation to increase chaos and to apply simple designs and crude abstractions. According to Hanseth and Lyytinen (2010), this change is not likely, as design communities are often locked into institutional patterns that reinforce design styles assuming vertical control and complete specifications.

3 RESEARCH CONTRIBUTIONS

This dissertation consists of eight articles, as studies, which are referred to in the text by their Roman numerals. First, this chapter presents the most significant research findings and the contribution of each of the eight studies by answering the expanded and iterative research questions presented in Chapter 1. Then, the main research question is answered by cross-case conclusions. The research methods used in these articles are discussed in Chapter 1 of this dissertation.

3.1 Operational environment

Study I deals with the research theme of LEAs' technical surveillance by providing an improved understanding of the operational environment in which LEAs apply GNSS-based tracking. The research question is: How can the operational environment be understood and categorized, where law enforcement authorities (LEAs) use tracking equipment for legal recording, retrieving and monitoring of criminal activities? The included conference paper can be referenced as follows:

> Jyri Rajamäki and Pasi Kämppi. Mobile Communications Challenges to Cross-border Tracking Operations Carried out by Law Enforcement Authorities. *International Conference on Information Networking (ICOIN)*, 2013, 560-565.

Organized crime has been increasing. To improve their evidence-gathering abilities, LEAs are constantly seeking new technological recording, retrieving and monitoring solutions that will facilitate their combat against criminal organizations. The criminals' counter measure activities, such as electronic counter-surveillance, jamming and constant changes in behavior to prevent eavesdropping or physical surveillance, are continuously increasing. The pressure to find new, hard-to-detect, strongly encrypted, long-lasting, quick-to-install and more adaptive intelligent technologies is building. Respecting the accountability and integrity requirements and smooth utilization of data in different phases of chains-of-custody is of utmost importance. In the current situation, the chain-of-custody is difficult to maintain due to different techniques that operate on their own while connected to different monitoring systems. This makes LEAs' work very labor-intensive; hence, the use of new state-of-the-art technologies should enable optimization of human resources. LE officers should have access to all investigation data, independent from the place and time. Special attention must be paid to the public awareness and concern over the use of surveillance equipment. However, legal recording, retrieving and monitoring of criminal activities in a safe and secret way also raises two problems: (1) how to ensure the accountability of a law enforcement officer who uses intrusive techniques and (2) how to ensure sufficient implementation of privacy safeguards. This also ensures that proper measures are used exclusively during overriding situations where interests prevail in a proportionate way.

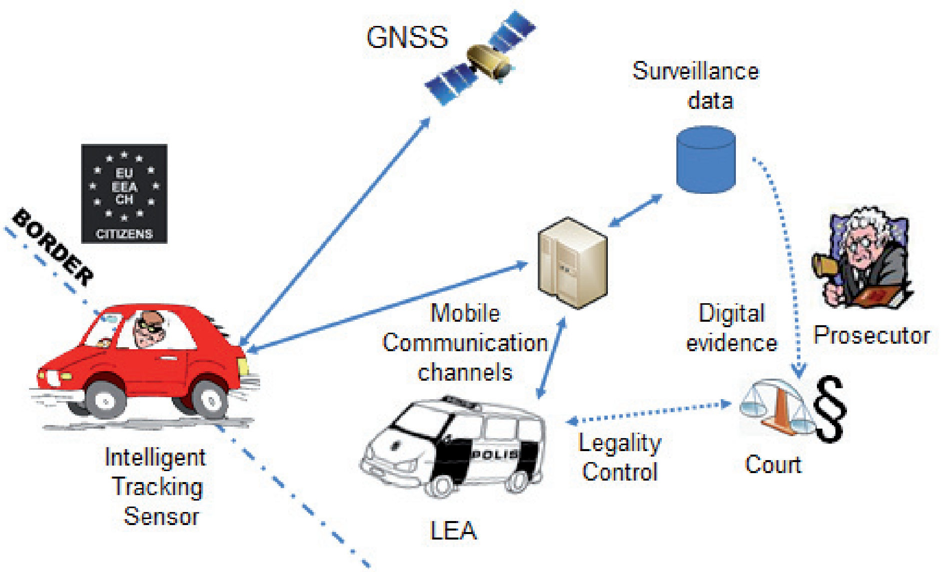


FIGURE 14 Operational environment

Figure 14 shows the operational environment where LEAs use GNSS-based tracking for non-cooperative targets. The existing solutions include identified deficiencies. With regard to operational and technological challenges, Study I identified the following five topics:

1) GNSS sensors: Commercial sensors do not fulfill the needs of LEAs.

2) Cross-border operations: Criminal activities have become internationalized, but LEAs are national organizations.

3) Secure mobile communications: This is becoming increasingly important in all operations.

4) Digital evidence: surveillance data should fulfill chain-of-custody requirements.

5) Transparency: It enables societal acceptance and monitoring-of-legality.

The topics from 2 to 5 are also valid for other systems and technologies apart from GNSS. After categorizing the challenges into five topics, Study I concentrates on the second and third topics, which that are discussed next.

3.1.1 Cross-border operations

Organized crime does not respect national boundaries, and international warehouses of crime involved in smuggling, drug and human trafficking and terrorism are becoming a stronger threat to European security. As a consequence, there is an increased need for European collaboration and information sharing related to investigation technologies; cross-border usability and interoperability of investigation tools have to be guaranteed. However, 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 the LEAs do not have common protocols and procedures in regard to how to pass information among each other. Particularly machine-to-machine (M2M) communication in cross-border covert operations has not yet been researched.

3.1.2 Secure mobile communications

Secure, uninterruptable communication is a pre-requisite in critical environments, for example in public safety applications and critical infrastructure telemetry. General purpose IP-based communication links may not be adequate or sufficient. For example, capacity of communication links and cyber warfare may present problems. Methods for ensuring constant connectivity and maintenance of unbroken communication in all circumstances are needed. Traffic engineering and multichannel communication may mitigate the aforementioned problems. The DSiP solution (Distributed Systems intercommunication Protocol) enables parallel use of different network technologies in a consistent and transparent way, enabling communications services platforms to be created. In cross-border operations, for example, this is a huge advantage.

Information security has at least five dimensions: availability, authenticity, confidentiality, integrity and non-repudiation. Violating any of these may cause considerable harm. Identifying issues related to information security in satellite-based tracking systems is a huge topic. The SATERISK project opened this playground. For example, it introduced technical architecture and data flow in General Packet Radio Service (GPRS) and pointed out vulnerabilities and unknown issues in information security (Kämppi, Rajamäki & Guinness 2009). Study I concludes that applicable security solutions or satellite-based tracking systems are, however, available. Study I also describes the major technical vulnerabilities of such systems. The field is divided into four segments: the satellite and tracking segment, the communication segment, the data-processing segment and the end-user segment. Each of these segments has its own set of risks and threats that can be reduced to an acceptable level. Preserving the confidentiality of data is seen as the most important issue.

3.2 Social acceptance of technical surveillance

Study II deals with the research theme of LEAs' technical surveillance in the following manner: (1) it provides an improved understanding of the theme of social acceptance of LEAs' technical surveillance and (2) presents the system with improved transparency and efficient surveillance operations that are acceptable to citizens. Study II is based on the results and lessons learned from the SATERISK project. The research question is: How can monitoring-of-legality of LEAs' actions and social acceptance of the use of tracking equipment be improved? The included conference paper can be referenced as follows:

> Jyri Rajamaki, Jutta Tervahartiala, Sofia Tervola, Sari Johansson, Leila Ovaska and Paresh Rathod. How transparency improves the control of law enforcement authorities' activities? *The European Intelligence and Security Informatics Conference*, 2012.

3.2.1 Transparency of surveillance

Study II weights the importance of transparency of LEAs' technical surveillance. The main issue in this study is trust. To prevent and investigate crimes, LEAs are able to conduct various operations that affect the privacy of citizens. People fear that a LEA can abuse its power and intrude upon their privacy, even though retaining phone data is not as intrusive as technical tracking or eavesdropping. Modern systems have some revealing features: for example, if phone or e-mail data are traced, the operator's system and log files will have marks indicating that a copy of the data has been delivered to the LEA.

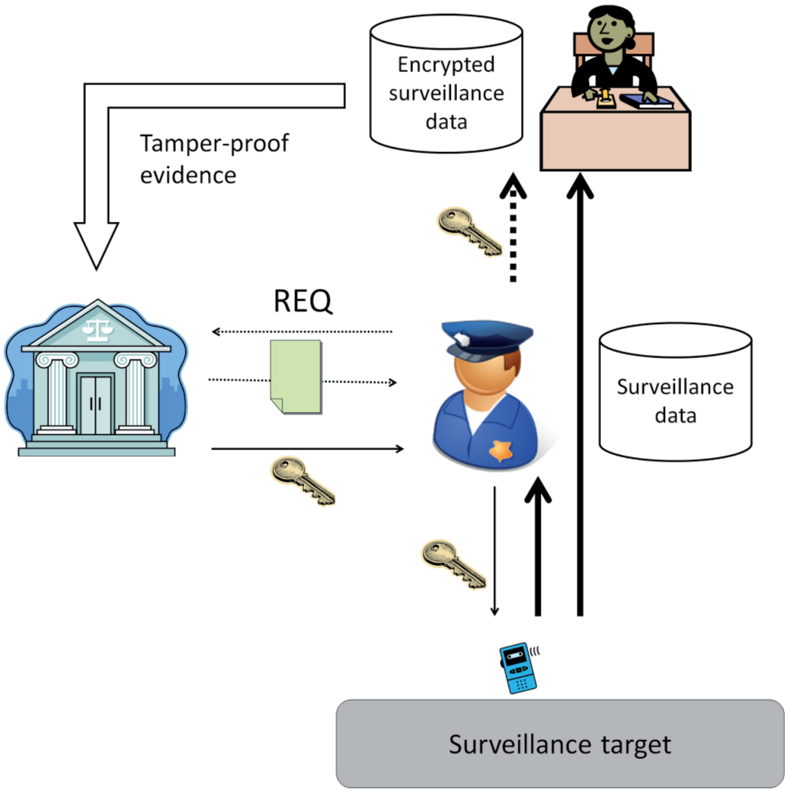
At present, many LEAs are using old-fashioned stand-alone investigation tools and tracking systems that create neither watermarks nor log file marks. For this reason, neither chain-of-custody nor social acceptance of transparency are achieved (Viitanen et al. 2012b). Non-transparent systems are a hindrance to LEAs. In general, LEAs act according to law, but they are not able to prove the correctness of their methods because these methods cannot be audited by a neutral outsider. The current practice is neither efficient nor transparent. With the lack of trust, there will also be a lack of new legislation that would allow the use of new crime-fighting tools. In this situation, all are compromising or losing security. A more advanced monitoring system is needed to provide faultless control of the surveillance equipment and procedures at all time. At present, no process or agency can present publicly accepted proof of correct use of equipment as long as there are no publicly proven technical control methods in the chain.

According to the opinion poll carried out for Study II, vague signs exist that Finns are willing to give more power to LEAs if the use of these intrusive means is made more transparent and can be better monitored by the public. The fact that makes this even more noteworthy is that in the all seven executed police barometers (1999, 2001, 2003, 2005, 2007, 2010 and 2012), more than 90% of Finns trusted the police. Results of the last barometer show that 48% of Finns trusted the police fully and 44% trusted them for most part (Marttila, Heikura & Käyhkö 2013). So, only 8% had no trust in the police. The recent results of the European Social Survey also showed trust in police in Finland (Jackson et al. 2011). The police are by far the biggest LEA in Finland. Hence, even when there is a widely accepted trust base, there is still a need for more transparency. What we can see here is that citizens are more willing to grant more jurisdiction-based rights to the authorities, if they have more trust in the system.

After the poll, a survey was conducted to find out the level of people's knowledge regarding how much information is being collected from them as well as their opinion on data collection. There was a significant positive sign from the result: The demand for privacy is blurred in the case of emergency situations, such as a disappearance. In emergency situations, people do not feel that their private life is interfered with if LE and rescue authorities use all the means available to them. In such situations, lives are often at stake. When it comes to other issues, citizens are more critical about who has the right to receive the location information at hand.

3.2.2 New solution for transparent and efficient surveillance

Figure 15 presents the idea behind transparent surveillance. When a LE officer desires to start a surveillance operation, (s)he submits a REQ(uest) to the court and gets the court order (thin dash line between LEA and court). The court also issues the mathematical encryption token for surveillance equipment (horizontal thin line and key). The LE officer forwards the token to the equipment (vertical thin line and key), which accepts it and sets the parameters for the operation as the court has ordered. The equipment collects data from the surveillance target (grey area) and encrypted them. The 'surveillance data' are consumed by LEA (thick line). All data are also delivered to the oversight officer at the same time (other thick line). The oversight officer can audit the conducted operations and related materials by contacting the LEA and asking for the key to access the data (thick dash line and key). All data are stored by both LEA and the oversight officer, but auditing the data contents requires an operation decryption key from the LEA. Without the decryption key, data cannot be accessed. Also, validity of surveillance data as a piece of digital evidence is assured because data are tamper-proof.



SOURCE: Modified from “Unbendable” project led by Trevoc Ltd.

FIGURE 15 System for transparent surveillance

Applying the system, LEAs can use publicly accepted authentication and cryptography functions in order to authorize and control the equipment and the data they produce. The technology and the procedure used consist of several parts. The most significant improvement compared to the current situation is that the new system is centralized, the parts are only working together and ad-hoc usage is not allowed. The process parts are:

- Court (instance of permissions),
- LEA (instance of cases and operations),
- Legal audit (monitoring, auditing and inspections of coercive means),
- Target (surveillance operation target).

The most intrusive parts used in surveillance operations are the surveillance equipment and the data they produce. At the moment, no authenticated permission token is needed. If a token is not required, this simply means that the usage cannot be monitored. There is not even proof of correct usage of the equipment. A similar kind of a problem exists with the data produced by the processes. With the current systems, it cannot be determined when, where and by whom the data were produced. Also, it cannot be said whether the collected data are the same kind of data that were authorized to be collected. When coercive methods are used, the authority should be asked if the equipment is able to work without a token, if there is someone who knows about the operation and can be identified, if the equipment can be used without authorization, if the amount of data can be identified, and if the equipment used has been under control the entire time.

A Proof of Concept (PoC) implementation includes a chain of trust between the process parties. Therefore, it is possible to create a transparent and secure surveillance operation base. Systems transparency is based on technology. All legal processes are firmly supported. Surveillance material can be obtained only with the technology authenticated for operation. Regarding supervision, all data from the source are sent in an encrypted form to a trusted third party, which is a trustee of the public. This trusted third party sees real data only when the LEA's representative is present with the decryption key. This way, the information remains secret and cannot be abused.

3.2.3 Discussion of Study II

The ideal situation would be to achieve a balance between surveillance and privacy. How is this balance going to be reached? The answer is to understand the threats to privacy, privacy enhancement mechanisms and the principles that make the balance possible. Surveillance should ensure that its exercise is fair, legitimate, proportionate, transparent and accountable (Hallinan, Friedewald & McCarthy 2012). Many countries want to improve law enforcement and general security. This leads to the fact that new surveillance technology as well as new legislation enabling its usage is needed. The citizens will be ready to give greater authority to LEAs if they believe that it increases their safety and security, and if they can trust that the authorities do not abuse the power granted to them. LEA officers have to understand that the systems must be linear and transparent so that the new legislation, which makes utilization of the new technology possible, will be enacted.

One important part of designing and developing a surveillance authorization process is by creating an open acceptance process for the technology. Both security and transparency are important in surveillance operations and must be at a sufficient level. LEAs work for citizens and the society. Citizens need high quality LE services in the ever-changing environment. Protection of citizens from more organized and internationalized crime requires new tools. Citizens should make the final decision regarding the balance between privacy and security.

3.3 LEAs’ legal digital evidence gathering

Study III concentrates on chain-of-custody requirements. Today, LEAs must perform many stages twice with the help of different technical tools. When investigating the identity of criminals, LEAs may apply technical tools that are totally different from those used when gathering evidence for a charge because the data provided by their investigations may not be valid in court. The research question of Study III is: How can investigation data also be used as digital evidence in the Courts of Justice? The included conference paper can be referenced as follows:

> Jyri Rajamaki & Juha Knuuttila. Law Enforcement Authorities' Legal Digital Evidence Gathering: Legal, Integrity and Chain-of-Custody Requirement. *The European Intelligence and Security Informatics Conference (EISIC)*, 2013, 198-203.

The evolution of societies has been rapid since the Industrial Revolution, and major changes are occurring one after another at an accelerating pace. Recently, telecommunication and computing technologies have converged under ICT and are jointly creating a platform for digital services. The Internet economy and digital services will be everywhere, from private houses to industrial plants (Paajanen et al. 2013). However, the public sector is somewhat late in competence building, including legal competences, and is currently only beginning to taste the surging opportunities to improve its operational procedures.

Increasing crime forces the police to find more accurate evidence. When carrying out criminal investigations, LEAs are able to obtain evidence in very effective ways that were impossible a few years ago. One remarkable aspect is that LE investigations increasingly generate a very large amount (terabytes) of data (European Commission 2012). Moreover, legislation on criminal procedures in most countries was enacted before these technologies appeared, thus having taken no account of them. The European Commission notes that, as a result, three very important problems appear:

> (1) The admission in Court of evidence obtained this way is frequently uncertain, giving judges no clear criteria on its admission and assessment, and therefore causing uneven application of the law.
>
> (2) These new technologies can loose their efficiency quickly, as soon as criminal organizations become aware of their existence, obtain technical details about them and adopt countermeasures. The absence of standards and regulations protecting them from having to be publicly exposed during trials, burn them out as soon as they are used. This is particularly valid for criminal transnational organizations, usually having almost unlimited resources.
>
> (3) Globalization of criminality requires the tight collaboration of the law enforcement and judiciary systems of different countries: evidence obtained in a State has to be shared and accepted in other States, while simultaneously observing fundamental

> rights and substantial or procedural safeguards. The lack of legislation and standards at the national and international level obviously makes this particularly difficult.[21]

To address the above-mentioned problems, we require a monitoring system that will go beyond state-of-the-art, thoroughly taking into consideration the organizational and procedural interoperability. There are three organizational layers that need attention:

- LEA: the people that actually retrieve and store the information.
- Prosecutors and their offices: the way they get access to the information.
- Courts: the final destination of the retrieved information.

Until now, the information gathering tools of LEAs have been engineered focusing only on the best way to retrieve the information from the target. The attention paid to the legal, integrity and chain-of-custody requirements as well as social acceptance and legal oversight in connection with retrieving information has been inadequate and guidance on these matters has existed only in manuals written by legal departments.

The banking sector is one of the most regulated sectors. However, in Europe it is completely digitized and compatible with the Single Euro Payment Area (SEPA). The existing systems could be used for a wide variety of event management issues or for something else where various accounts are involved: inbuilt security is certainly a very valid asset in almost any service category (Paajanen et al. 2013). In the banking sector, the security requirements of digital services are very high. For this reason, it is a good area for benchmarking most forensic evidence moving from the physical to the digital realm.

LEAs have developed a new informal forum to team up quickly with the best possible experts to counter-attack economic cyber-crime, an area where legislation is far from comprehensive.

3.3.1 Requirements for the monitoring system

LEAs' monitoring systems should have a central control station that collects and stores all the information according to the rules and that also provides legality control. The real-time information should be sent on demand to the end-user wherever he or she is. In many cases, the users of information are not in the office but in the field, using portable devices. This is called front-deployed knowledge.

Safety, encryption and availability of the data are very important. Information must be understandable and collected in a trusted way. Data need to be available in spite of location, but one needs to be aware of the law when han-

[21] European Commission C (2012)4536 of 09 July 2012, "Work programme 2013, Cooperation, Theme10, Security." Available: ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k-wp-201301_en.pdf

dling data. Integrated multimedia sensor systems collect data and must become more miniaturized, sustainable and operable with low power.

Data must be reliable and must include position marks and time stamps indicating where, when and by whom the data were produced. Multimedia files must contain all the information but should be compressed to as small a space as possible. Video and sound data always include information about when and where that data were generated. All this information must be put together into a single file so that there won’t be any need to search for parts of information from various systems.

The gathering, conservation, communication and presentation of computer-derived evidence must fulfill legal requirements with respect to the admissibility of the evidence, which should be admissible, authentic, complete, reliable and believable. Electronic evidence not gathered in accordance with the law will be inadmissible and ruled out of court. Today’s main evidence authentication system is the hash value calculated from the retrieved information. With the hash value, you can prove that the data are original and no one has tampered with them. The problem is that systems like hashing are incapable to show when, where and by whom data were produced.

Life-cycle of the data are also important and have to be included when designing systems. This has led to a situation where commercial systems are preferred in the field.

With regard to tracking devices, many problems may occur. Better quality devices need to be big, and for that reason power consumption becomes too high. Bigger size also makes tracking devices more easily exposed. Smaller devices with lower power usage mean lower quality. But lower quality is out of the question. At the moment, there are no devices that can support cross-over platforms for positioning and communications. It is easy to interrupt tracking devices because they don´t have built-in alarm features. The tracking devices’ own time is not trustworthy because it can be easily modified. Position and time obtained from a satellite make it more reliable.

3.3.2 Possibilities of new digital services for crime prevention

To bring into use the LEAs’ special requirements for digital evidence, technological and socio-technical research and development research is needed. The development of novel monitoring systems and new sensors improves LEAs’ evidence-gathering abilities while respecting the legal and ethical expectations of society. The overall development target will be accomplished through the following specific objectives:

- to enable new operational investigation models for LEAs by improving existing technology and developing new integrated digital services for tracking and audio and video retrieving and monitoring.

- to develop methods of working that are legally binding and socially acceptable; information gathered is legally binding and court-proof technology developed will enable an audit trail, accountability and further societal acceptance.

- to support wider European goals, such as recognizing the needs for regulation and harmonization and promoting the use of other European technologies like Galileo, and to create the needed interfaces.

Despite all the challenges, bank documents bring huge value by providing the proof of who of which company paid or received money. The evidence consists of forged signatures or endorsements and fake company names or people. Investigating this kind of evidence may lead to other clues that may help unravel complexities (Coenen 2009). Economic crime investigation has always relied on known scenarios of economic crime. For example, when a gang of cybercriminals stole $45 million by hacking into a database of prepaid debit cards and draining cash machines around the world, law enforcement agencies in Japan, Canada, the UK, Romania and 12 other countries were involved in the investigation (BBC News 2013). Economic crime still follows it roots, using methods known for ages. By using the technology created for bank transactions, it is possible to get deeper into the details of crime. Investigating bank transactions can be challenging, but it provides very useful and reliable financial documents in fraud investigations. With modern technology, it is possible to obtain reliable and accurate digital evidence for economic forensics.

3.3.3 Legislative and political view

The focus of Study III is on the latest technological developments in crime investigations, which are framed by societies' laws and practices. On the legislative and political level, several nations are taking steps to enhance LEAs' possibilities and readiness to tackle "not so entirely new" ways and means of transnational crime, which are put into historical perspective by Political Science Professor (Andreas 2013) :

> The particular smuggling activities and policing priorities will surely shift over time, as they always have, but it is safe to predict that the centuries-old illicit trading tradition will survive [15]. This is now fueled by the United States´ addictions to cheap immigrant labor and mind-altering substances. The United States will make little progress if policymakers continue to see these problems as primarily rooted in transnational crime, rather than in outmoded labor-market regulation, a dysfunctional immigration system, an overly punitive drug-control system, and failures in education and public health policy.

International warehouses of crime route their activities into the most lucrative avenues. Nation states are responding with a slower pace: Wassenaar-[22] and Prum[23]-type and bilateral agreements are made in a relatively ad hoc manner outside international bureaucracies to give more international leeway to LEAs. This has and will be facilitated by the newest technical principals and applied research. Therefore, researchers should approach LEAs in order to address real

---

22 Wassenaar Arrangements, Available: http://www.wassenaar.org/

23 "The Treaty of Prüm: A Replay of Schengen?" Available: http://www.eu-consent.net/library/deliverables/D38c.pdf

problems while drafting their research agendas and approach politicians when disseminating their results.

3.3.4 Discussion of Study III

To form the basis for the technological development concentrating on the development of new sensors, monitoring stations and their communication channels for LEAs, this study will contribute towards the operational environment and different phases of chains-of-custody applied in various countries. This will be done by adding a legal / societal layer to technological development and by developing mechanisms and recommendations that will enable safeguarding the accountability, legality and social acceptance of the developed technologies. In this regard, two research tracks should be developed: (1) procedural safeguards and (2) data protection safeguards from "privacy-by-design" to "accountability-by-design." Procedural safeguards will ensure the transparency (for purposes of accountability of law enforcement officers) of investigation techniques used. Specific attention should be paid to privacy safeguards. In data protection safeguards, specific relevance should be given to the introduction of accountability mechanisms into the design of the system.

The monitoring system should enable a use process where the fulfillment of legal oversight requirements is possible in all phases. In practice, this means that we are no longer building just the equipment that someone is using and the output of which is used in part in courts. Instead, we are creating a total solution that creates an auditable log for every phase of the process. The tools will not start operating when a battery is installed in them; instead, they are always connected to the authority's central system that will give them the permission to operate. The authority giving the operation permission has to connect to the system always via authentication, which creates a log mark on who gave the permission in the system. As long as sensors are capable of operating without an authenticated permission token, there is no means for controlling their use. The new kind of a monitoring system will be able to present publicly accepted auditable log-based proof of correct use of the equipment. This will be done with publicly proven technical control methods involved in the command chain. It does not only provide tools for LEA use, but also provides important building blocks for the creation of a more open society with built-in oversight and legal audit systems (Rajamäki et al. 2012).

Submitting electronic evidence before a Criminal Court as evidence means it should have all attributes of conventional evidence: It must be admissible (i.e., it must conform to legal rules to be put before a court); it must be authentic (i.e., it should be possible to positively tie evidentiary material to the incident); it must be complete (as much as possible); it must be reliable (i.e., there must be nothing about how the evidence was collected and subsequently handled that would casts doubts on its authenticity and veracity) and it must be believable (i.e., understandable by a court) (Leroux 2004).

The information created for LEAs by the sensor is always multi-sensor information—that is, the video or sound must always include the data on its production time and place, which can be checked based on the geometry of the positioning satellites. A mere time stamp based on the tool's own clock is not reliable as it can be changed. Furthermore, the system always calculates the hash value from stored data that safeguards the unchanged character of the original data. All log information can be sent in an encrypted form to LEAs or even to courts of justice, to whom the LEA can provide the encryption key for oversight purposes. All information created by the system will be encrypted, as inserting unencrypted information into public networks endangers the subject's privacy in a way not allowed by law for LEAs.

3.4 The reference architecture and stakeholders' needs

Study IV is part of the exploratory research stage of systems engineering to search for new ideas or enabling technologies and capabilities, which then will mature to initiate new systems-of-interest. This action is aimed at substantially improving existing technologies and developing new ones and their direct and practical application to the day-to-day needs that LEAs are not able to address efficiently with currently available commercial products. Study IV designs the reference architecture for the tracking of non-cooperative targets. It also examines the needs of stakeholders for the new types of GNSS-sensors, a monitoring station and their associated communication channels in the field, taking into account societal acceptance of the proposed solutions. The research question of Study IV is: How can the beyond of the state-of-the-art (SOTA) reference architecture for a new LE tracking system be designed, and how can its main stakeholders and their needs be understood and categorized? The included article can be referenced as follows:

> Jyri Rajamäki. Satellite based tracking systems for better law enforcement: a systems engineering exploratory research via a multiple case study analysis. *WSEAS Transactions on Systems and Control.* [In review]

The main idea for the transparent surveillance system was presented in Study II, and Study III concentrates on how investigation data could also be used as digital evidence in the Courts of Justice. Figure 16 shows the main logic behind the reference architecture: the integration of technical surveillance and the monitoring-of-legality to the same system. The next paragraphs deal with the main components of the system: GNSS sensors, the future monitoring system (FMS) and data flow and communication channels. The FMS is also valid for forensic technologies other than GNSS.

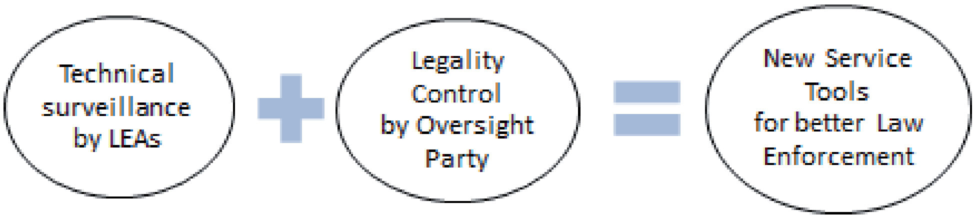


FIGURE 16 Idea behind the reference architecture

3.4.1 Reference architecture

3.4.1.1 GNSS sensors

A new tracking sensor system, which has multi-GNSS capability (Galileo, GPS, CLONASS) should be developed. If accuracy is also needed in the Arctic area, then Iridium support is desirable. Because the battery is the biggest part of these sensors, miniaturizing will mainly be achieved by optimizing the sensors' power consumption and by utilizing energy harvesting and new high-power rechargeable battery technologies. For easy concealment, recharging will be wireless.

Applying a machine learning type of artificial intelligence, the sensor can adjust according to the behavior of the target. A multi-talented, intelligent and smart device can monitor the environment, such as light conditions, temperature, vibration, GNSS location and cell location. This information helps to visualize what is happening at the location. The device's own AI-brain makes the necessary decisions, generates alerts and facilitates obtaining help in tough situations. By optimizing the use of radio transmitters, sensors could increase their power efficiency significantly.

To address legal, policy and social acceptance issues, the sensor would need an authentication authorization token to run. Encryption should be completed in the first possible phase, so that no plain information were stored in the system. Self-protection and countermeasure protection, as well as jamming detection, should be included.

3.4.1.2 Future Monitoring System (FMS)

The future monitoring system (FMS) should be a system with improved performance of importance and priorities. The FMS will be more than a storage and display system. By this, we do not mean simple systems like geo-fencing (virtual perimeter for a real-world geographic area) that already exist. The FMS could combine various forms of information: for example, temporal, spatial, audio, and visual. However, combining information from many sources is a technically, operationally and legally difficult task.

Looking after the tracking information is seldom the main control room staffs' duty, but is rather the work of a small team of investigators. Keeping someone looking after the information on a 24/7 basis creates labor costs that are too high. The FMS, cooperating with the tracking sensor, should be able to keep an eye on the target's behavior and learn from it. After the learning period, the FMS can tell when events are presumably related to crime and when not. This can be achieved by combining all the information obtained: such as the target's daily routines, different routes, and changes in driving behavior (e.g., known patterns such as many U-turns taken to find tailing LEAs). The FMS should be able to provide the necessary information without human involvement and alert the case officer, who might be busy with another case: "Look at me now, something important and interesting is happening!" The FMS will enable front-deployed knowledge. The information will be sent to the case officers wherever they are in real time and in a secure way.

All this requires close cooperation between back-end monitoring, the case officer's communication channels and the sensors. The key issue is to produce only the piece of information required to get the job executed: this information and nothing more. The FMS will know in real time when the case officer is looking at the track and will also be able to tell the sensor if no one is attending. In this case, information is not sent in real time; it is just stored and forwarded in one package, for example, in the next morning or when asked. This will save a lot of the battery power. However, if something out of the ordinary happens, the sensor's AI-brain will override this and send an alert through the FMS to the case officer's mobile phone.

The FMS should provide sensor management via the Provisioning Server (PS). The PS will allow centralized management and control of the full fleet of devices allowing authentication and authorization for legal and technical personnel, as well as an audit trail and log for oversight. The FMS and PS will (1) authorize investigation tools and tracking devices to operate, (2) define legal and technical limits for surveillance nodes, (3) define the role-based operation green light, (4) enable legal monitoring and (5) unify authorization and legal inspection functions over the wide range of sensors used in surveillance.

The FMS should contain support for front-deployed knowledge—a safe way to forward data securely to the terminals of LEAs in the field. There can also be new oversight of the LEAs using these intrusive information techniques without making them less effective. The FMS should be designed with oversight in mind, and people from the law-making community should participate in the design of the FMS. This will be the first built-in oversight and legal audit system for law enforcement. The FMS will provide a lot of new opportunities to lawmakers to better control LEAs without making LE operations less effective. For example, the warrant area or time limits can be fed into the FMS. The FMS can autonomously force the sensor to stop its operations when the limits are met. It can also make an auditable log from the operations for legal oversight. LEAs need advanced surveillance technologies to fight professional crime, and with the FMS, LEAs can have real proof that they are exercising given powers according to legislation and public benefit, thus improving societal acceptance of the proposed solutions.

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

It is impossible to achieve the result we are looking for by studying only one part of the system at a time. We must look at all system parts at the same time; otherwise, we end up with a system of systems without any optimal solution. However, we must keep in mind that no LE organization can afford to buy a completely new system all at once. Being down-gradable, the FMS should be able to communicate with and accept data from old equipment.

As Study III states, there are three organizational layers that need attention: (1) LEAs, (2) prosecutors and their offices and (3) courts of justice. All these organizations have slightly different procedures and organizations in different countries. The FMS should take into careful consideration the organizational and procedural interoperability and offer a new, flexible backbone concept for secure intelligence gathering, collection, exploitation and sharing. It should include strong encryption and access control by encryption key management. This structure facilitates logical communication as it can be used as the basis for access control and information flow policies. Information encryption guarantees that messages arrive at the right users only.

3.4.1.3 Data flow and communication channels

The conceptual model of LEAs' information gathering management consists of actors, information exchanging models and information flows between actors and actors' information systems. The secure communications concept identifies all the hardware and software components that are needed to protect it against cyber-crime or other attacks. The standardized development of access technologies, interfaces and protocols should be applied for (1) the radio channel (or other type of communication channel) gathering information from tracking sensors and (2) the wireless remote control of the tracking sensors.

Administrative and technical communication solutions improve both internal and multi-organizational LEA operations. The focus should be divided up into communications between (1) back-up systems and end-users in the field, (2) sensor nodes and monitoring stations, (3) monitoring stations and data storage and (4) organizations.

End-to-end encryption from the sensor to the FMS and/or data storage equipment with strong authentication mechanisms ensures that the information is available only to LEA and that no one can find it among other commercial traffic. Regarding oversight, all the data from the sensors could be stored in encrypted form to a trusted third party (ombudsman, etc.), a trustee of the public. The data storage system (repository system that collates sensor data) would include the needed communication and token handling protocols. A front-deployed knowledge scenario is also needed. It shows how the retrieved information can be delivered from the sensor through a centralized system to the end-user in the field in real time. The information flow from other older sensors enables the feeding of information from old equipment to the FMS.

3.4.2 Stakeholder needs

In SE, stakeholders of a system may vary throughout the life cycle of the SoI. The Stakeholder Needs and Requirements action works with stakeholders across the whole life cycle to elicit and capture a set of needs, expectations, goals or objectives for a desired solution to a problem or an opportunity. This action is used to produce a clear, concise and verifiable set of stakeholder requirements. According to Pyster and Olwell (2013), stakeholder needs and requirements identify and define the needs and requirements of the stakeholders in a manner that allows the characterization of the solution alternatives.

3.4.2.1 Citizens

Citizens need high quality law enforcement services in the ever-changing environment. The protection of citizens from more organized and internationalized crime requires new tools. As the main taxpayers, citizens are the sponsors of LE. Their main requirement is Value for Money (VfM), meaning efficient LE. In recent years, the productivity growth in the public sector has been much slower than in the private sector. Today, most European countries are faced with rising health service costs and have to meet the needs of their increasingly aged population. As for all public services, there is a huge need for making LE more efficient.

A public concern has arisen about the growing trend of the use of personal data accumulated by both private companies and authorities. People may feel that they are threatened by the transition towards a ubiquitous information society in which individuals can be located and identified, and accurate information about their actions, communication and location can be collected without them even knowing. Accepting commercial and technical solutions and their influence on fundamental rights and information security without criticism may be fatal. Warning signs appeared as early as the 70s. In the NordData 1975 conference, it was suggested that if citizens remain uncritical, there may be a drift into a situation of no choice and no freedom. Orwellian views of societal development may be accepted, or one can reject them as overly paranoid (Sprague 2008). As Study II states, from the citizens' point of view, the ideal situation would be to achieve a balance between surveillance and privacy.

3.4.2.2 Targets

Only criminals and/or criminal activities should be the target of surveillance. Applying artificial intelligence, the tracking sensors are able to adjust according to the behavior of the target. For example, AI can conclude from the behavior whether the target is driving the car or whether it is driven by his/her mother alone going shopping. One target for the tracking sensor development is to learn the driving habits of multiple drivers, such as the way they take corners, accelerate or change gears. With a built-in accelerometer and AI, the system should learn to track only the suspect, not just any driver.

3.4.2.3 Authorities

Of the authorities, the main stakeholders of the SoI are LEAs, prosecutors and their offices, the courts of justice and legal officers on legality control. Due to the economic situation in Europe, authorities' resources are meager. For this reason, most authorities' main need is to maintain their core services with reduced budgets. The only realizable solution in view is better piggybacking of ICT. This means that in surveillance as well as covert operations, ICT applications and services play an increasingly important role.

Because the activities of organized crime networks are thought to be more complex, diverse and international in scope than ever before (European Commission 2013a), LEAs need better tools and processes for cross-border operations and cooperation. Current tracking and monitoring systems are lacking in performance and old equipment is too big in size, hard to disguise and energy consuming. A new alternative to GPS is required; the implementation of Galileo will create new interdependence possibilities and advantages for tracking. As stated in studies I and II, LE officers need to have easier access to all investigation data, independent of place and time. This means that the FMS should also include mobile solutions. Most devices produced for LE take account LEAs' needs. However, commercial interests are sometimes a stronger incentive than LEAs' requirements. This situation means that the best solutions are not always for sale, and the manufacturers sell out of the first-generation products before bringing in the next generation. Subsequently, LEAs end up with having several inefficient systems lacking integration. This requires a lot of support and logistics. The open IT solutions launched on the markets should be adaptable with new (experimental) sensors. Counter measures by criminals are posing new challenges as criminals use advanced detection and signal-jamming technologies. Because of this, the technologies used by LEAs have to be concealed in better ways, such as in regards to size and appearance and having jamming detection capabilities. Safety, encryption and access control are very important tasks for LEAs. Investigation data have to be protected so well that unpermitted access is impossible and the content will not be revealed. Encryption safeguards privacy; tampering will be recognized, and encrypted files will guarantee a strong chain-of-custody.

Submitting electronic evidence before a criminal court as evidence means it should have all attributes of conventional evidence—that is, it must be admissible, authentic, reliable, complete and believable. The information collected by the system should be applied as a piece of evidence. Special focus should be placed on the issues raised by the disparities among the rules on the admissibility of evidence between Member States, as stressed by the EC Green paper on criminal evidence (European Commission 2009). Recommendations should be formulated to design a system that would be compliant with all EO member states.

Operational models of LEAs' information gathering do not comply with the legal and societal requirements and expectations at the needed level nor with the possibilities modern technology would allow. Harmonizing by implementing legal requirements into a new system that would be useful for all LEAs in Europe is the first step. When making use of covert investigation tools, not only should the system designed be respectful of fundamental rights and its use compliant with the applicable legal framework, but oversight mechanisms should also be put in place in order to ensure the transparency of the measures installed. Strong transparency mechanisms are particularly required to frame surveillance systems that are necessarily opaque to the individuals monitored and to counterweight the increase of power given to LEAs. Accountability of LEAs becomes pivotal in ensuring a balance between security and privacy and to create trust. The concept of "accountability-by-design" from a technical and legal perspective proposes innovative solutions to tackle this problem. The objective for the system is to always ensure accountability and to guide users to legitimate procedures. The requirement is to have an audit trail system instead of users writing logs themselves.

3.4.2.4 Manufacturers and service providers

Within the category of manufacturers and service providers, the main stakeholders of the SoI are GNSS operators, telecommunication operators, information system providers and GNSS sensor manufacturers. Most of these actors are private companies whose prime interest is to win growing business. Public operators' main interest is to get more users, and at this rate, financial continuity to their services. From the technology and service providers' point of view, the market of law enforcement for ICT products is too highly fragmented. All law enforcement organizations have their own specifications that, on top of everything else, differ from country to country. Development of a new ICT concept incurs significant expenses, thus making access to the international market desirable. Standardization work is needed because it will facilitate the entry of especially small and medium enterprises (SMEs) to the market.

3.4.2.5 Policy makers, legislators and funding agencies

Policy recommendations for public authorities dealing with regulatory aspects of the use of covert investigation tools by LEAs should be formulated. More research is needed for identifying the legal barriers to the EU-wide deployment of the SoI-like prototypes and shortcomings in the current legal framework. The expected outcome of the research is to issue legal recommendations in order to remedy these shortcomings, fostering the deployment of covert investigation tools that take into account individuals' fundamental rights and concerns as well as ensure a great level of transparency. Recommendations as regards standards for the collection of admissible pieces of evidence should be formulated based on the analysis of a selected number of national legal frameworks.

The funding agencies' main requirement is an efficient return on investment (ROI) ratio. Calculating the current net value of the project's life-cycle cost (LCC) can be difficult. It requires taking into account all the costs of designing, building and facility management (operating, maintenance, support and replacement) (El-Haram, Marenjak & Horner 2002). The LCC must also consider the costs associated with the transition of the project from the private sector to the public sector at its conclusion.

The national institutes of standards and technology have computer software for calculating LCCs if the costs of a project can be grouped into the following categories (Fuller & Petersen 1996): (1) initial investment costs, (2) operation and maintenance costs, (3) energy costs and water costs, (4) capital replacement costs, (5) residual values and (6) financing costs.

A public-private partnership (PPP) is an increasingly used method to deliver infrastructure assets in the education, transport, health, defense and security sectors. It allows the public sector to harness the expertise and efficiencies that the private sector can bring to the delivery of certain facilities and services traditionally procured and delivered by the public sector (Carty 2006).

3.4.3 Discussion of Study IV

This section evaluates the research process and the findings of Study IV from the viewpoint of the research questions of Study IV. Study IV belongs to the Exploratory Research Stage of systems engineering. Study IV summarizes the main stakeholder needs of new types of GNSS-sensors, (mobile) monitoring stations and their associated communication channels for LEA operation in the field, taking into account the chain-of-custody requirements and societal acceptance of these solutions. The next SE stage, the Concept Stage, is a refinement and broadening of the studies, experiments, and engineering models pursued during the Exploratory Research Stage (Haskins et al. 2011). Concept definition is the set of SE activities in which the problem space and the needs of stakeholders are closely examined. The activities are grouped and described as generic processes that are performed concurrently and/or iteratively, depending on the selected life-cycle model (Pyster & Olwell 2013). In order to bring out the LEAs' requirements for tracking non-cooperative targets, technological and socio-technical research and development work is still needed. This research should go beyond the SE principles because, for example, cultural effects are prominent, and new methodologies such as the critical research bricolage (Kincheloe, McLaren & Steinberg 2011) should be applied.

Development of FMS and miniaturized GNSS-based tracking sensors improves LEAs' evidence-gathering abilities while respecting the legal and ethical expectations of society. The overall development target should be accomplished through the following specific objectives: The first target is to enable new operational models for LEAs' investigations by improving existing technology and by developing new integrated digital systems for tracking, retrieving and monitoring. In addition, the next level in digital miniaturization and state-of-the-art development should be reached, including (a) easy usability—equipment can be handled under difficult conditions; (b) long life-span—extended to several months or even over a year; (c) (self-) protection—applying artificial intelligence, the sensor is capable of monitoring its surroundings and can change its operation model autonomously for its own safety and (d) securing data through deep encrypting. The second development target should be to develop methods of working that are legally binding and socially acceptable; information gathered is legally binding, and technology developed for court evidence will enable audit trails, accountability and further societal acceptance. The third target would be to support broader European goals in recognizing the needs for regulation and harmonization, promoting the use of other European technologies and systems such as Galileo and EUROSUR and creating the interfaces required.

3.5 Cyber-secure communications

As stated in Study IV, the conceptual model of LEAs' information gathering management consists of actors, information exchanging models and information flows between actors and actors' information systems. The communication systems LEAs use are a part of the cyber-secure governmental communications concept applied by different public organizations. The research question of Study V is: How can global cyber-secure communication channels be created for LEAs and their sensors, taking into account interoperability with existing systems and economic issues? The included conference paper can be referenced as follows:

> Jyri Rajamaki, Paresh Rathod & John Holmström. Decentralized Fully Redundant Cyber Secure Governmental Communications Concept. The European Intelligence and Security Informatics Conference (EISIC), 2013, 176-181.

The European Defence Agency (EDA) was established to enhance European defense capability, especially in the fields of crisis management to help European Union (EU) nations and the council. The broad goals of the EDA are to sustain the European Security and Defence Policy in the present state and develop it to keep it up to date. EDA must ensure coordination and synergy with the member states and European investment to enhance and update capabilities in civilian security (Lapierre 2011). It is a common practice in EU nations to use military and civilian defense actors during crisis management and operations. The partnership ensures the safety and security of EU residents and citizens. Researchers have often observed an overlap of military and civilian functions, especially in the areas of communication, information gathering and command and control operations. Increasingly, the research, development and innovation in technology are based on 'dual-use' requirements provided by both civilian and military actors (Lapierre 2011).

Critical infrastructure protection (CIP) is the analogous shared concern and responsibility of the society. Water, power, finance, Internet, transport and all communication systems are part of the critical infrastructure (CI) and are essential to daily activities. Private industry owns and operates most of the CI assets, and the government serves as a regulator and consumer but often has a limited role. The various CI components are, to varying extent, dependent upon one another within a country's borders and internationally. As such, problems in one CI component can quickly spread to others (George 2008). The operation of most CIs rests partly on their own dedicated communication systems as well as simultaneously on commercial networks.

In recent years, the capabilities of PPDR organizations across Europe have significantly improved with the deployment of new technologies, including dedicated TETRA networks. Nevertheless, events like the London bombing in 2005, the Schiphol airport disaster in 2009 and the flooding disasters in 2010–11 have highlighted a number of challenges that PPDR organizations face in their day-to-day work. Secure and reliable wireless communication between first responders and their emergency control centers is vital for successful handling of every emergency situation. This also applies to each connected respondent and includes police, fire, medical or civil protection (Goldstein 2012).

PPDR, CIP and MIL organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe but also collective responses to threats and crisis must be enabled in an increasingly interconnected network. In addition, the organizations stand to gain from the interoperability functionality in their routine work. On one hand, Europe is a patchwork of languages, laws and diverse cultures and habits that can change abruptly across borders. On the other hand, even in the same country, each security and CIP organization develops its own operational procedures. For efficient operations, many serious challenges need to be addressed, including critical governmental communication systems (which are not compatible even when they use the same technology) and differing procedures as well as inadequate language skills in cross-border cooperation. Study V addresses not only the technical challenges of security and interoperability but also the strategy to build a redundant critical governmental communication system for a multi-organizational environment, enabling external users to collaborate in keeping the intrinsic and vital cyber security mechanisms of such networks. Study V presents a solution based on the Distributed Systems intercommunication Protocol (DSiP).

3.5.1 Distributed Systems intercommunication Protocol—DSiP

DSiP forms multiple simultaneous communication channels between the remote end and the control room: if one communication channel is down, other channels will continue operating. DSiP makes communication reliable and unbreakable by using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF-radios and other technologies can be used simultaneously.

DSiP manages the selection of communication channels and overcomes link establishment issues. DSiP solves incompatibility issues and is an invisible layer to end-users' applications, hardware and software. It provides modularity, data integrity, security, and versatility to data communications systems of any size. The DSiP software uses both IP and non-IP based communication links when required. DSiP is capable of converting classical polled systems into an event-driven function. This feature improves response time and speed. DSiP also compresses data, which, according to Riippa (2011), is useful with low-capacity communication channels.

Virtual Private Networks (VPN) can be tunneled through the DSiP communication system. This feature makes it possible to maintain constant communication without re-authentication even though one communication channel is at fault. The DSiP telemetry system brings many significant benefits and useful functions. The DSiP system (1) increases reliability and security; (2) is resistant to network Denial of Service (DoS) attacks; (3) decreases the risk for viruses and malware; (4) results in less system downtime and lower maintenance requirements; (5) contains authenticated and encrypted communication; (6) allows connections to TETRA and mobile handsets; (7) has the capability of interfacing with many different kinds of hardware and software like radar, Automatic Identification System (AIS), Radio Direction Finders, and Closed-circuit television (CCTV) equipment; (8) is a transparent communication of Distributed Network Protocol (DNP) 3, IEC101/104, Modbus, National Marine Electronics Association (NMEA) and other protocols and (9) includes network monitoring and management tools improving overall system performance.

Mobile multichannel communication improves communication reliability and quality, for example in PPDR applications. Police cars, ambulances and fire engines benefit from uninterruptable secure communication. DSiP provides a uniform, reliable and maintainable communications services platform capable of withstanding time. The system is not dependent on any particular telecom operator's services or communications protocols. There are layers of components including Remote Terminal Units (RTU); secure network routers and switches and communication frameworks like TETRA, satellite, LTE and others that connect with command and control centers using the DSiP front-end hub. The secure routers and switches carry advanced hardware and software firewalls to ensure a high degree of security. The sensors allow a communication channel to connect with RTUs. Secure routers and switches establish multiple parallel communication links to communication framework equipment where layered firewalls are implemented on a redundant DSiP front-end. This ensures secure communication connections with the command and control room.

DSiP is currently in pivotal use by the Finnish Frontier and Coast Guard in a coastal surveillance application, by Fingrid Oyj for controlling Finland's main power grid, and by Elenia Verkko Oy (former Vattenfall Verkko) for controlling and operating the mid-voltage power grid.

3.5.2 Quality of service and cyber-secure communications

IP traffic and its packets have methods for controlling priority and quality. The IP QoS is either not supported at all or is supported in non-conforming ways in operator traffic. Customers using DSiP have enhanced controlling possibilities for data flow and traffic, including (1) control priorities—important information is routed first, less important information later; (2) control over network timeouts—no undetermined delays or waits; (3) control of the usage of communication and bandwidth—DSiP always ”knows” the condition of all routes; (4) better control over maintenance and configuration; (5) the DSiP telemetry system with its built-in congestion control and (6) routing services based on cost-factors enabling certain, less important traffic to be filtered, such as the used low-capacity communication.

The decentralized architecture based on DSiP is highly fault-tolerant in normal conditions as well as in crises. 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. 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 (European Commission 2013b).

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, DSiP system provides a high level of reliability and security for applications demanding uninterruptable communication and extended usability.

3.5.3 Key elements and functionalities of DSiP

As mentioned earlier, DSiP is entirely a software protocol solution. There are fundamentally two types of software elements: DSiP-routers and DSiP-nodes. Figure 17 depicts the blueprint of the solution. The nodes constitute interface points (peers) with the DSiP routing solution, and the DSiP-routers drive traffic engineering and transport in the network. DSiP-routers establish multiple authenticated and encrypted, sometimes parallel, connections according to configuration parameters, between each other. The nodes establish multiple simultaneous connections to one or more routers in the system. All connections can be strongly encrypted based upon usage of certificates. This effectively means that all elements in the DSiP routing solution are known. As routers may use multiple parallel connections between each other and as nodes may make multiple parallel connections between themselves and one or more routers, the solution results in a true mesh-like structure between the network peers (nodes).

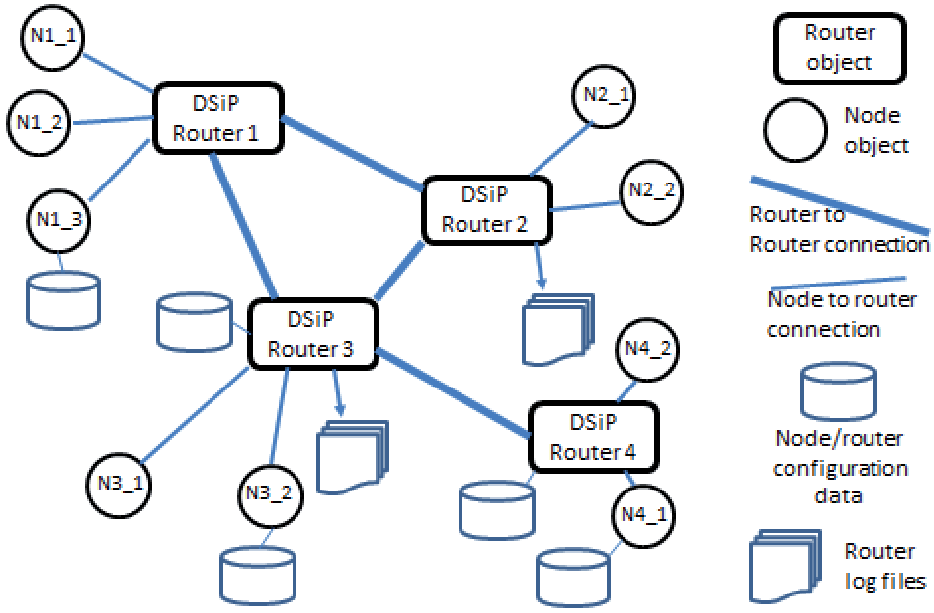


FIGURE 17 Blueprint of DSiP network solution

DSiP-routers in the routing network are typically distributed to different physical locations. The nodes are typically located at but not limited to, for example, emergency service vehicles and control rooms. The connection establishment is always constructed from the node towards the router element and one router to another router in a preconfigured manner. The system features a third element, called configuration server software, from where nodes may read new configuration data should the underlying physical transport layer request changes or configurations need to be done.

The nodes and routers maintain multiple parallel physical connections between each element in the DSiP routing solution. This removes the complex burden from the external equipment and software that use the system for routing. Consider, for example, a vehicle computer in an emergency service vehicle. This computer either contains a DSiP-node that uses multiple wireless modems, or it connects to a vehicle router-hardware containing a DSiP-node and multiple modems. The DSiP-node is performing the tunneling of the user applications' IP-traffic from the vehicle to the control room and vice versa, thus mitigating complex routing issues in-between network peers. The DSiP solution is capable of transparently maintaining the connections and communications between users' systems or applications or hardware without this functionality having been programmed into the applications—DSiP is thus fully transparent to its users. For example, a user may run VPN client software in his laptop. The nature of the VPN demands that it must establish its connections over a single physical communication line. If this line has a problem or breaks up, the user must re-authenticate his or her VPN session over another physical media. When DSiP is used, the user can use his or her VPN client or server to establish a VPN session over multiple physical connections—should one or more have problems, the VPN session remains intact as the DSiP tunnels the session through itself. This feature is of utmost importance in critical applications.

Another extremely essential aspect of critical networks is their sustainability and handling of Denial-of-Service (DoS) network attacks. As the communication in the DSiP routing solution is based on multiple connections over multiple physical media, it is not sensitive to DoS-attacks, there always being "some route" between the network peers. It is highly unlikely that an attacker would, or could, attack all the elements in a heterogeneous network simultaneously.

The transport layer in the DSiP routing solution may use IP networks. However, DSiP is not limited to the use of IP—it can use proprietary, non-IP networks as well. This feature adds to the security and robustness of a DSiP routing solution. The DSiP can interconnect peers in an IP network by using non-IP connections. In addition to the aforementioned, DSiP is a tunneling protocol. It can interconnect so-called 10-based IP networks over a regular teleoperator service provider's IP networks, although 10-networks are not routable regularly.

The DSiP-network and solution contain decentralized authentication server software (no credentials are stored at the routers), mitigating the complex task of providing access to peers. In addition to this, the DSiP-network management server software provides reports and material over DSiP-node accesses, transported number of bytes and detected link latencies, which all contain useful information for the system maintenance team. A DSiP-node can be constructed in native programming languages (e.g., C, C++) and Java. The latter typically provides an easy path for creating DSiP-based applications in, for example, mobile handsets.

All addressing in DSiP is based upon individual node-organization and routing-cloud-numbers. The ending points in DSiP routing solutions do not need to "know" the IP addresses or locations of their counterparts. The addressing scheme, in addition to a concept called DSiP-translation barrier, makes it possible to interconnect users from different organizations with different IT-policy statuses because the DSiP may constitute a service-providing network and not just a "pipe" or "tunnel" from one network to another. The translation barrier functionality residing in the DSiP-nodes may be used for fetching data from core networks and filtering access to the core in much the same way as HTML and PHP are used in browsing applications. A typical multi-user, multi-policy DSiP routing solution may look like the one in Figure 18.

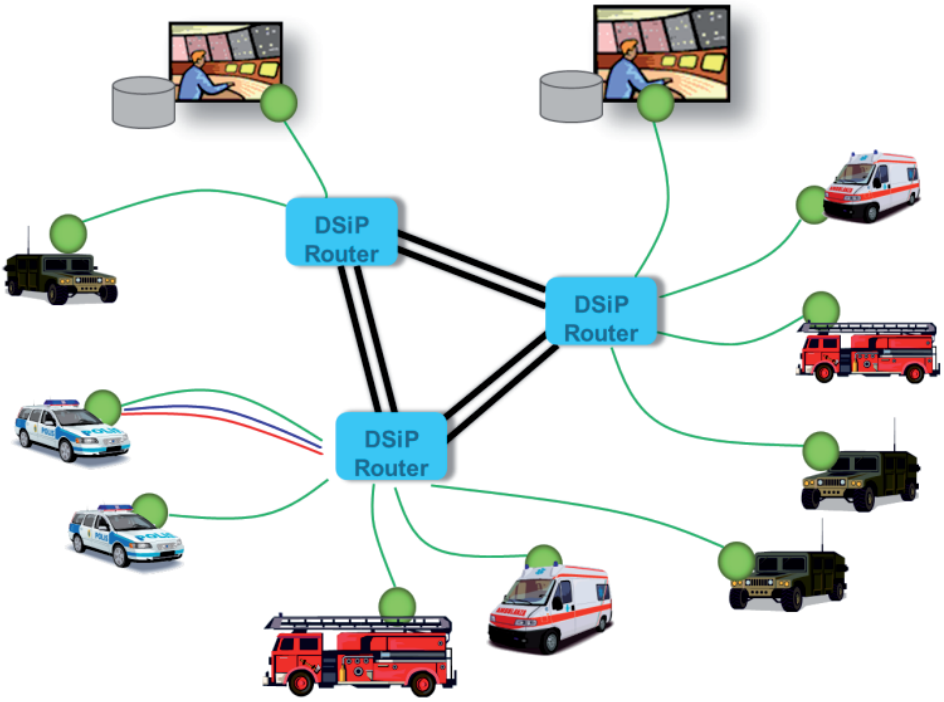


FIGURE 18 Multi-user DSiP network solution

Maintaining an IP network is a tedious and often difficult task requiring a thorough understanding of IP-firewalls, switches and routers. It can be highly risky to parameterize a firewall, as a faulty firewall rule may endanger a complete network. The DSiP solution mitigates this task. The IP network maintainer or creator may set up his or her network and tune firewalls and routers locking the tested/hardened IP-routing. Then the DSiP can be used as a logical traffic-engineering layer on top of the robust IP-network.

3.5.4 Discussion of Study V

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, CIP and MIL users can rely on the adequacy of regular telecom operators' latency, but not on the performance of a single operator. This is also valid for the communication channels to be used by LEAs and their sensors globally. Mission and safe critical communications should use communication channels distributed in parallel because it must be failsafe and unbreakable.

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 surveillance, command and control 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.

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 a 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.

The communication channels for LEAs' satellite-based tracking sensors and systems should be integrated within the cyber secure public safety communications system.

3.6 Mobile digital services for law enforcement

European LEAs fight against organized crime every day to protect and serve European citizens. In this fight, they have to face the fact that international, mobile warehouses of crime are getting smarter every day and use modern technology to support and protect their criminal actions, which include human trafficking, drugs and terrorism. The task of the LEAs is to retrieve information from, monitor and record these criminal activities in a legal, traceable and unnoticed way. This means that the electronic equipment the LEAs require has to be smart, small, secure and have low power consumption to survive in the hostile criminal environment. Current devices are mostly based on a single-purpose use: a video sensor takes pictures, an audio recorder records sound. But what if these single-purpose devices were combined and integrated into the latest high-end technology made possible through research conducted by specialists and innovative manufacturers in Europe? Then, instead of individual single-purpose solutions, the LEAs would have at their disposal high-end integrated surveillance intelligence system suitable for diverse situations and easily adaptable to their demanding operations. Study VI focuses on border protection and its research question is: How can the digital services (e.g., mobile monitoring of sensors) LEAs need be effectively brought to the field, taking into account interoperability of systems and economic issues? The included conference paper can be referenced as follows:

> Jyri Rajamaki. Mobile Digital Services for Border Protection: Standardization of Emergency Response Vehicles. The European Intelligence and Security Informatics Conference (EISIC), 2013, 256-261.

3.6.1 Why mobile digital services for border protection?

LEAs, such as border guards, customs and police suffer from intensive human involvement. Due to the economic situation, LEAs' main issue is to maintain their core services on significantly reduced budgets. According to Study VI, the only realizable solution is better piggybacking of information and communications technology (ICT) and digital services. This also means infield operations, and thus in emergency response vehicles (ERV), ICT applications and digital services play an increasingly important role.

Recent developments regarding smart borders have highlighted the challenge of the smooth passage of third-country passengers and their requirements. First, border checks should be developed so that as large a portion as possible of third-country passengers themselves will register with RTP. Special attention must be given to the differentiation of information flows generated from border checks to EES purposes on one hand, and to the RTP purposes on the other. These information flows are complimentary and should be adjusted to those in the EUROSUR system with routine international messaging through official channels between border authorities and Frontex. This requires elementary development towards an automated border-check (ABC) process for RTP applicants. A similar procedure has been tested by the US Customs and Border Protection in Nogales, facilitated by an interviewing avatar kiosk developed by the BORDERS-network funded by the US Department of Homeland Security (DHS).

However, the inflows/outflows of travelers at some border crossing points (BCP) are highly seasonal. Hence an integrated border management approach cannot be tackled without taking into consideration 'ABC-lite' products, such as handheld/portable devices. This becomes more apparent when we consider the integration of all information from a BCP having to work with remote systems, such as EES, and crucially the RTP. With regard to mobility, the vehicle is the most important tool for all first responders (FR) due to the long patrolling distances; this is especially true with border troops in their field operations; FRs should have access to most of their digital services from their vehicles. The basic requirement for all mobile digital services is an infrastructure that includes data communications and a service platform.

3.6.2 Emergency response vehicles and their standardization aspects

The MOBI project has shown that the best way to provide digital services to the field for LE officers is via their vehicles. In field operations, LEAs' most important tool is their vehicle. However, typical Finnish patrol cars have more than 40 human machine interfaces for communication, navigation, field command, blue lights and other things on the deck beyond the car's own user interfaces. One big problem is that all these stand-alone systems consume a lot of power. We have measured a maximum of 203 amps when all possible systems are on. Also, wiring and ergonomics are problematic. This means that systems integration is really needed.

The review of current ERVs emphasizes that the design, services and solutions work under normal conditions. There are effective implementations of services and solutions in existing ERVs across various spectrums. However, the research study shows shortcomings in various respects. The study of the MOBI project emphasizes the end-users' requirements and their needs under various conditions, especially in challenging conditions. There are possibilities for improvements in various aspects of ERVs. These will enhance performance, effectiveness and optimum use of resources. Research studies show that the areas of improvement include emergency response preparedness, critical communication and real time updates, optimization of power supply, availability of resources and equipment, safety and sustainability and ease of use and optimization of computer systems (hardware and software). The EVRs are used in different conditions and environments. Hence, keeping end-user needs in mind leads to better and more sustainable services and solutions (Rathod & Kämppi 2013).

The end-user requirements specification has functional and non-functional requirements (Rathod & Kämppi 2013). Requirement gathering, analysis and specification resulted in working closely with end-users. Popular requirement-gathering techniques, such as the interviewing of LE officers and users of Finnish ERVs, joint application development, literature reviews and observation, have been used to generate the requirements specification. In certain requirements, an activity diagram and use cases are provided to visualize the logical modeling of business processes and workflows as well as the basic function of the systems in ERV. The end-user requirements specification reflects the actual users' views and how they see things in ERV. Hence the focus of the requirements specification is user-centric, along with the conducted research.

The grounded theory-based research of end-user requirements results in a layered approach. According to this approach, ERVs' electrical, electronic and ICT systems are divided into four layers that have standardized interfaces, as shown in Figure 19. These layers 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 layers.

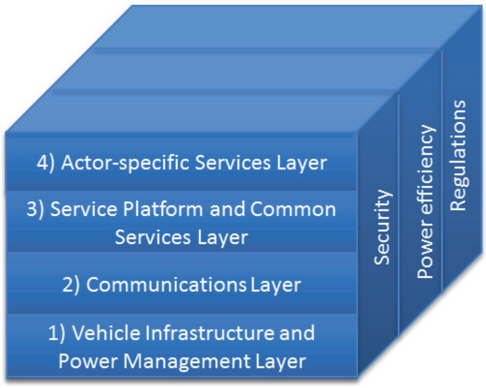


FIGURE 19 Four standardization layers of ERVs

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

In the current digital world, FRs are aware of the benefits that interconnection between different professional mobile radios (PMR) and the integration of new advanced data services could bring to their professional sectors. LTE is considered an appropriate technology for building next-generation broadband public safety networks. However, it does not yet support some voice communication characteristics that PMR technologies already offer. Also, PMR systems are widespread all over the world, making their replacement quite difficult within a short period. Therefore, some public safety organizations are working on dual solutions to provide TETRA voice capabilities together with broadband data transfers. The aspects to standardize within the communication layer could be divided into (1) long distance communications, (2) vehicle area communications and (3) personal area and accessory communications. Long distance communications includes vehicle–to-command–and-control-room and vehicle–to-vehicle communications. Vehicle area communications includes CAN, local area networks (LAN) and wireless local area networks (WLAN) as well as ad-hoc broadband communications between vehicles in field operations.

All ERVs have many similar applications, such as a navigation system, patrol tracking, target maps, activity logs, alarms and remote access to central databases as well as the control of blue lights and sirens, power supply systems and communications equipment. The common needs of the service platform and common services layer could be divided roughly into two main areas: (1) a decrease in the number of physical Human-Machine Interfaces (HMIs) and (2) a common field command system for all FR that also improves interoperability between different FR. However, several physical HMIs are needed for different modes of operation. For example, the HMIs when driving at full speed should be totally different from those in a mobile office mode, where ergonomics have an important role. In applying the design principles of service-oriented architecture, from an end-users' point of view, different existing systems will seem to form one part of the field command system.

When looking at new actor-specific services for border protection, unmanned border patrol systems, such as unmanned aerial vehicles (UAV), employ high-tech devices. For example, the border between Russia and southern Finland has many twists and turns. Small UAVs and micro air vehicles (MAV) could be posted at intervals and launched either automatically to check abnormalities detected by static surveillance sensors or by duty officers at the command posts (Ruoslahti, Guinness & Viitanen 2010). The United States uses a full-scale military UAV MQ9 Predator B to monitor its borders; however, there are limits to their intended use (Waterman 2007). According to (Bolkcom 2004), UAVs are likely to be fielded as part of a larger system of border surveillance, not as a solution in and of themselves. MAVs launched from command posts along hard-to-access borders could provide low-cost, rapid-response imagery and other data in response to suspected border incidents (Ruoslahti, Guinness & Viitanen 2010). A new ERV should be able to act as a mobile field command and control station. Future field command system standards should to take account the control of UAVs/MAVs.

3.6.3 Discussion of Study VI

The economic pressure decreases the budgets of the LEAs, which in turn increases the pressure for developing novel innovations. Study VI presents a layered approach for standardizing the electrical, electronic and ICT devices of ERVs. The generic framework for all ERVs is the baseline on which the harmonization and standardization of the proposals will be based. On the top of the framework, LEAs would operate new mobile digital services, such as mobile monitoring of GNSS-based sensors.

The benefits of the approach presented in Study VI to the development of ERVs are similar to those that the Open Systems Interconnection (OSI) reference model brought to the field of data communications. The layered approach breaks ERVs' electrical, electronic, information and communication technologies into smaller and simpler parts, as well as smaller and simpler components, thus aiding component development, design and troubleshooting. The standardized interfaces allow modular engineering, meaning that different types of hardware and software components communicate with each other. Interoperability between vendors allows multiple-vendor development through the standardization of ERV components. It defines the process for connecting two layers together, promoting interoperability between vendors. It allows vendors to compartmentalize their design efforts in order to fit a modular design that eases implementation and simplifies troubleshooting. The layered approach ensures the interoperability of technologies, preventing the changes in one layer affecting other layers, allowing quicker development and accelerating evolution. It provides effective updates and improvements to individual components without affecting other components. All these aspects have already been found to be highly valuable in the field of data communications after the OSI model was applied. In particular, open standards ease the ability of SMEs coming into the market, which improves the supply of new public safety ICT products and decreases their price. In addition to cost savings, the interoperability and availability of new public safety ICT services is improved.

3.7 Designing the future emergency response vehicle

In Finland, border, custom and police patrol cars are already quite similar because they are all equipped by the Police Technical Center. In addition, other ERVs such as fire trucks and ambulances have similar needs for their navigation systems, patrol tracking, target maps, activity logs, alarms and remote access to central databases as well as the control of blue lights and sirens, power supply systems and communications equipment. With the proliferation of ICT facilities and applications in ERVs, the number of HMIs has also increased dramatically. This has led to problems with functionality (e.g., lack of space for airbags) and technical issues with power supply and cabling and has highlighted several questions; for example: Can two items of equipment be combined into one to make it easier to use and decrease power consumption? Study VII aims to create a common ICT infrastructure for all ERVs, based on better integration of ICT systems, applications and services. Study VI also includes lessons learned from equipping the MOBI demo vehicle. The research question of Study VII is: How can LEAs' core services be guaranteed with significantly reduced budgets? The included article can be referenced as follows:

> Jyri Rajamaki. The MOBI Project: Designing the Future Emergency Service Vehicle. Vehicular Technology Magazine, IEEE , vol.8, no.2, June 2013, 92-99

The most essential tasks undertaken by PPDR responders include dealing with different kinds of emergency situations on land and water and in the air. The vehicles they use and the devices installed in these vehicles must be suitable for very demanding and variable conditions. Today's ERVs are packed with a large body of equipment. This has generated new problems with air bags, power supplies and cables, among other things. The documentation of applied solutions has been variable, and there has been no standardization, which is needed in this field, particularly because of the diversity of the equipment suppliers.

PPDR responders operate a large number and variety of vehicles, which are normally production vehicles that are retrofitted with a wide range of aftermarket equipment according to their roles. Study VII concentrates on van-sized vehicles. Depending on the organization, a PPDR vehicle can be divided in two or three sections. EMS vehicles might have two or three sections. In general, vehicles used by the LEA and rescue services have three sections. The cap comprises the front of the vehicle from which the vehicle is steered and controlled. The cap can also be applied for field-command. The mobile office is a space where troops can be chauffeured and/or in which a longer-lasting field-command environment can be set up. The transport unit is used for transporting goods, equipment, police/sniffer dogs and/or clients. The patient service unit of an EMS vehicle comprises the space where the patient is nursed and transported. Modern ERVs hold more information technology and other technical devices than ever. For example, police vehicles are mobile offices in which many customer interactions, such as ticketing and filling passport or driving license applications, can be dealt with. Police vehicles also contain many tools, cameras and technical devices for speed control and other traffic surveillance.

3.7.1 End-user and market needs

As an ever-increasing amount of technology is being installed in vehicles, the number of electronic devices, cables and user manuals that need to be carried also increases greatly, eating into the space available and making it rapidly unmanageable. The trend to transmit more data is also accelerating, driven by the necessity to provide the fast transfer of photos, videos and heavy documentation between the different units combined with strong network security. Mobile data connection must be available for PPDR responders in all situations. The essential features are network capacity, secure connections, transfer rate, load capacity and flexibility (Riippa 2011). In the future, it will be necessary to ensure transmission of more data. Especially in Finland, the amount of transferred mobile data is growing very rapidly because of increased co-operation between PPDR organizations, new data systems with better situational awareness and the moving office concept for the police. Current mobile terminals are not responding to users' needs for short-term mobile data operations, and new multi-channel devices are needed. In the near future in Europe, TETRA/Tetrapol and commercial mobile networks will act in parallel as service platforms for PPDR.

Due to the economic situation in Europe and the US, PPDR organizations' resources are meager. This has increased pressure on those organizations to pick up their slack. The tools for this are better cooperation between PPDR organizations and the utilization of ICT systems. PPDR responders have increasingly more ICT facilities and applications in their vehicles. However, each country and even each PPDR organization is developing its own solutions according to its legislation and requirements because uniform standards are missing. Tailored systems are expensive and difficult to support, and they have no built-in interoperability. This problem has been recognized. For example, the European Commission, the European Law Enforcement Agency EUROPOL and the European Agency for the Management of Operational Cooperation at the External Borders FRONTEX have come to the conclusion that the lack of interoperability limits the effectiveness of PPDR practitioners in actual operations (Baldini 2010). However, many potential aspects to interoperability exist, and it would be unaffordable and probably undesirable to provide for arbitrary seamless interchange of information. Whilst most potential user requirements for interoperability have been catered to in the technology standards, they have not always been implemented or activated in actual systems. So while user needs were addressed in the formulation of the standards, these interoperability needs were not specified when procuring and operating communications systems (Baldini 2010).

Technical standards are currently developed by separate bodies focused on critical communications or Intelligent Transport Systems (ITS). The TETRA + Critical Communications Association (TCCA) is focusing on mobile broadband for professional users. ISO/TC204 develops ITS standards at a global level, and CEN/TC278 and ETSI TC ITS do so at the European level. These technical standards define the capabilities of the systems. There is a need for an overarching body that can harmonize the profiles across systems and also agree on optimum means for achieving interoperability between critical communications and ITS. As the need for consistent data semantics grows, such a body might have a growing role in defining data standards and making PPDR adapt the much faster moving standards that are emerging from commercial mobile services. This role would be similar to that of the Internet Engineering Task Force and might be carried out by the Law Enforcement Working Party (LEWP) in conjunction with ETSI and CEN.

3.7.2 Solution approach

The main challenges of the MOBI project are how the ERV's ITC architecture should be arranged and how the vehicle should be built. In parallel with vehicle control systems, components of PPDR equipment have historically been been stand-alone equipment that is individually hard-wired using bespoke cable runs and connectors. Our solution for simplifying the ICT services provided for ERVs is to divide vehicles' ICT architecture into certain layers that have standardized interfaces, as presented in Study VI. The starting point of this solution is the needs of FRs: we apply the basic lines of human-centered design processes for interactive systems outlined in the ISO 9241-210 standard. Our solution is based on the technology available. The future development work is to standardize the three interfaces between these four layers.

Usually, a van-sized ERV is a generic van with added features. In Study VII, our example is the demo vehicle we have equipped. Our van-sized police car is a standard VW Transporter that has been customized by cutting off the roof from the cap and mobile office sections. Then, a higher fiberglass ceiling including emergency lights, alarms and GPS, 2G/3G and Wi-Fi antennas were retrofitted. The antennas were wired on the top of the original metal roof above the transport unit. In addition, for example, the bars of the transport unit (also used as a jail) in the rear were installed as well as a mobile office room table and seats.

Our demo vehicle includes an intelligent electric power distribution and control system that contains the control unit, which turns off low-priority systems during low battery voltages. The inverter converts 12Vdc battery voltages to 230Vac needed, for example for the laser printer. A 230Vac/12Vdc rectifier is used in garages and other places where the mains current is available. STANDBY includes headlights, an alarm and work lights and their control systems as well as electric central locking systems and fans for cooling. When the engine is running, the van's start battery charger also recharges STANDBY's own batteries. Certain information from the vehicle's Control Area Network (CAN) bus, such as engine performance, available fuel amount and level of battery voltages, is passed to the STANDBY system.

Power consumption is one of the biggest challenges in PPDR vehicles. For that reason, we are at present determining the number of necessary physical and virtual computers and examining the power consumption of other power-consuming devices during various operational modes. Currently, our demo vehicle includes a lead-acid start battery (72Ah) and Nickel-Metal Hydride (Ni-MH) batteries (3x30Ah) for PPDR ICT systems. In the near future, other options for power generation, such as fuel cells, will be examined.

3.7.3 Communications layer

ERVs' communications needs can be divided into long distance communications, local area networks and accessory communications. Furthermore, each category is scaled from light to heavy. ICT solutions have to be robust and easy to install. Special attention has to be paid to information security. Various encryption methods between different kinds of systems bring their own challenges to this project and its information security solutions. In addition, all PPDR actors have their own requirements regarding how to implement information security into their vehicles' systems.

Our demo vehicle is equipped with a TETRA radio, used mainly for voice communications, and with a separate multichannel router, which is connected to the control and command room applications via parallel TETRA, 2G/3G, LTE/4G, WLAN and satellite data access technologies. A multichannel router offers a redundant solution when more than one functional data communication channel for data transmission exists. Our demo uses DSiP, which allows the use of several parallel communication paths simultaneously, as discussed in Study V. DSiP handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution. Multichannel Router's Quality of Service (QoS) option sets the desired order of network access by desired Cost of Service (CoS) value. Therefore, when operating in areas where the network availability and signal strength vary widely, the network exchange proceeds without the user noticing it and without breaking the connection. The user organization will choose in advance whether to use either the strongest signal or the cheapest cost network, or some combination of these. This selection is made by setting the value of the CoS.

There is a need for secure, uninterruptable communication in many applications. Different approaches have been addressed to mitigate the problems; examples include Multi-Path TCP-stack (MPTCP) and an open source project with a multichannel VPN solution (OpenVPN). However, DSiP appears to be the only commercially available solution today addressing a large number of known problems. When comparing, for example, Communications Access for Land Mobiles (CALM) for intelligent transportation systems initiative by the ISO to DSiP, it becomes apparent that CALM is still a work in progress. Therefore, large-scale implementations of the standard do not yet exist. DSiP-based systems, on the other hand, have been in operative use in critical installations for several years, such as in the Finnish Coast Guard's coastal surveillance solution and the SCADA control of Finland's main power grid. Another reason for selecting the DSiP solution for our demo vehicle is that the CALM architecture is based on an IPv6 convergence layer that decouples applications from the communication infrastructure, whereas DSiP is insensitive towards the transport layer and can freely use the IPv4 and IPv6 networks as transport with tunneling capabilities. In addition, compared to CALM, applications can use and transparently communicate through the DSiP mesh without having to implement the interfaces with APIs. This effectively means that there is no need to modify applications or equipment when applying DSiP.

3.7.4 Service platform and digital services

The standardized communication layer for all PPDR organizations enables cooperation between authorities, for example by setting up a common talk group for incident communications. The next pitch of harmonizing is the service platform and common services layer, where the design principles of Service Oriented Architecture (SOA) can be applied.

With a plenitude of new ICT systems in PPDR vehicles, the number of user interfaces has increased by dozens. Of course, ICT systems require HMIs. However, the number of different HMIs should be reduced. So whenever possible, HMIs should interact with multiple systems and/or functions. HMI functions and logic should be standardized in order to simplify the use of multiple systems. Standardized HMIs (a standard keyboard, touch screen, mouse) increase the ease of the user's experience and improve efficient usage of the systems. ERVs' HMIs should be robust and easy to operate under all conditions. ERVs must be operational in varying natural conditions, such as when the environment is dark, cold, hot or moist. HMIs must be easy to access and use even when the vehicle is moving at a high speed. All these should be operable with thin gloves, at least to some extent. The systems should be able to generate any information, notice or warning in the same language as the HMI. The system navigation should be clear and easy to adopt. The user should be able to get 24/7 operational support related to the system. In our demo vehicle, a key feature is the graphical HMI that has replaced many hard keys on the dashboard with soft keys on a touch screen. It enables an easy-to-reach functionality in the main applications, such as the field command system, power management, emergency lights, alarms and voice radio as well as management of the PC itself and any other third-party applications running on a Windows platform.

A field command system is a complete solution and platform that integrates different applications into one easy-to-use interface. The same technology and application could be used by all PPDR responders. This improves interoperability between PPDR organizations and enables field operations to be more effective. Today, the most important data system of Finnish police vehicles is the POKE Field Command System. It consists of different kinds of maps including aerial photos, patrol tracking, messaging, activity logs and information sharing. The system has access and enquiry facilities to several databases, and it includes resource management and dispatching as well as reporting applications. POKE has many other features and several devices, such as fingerprint scanners, that can be connected to it (Hätönen 2012). It is also used by other Finnish authorities and some information is shared. However, only the police use this system nationwide. The system is created for the police and does not fulfill the needs of all PPDR responders. So, further development work is needed; however, POKE is a good starting point. Other field command systems to be studied include, for example, the MERLOT product family developed by Lociga Ltd and used in some Finnish regional rescue departments, SAFEcommand developed by EADS Astrium Company and used in rescue services in the United Kingdom and an army-specific Blue Force Tracking (BFC) technology Force XXI Battle Command Brigade and Below (FBCB2) used by the United States Army, the United States Marines Corps and the British Army.

3.7.5 Discussion of Study VII

Study VI divides ERVs' ICT systems into four layers with standardized interfaces. For Study VII, we equipped a demo vehicle that is used for tests and further research by the PPDR actors and business partners. Our end-user requirement analysis shows that whilst ambulances, police cars and fire trucks are quite different, their communications layer as well as the service platform and common services layer could be identical. Similarities within the two middle layers will also help in standardizing all the three interfaces.

The adoption of open standards and the capability to change between vehicle and equipment suppliers will become increasingly important for PPDR organizations, which are facing significant pressure to maintain core services with significantly reduced budgets. Open standards ensure that PPDR equipment is generic and has a high level of interoperability. The equipment fitted to a vehicle may well be replaced over its operational life as organizations introduce new technologies. Similarly, equipment may be added, removed or refreshed, for example when there is a change of equipment supplier. Standardized interfaces will minimize or ideally eliminate the requirement for a partial or full refit of the cabling and additional control systems within the vehicle, resulting in significant reductions to the costs involved in stripping out and refitting proprietary control systems. PPDR organizations will also promote innovation and competition between equipment providers in terms of the provision of user functionality, interoperability and services to actively support the delivery of front line services. In the future, standards should also be suitable for actors other than just PPDRs. For example, critical infrastructure companies, the private security sector and fleet management services may have needs for mobile monitoring station-like vehicle solutions.

It is a proven fact that standardization strongly affects businesses that develop and sell technologies and technology-based products and services (Kivimäki 2007). The development of a new ICT concept is significantly expensive, thus making access to the international market desirable. By improving on the supply of new PPDR ICT products and decreasing prices, standardization makes it easier, especially for small and medium-sized enterprises (SMEs), to compete against bigger firms. Applying standardized interfaces and common platforms enables new innovations to place more emphasis on the development of digital, rather than physical, services. SMEs are often quicker at making digital service innovations.

At the moment, in many countries, de facto standardization of ERVs is ongoing with the participation of the car industry, public safety organizations, critical communications equipment suppliers and software integrators. Moreover, many de jure standardization projects are under way, for example in the field of public safety communications by the European Telecommunications Standards Institute (ETSI), the International Telecommunications Union (ITU), 3GPP, the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE), and in the field of intelligent transport systems by the International Organization for Standardization (ISO), the European Committee for Standardisation (CEN) and ETSI. Our goal is to work towards an international open standard that enhances and eases the cooperation between PPDR actors. To improve interoperability and availability of new PPDR ICT services, standardization development with like-minded countries should be started in Europe. The potential entity behind such development could be the Law Enforcement Working Party (LEWP) in conjunction with ETSI and CEN.

Study VII broadens the ERV concept presented in Study VI to first responders other than just LEAs. This "out-of-the-silos" thinking enables new business models for PPDR actors, their equipment and service providers. PPDR organizations will also promote innovations and competition between equipment providers in terms of the provision of user functionality, interoperability and services to actively support the delivery of front line services. This development also guarantees the continuance LEAs' core services in the case of significantly reduced budgets.

3.8 IT service governance model for PPDR organizations

Study VIII deals with the research theme of how PPDR organizations, such as LEAs, should choose their service delivery models for new digital services, such as tracking systems. The research question is: How can LEAs manage the multi-supply environment of their new ICT systems? The included conference paper can be referenced as follows:

> Jyri Rajamaki and Markus Vuorinen. Multi-supplier integration management for public protection and disaster relief (PPDR) organizations. *International Conference on International Conference on Information Networking (ICOIN)*, 2013, 499-504.

According to the results of Study VIII, the foundation for IT service governance should be based on ITIL service management. The service strategy is driving the service portfolio based on the operational requirements of PPDR organizations. Figure 20 shows the new framework for IT service governance designed within Study VIII. Around the service strategy is the cycle for planning, implementing and operating services. The input for service requirements comes from within the service strategy.

The way the service should be delivered is planned within the service design phase. For service design, there are alternatives from standard utility servers to tailored in-house systems. The aspects of utility-based computing and selective sourcing should be planned as presented by (Lacity, Willcocks & Feeny 1966) and is shown in Figure 11 and Figure 12. The questions to be asked are: Would the service be somewhat more effective to operate in-house? Is the service something that can be provided as cost-effectively as a cloud/utility service? The main sourcing strategy for the service is chosen at this stage. PPDR organizations should use the selective sourcing matrix to regularly categorize their services in respect to which group the services belong to. For some organizations, there could be plenty of useful differentiators that are costly to maintain and provide only a little operational value. Correct usage of the matrix helps PPDR organizations to focus on value-adding IT services and eliminating or outsourcing non-value-adding IT services.

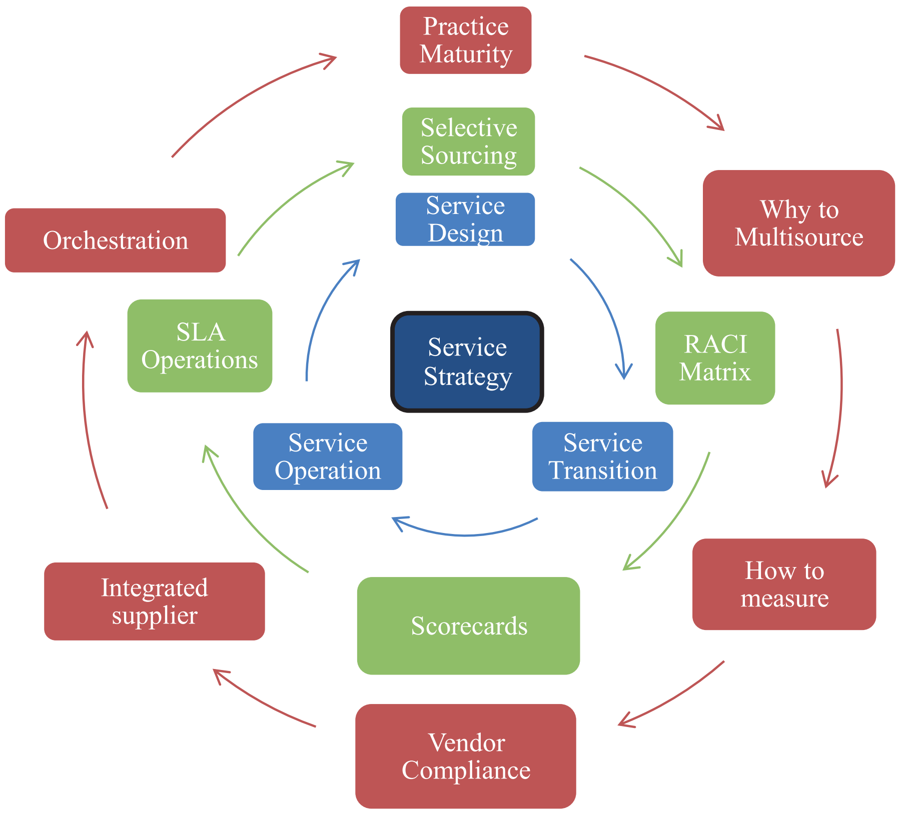


FIGURE 20 Selective sourcing, RACI matrixes, SLA's and ESM at the different phases of service strategy

The next phase is the service transition, where the service is implemented and defined at a detailed level within the service operating model. In order to assure an effective governance model in the service transition phase, a RACI matrix should be created. The matrix informs the deliverables and responsibilities between the client and the suppliers. Creating a RACI matrix assures that during the service operation phase all roles and scope are defined in advance, and the service can be operated. Based on the RACI matrix and the service, deliverables can be initiated with the design of Service Level Agreements (SLAs) and other Key Performance Indicators (KPI). These service levels will be included in the agreement between suppliers and the client.

The final service operation phase is when the service is in the production phase and is being used. Based on the responsibilities defined in the service transition, initial SLA measures can be designed for the agreement. This way, it can be assured that SLAs are in line with supplier accountability and deliverables. The SLA's must be flexible in order to maintain their capacity to adjust to changing business requirements.

The ESM framework guides in checking the readiness for sourcing at different phases of service design. Here, the main questions are: Is the organization ready for multi-sourcing? What are the targeted benefits and how can they be measured? Are the suppliers compliant with PPDR requirements? How can they be migrated to an integrated supplier? and Are some further orchestrations required in the operation phase? The ESM practice is described in the outermost cycle.

3.8.1 Benefits of the new framework

If the multi-supplier governance of service strategy is done based on the described practices, several benefits can be gained. The ITIL service strategy is divided into three phases: design, transition and operation. In this section, the benefits for each phase are described.

The decision over what and how to outsource is made in the design phase. There are areas that can be more effectively outsourced and areas where insourcing is more effective. Further, there can be some areas where utility-based services are more effective than traditional services. Using this framework gives organizations the right sourcing solution from the start. The ESM practice also guides in answering why that is being done.

Within the service transition phase, usage of the RACI matrix will clarify in a clear documented form the responsibilities between the client and suppliers. If this RACI matrix is used prior to the service operation phase and all the gaps and responsibilities are defined in advance, a lot of problems during the operation phase can be avoided. Based on the responsibilities defined in service transition, the initial SLA measures for contract can be designed. This way, it can be assured that SLAs are in line with supplier accountability and in line with deliverables as well—that is, information about what is measured and how should be provided is taken care of.

Prior to going into the service operation phase, the service compliance must be verified so that it will be compliant with the PPDR service and policy requirements and assign correlating scorecards. The service operations phase is the phase where the service is in operation and the supplier has integrated to a part of the PPDR services. During this phase the service is reviewed and performance evaluated if there are requirements to change the SLA levels. The benefit of adjusting SLA measures and levels at this stage is to have service levels responding to the business requirements.

In brief, the new model will allow multi-supplier governance deliverables to be well defined, measurable, aligned and sourced best way and service levels to be adjustable based on requirements. This model also provides PPDR organizations with answers to why they are multi-sourcing certain activities, whether they are they compliant with their service requirements and whether the targets have been achieved.

3.8.2 Discussion of Study VIII

Multi-supplier governance has been well studied over the past years. Despite the research, no standardized best practices for managing multi-supplier governance are yet in place. ITIL and other Information Technology Service Management (ITSM) methodologies support and give certain advice on this matter. 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 (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.

Study VIII proposes a new framework for an operating model in multi-supplier sourcing of ICT systems and digital services. This new model is a combination of smart sourcing, usage of RACI matrixes and on-going SLA management. When correctly applied, the model improves the service quality, supplier collaboration and cost efficiency of IT services. The proposed framework provides organizations with a sourcing method aligned with corporate ITSM practices.

3.9 Cross-case conclusions

This section makes cross-case conclusions for the eight cases and answers the main research question: *How can new types of satellite-based tracking sensors, mobile monitoring stations and their associated communication channels for law enforcement (LE) operations be understood and designed, taking into account the chain-of-custody and monitoring-of-legality requirements?* Section 3.9.1 deals with answering the research question, and Section 3.9.2 presents a model of the intelligence system for improved law enforcement.

3.9.1 Understanding satellite-based tracking systems for law enforcement

The 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 the constitutional state. It has been verified by means of participative observations that LE organizations have a tendency to create two-level systems: some that work on the streets and others that are valid in the courts of justice. Some European countries are well on their way towards this phase of development. 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, LEAs' investigations and data capture cannot be made public. However, they could be so transparent that the criticism and control made by citizens is possible to come true.

Due to the economic situation, the main need of LEAs is to maintain their core services with significantly reduced budgets. This means that they need new automation equipment and digital services for routine tasks. Also, all ICT systems should have long life-spans, and new systems should be interoperable with old ones. The Finnish approach to providing digital services to the field for LE officers is via their vehicles. Under this economic pressure, it is vital that different safety authorities develop a common ERV concept together. This enables new mobile digital services for first responders in their field operations. However, IT service governance needs development.

According to the qualitative multiple case study analysis, the major challenges that LEAs confront when using tracking equipment in crime investigations and prevention are as follows: (1) Commercial GNSS sensors do not fulfill the needs of LEAs; (2) Cross-border operations are problematic because crime has internationalized but LEAs are national organizations; (3) Secure mobile communications should be available worldwide, energy efficient and invisible to suspects; (4) Investigation data should fulfill chain-of-custody requirements and (5) LEAs' operations should have societal acceptance and monitoring-of-legality.

Utilizing artificial intelligence and machine type learning, the functional quality and energy consumption of tracking sensors could be improved in many ways. Because the battery is the biggest component of GNSS-sensors, the size of the sensors could be made smaller without functional compromises.

LEAs as well as their preventive and forensic tracking, audio-visual and other types of sensors need global cyber-secure communication channels. According to this dissertation, these communication needs could be fulfilled by a distributed system applying multiple simultaneous access technologies and communication paths. Taking into account interoperability with existing systems and economic issues, this communication system could be realized in conjunction with other public safety and critical infrastructure protection actors, such as military, fire and rescue services, emergency medical services, energy management, water supply and sewerage.

LEAs' present-day ICT systems do not support cross-border cooperation. In addition to these technical challenges, the distrust between LE organizations causes trouble. Unfortunately, this distrust also exists at the national level, and even between units of one organization. However, common ICT systems and operational procedures could increase the trust between parties. 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 EU's presidency country) should develop common procedures to apply new LE technology. In the future, these procedures could be extended to other European countries as well as standardizing procedures for applying older LE technologies.

3.9.2 Model for future law enforcement intelligence system

Figure 21 shows a model for LE satellite-based tracking systems that demonstrates the identifiable networks across all three SIS layers of the different systems.

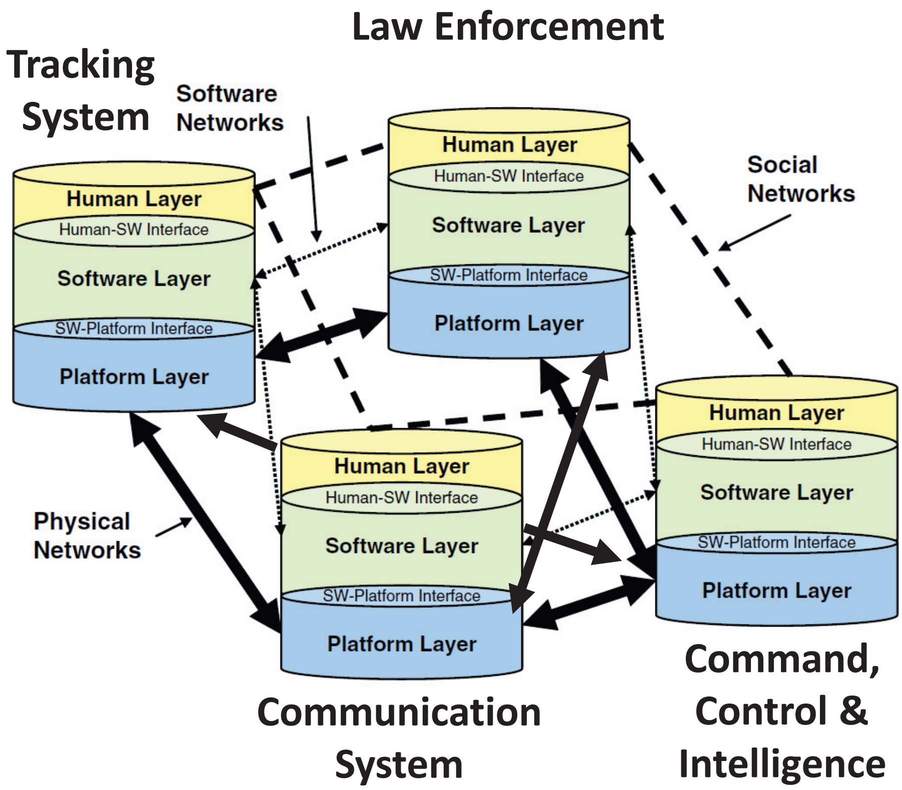


FIGURE 21 SIS model for law enforcement tracking systems

Figure 22 shows the principle of multi-use of law enforcement forensic sensor data that could be a part of the command, control and intelligence system of law enforcement. Integrating criminal investigations, chain-of-custody and monitoring-of-legality into the same system of software-intensive systems offers many advantages. One of the key strands of integrated criminal prevention policy starts with the multi-use of relevant information across sectors and borders, boosting the effectiveness and cost-efficiency of law enforcement activity. Currently, however, the EU, national law enforcement and other public authorities are responsible for different functionalities of criminal preventions. A political, cultural, legal and technical environment should be created for enabling information sharing and multi-use between existing and future criminal investigations, chain-of-custody and monitoring-of-legality systems. The system should ensure data security, and especially information integrity and authenticity. It is also evident that the state authorities require some sort of institutionalized and standardized procedure in order to accept and trust the system. In addition, informal systems are needed to support the formal ones in order to survive the present social and political situation. According to conventional wisdom, trust is critical in such multi-use systems and procedures.

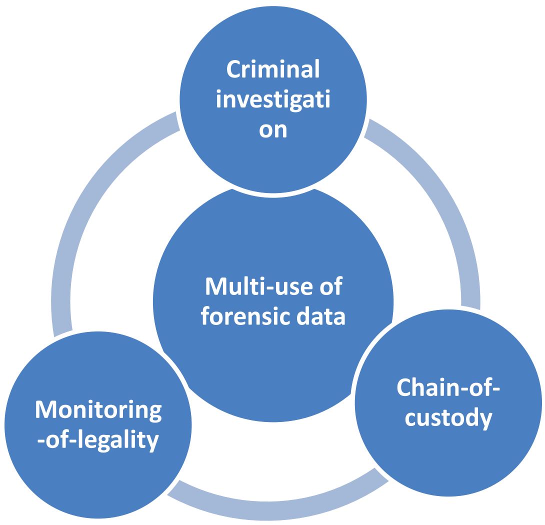


FIGURE 22 Multi-use of law enforcement sensor data

4 DISCUSSION

4.1 Additions to the knowledge base

Organized crime is a real cross-border threat with the emergence of international warehouses of crime. To improve their evidence-gathering abilities, law enforcement authorities (LEAs) are constantly seeking new technological recording, retrieving and monitoring solutions to facilitate their combat against criminal organizations. The criminals' counter-measure activities, such as electronic counter-surveillance, jamming and constant changes in behavior for preventing eavesdropping or physical surveillance, are continuously increasing. The pressure to find new intelligent technologies—which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive—is emerging and is a high-priority task. Study I provides an improved understanding of the structural characteristics and dynamic evolution of mobile communication challenges to the cross-border satellite-based tracking operations carried out by LEAs. Before the SATERISK and MACICO projects, this field was unresearched.

In preventing and investigating crimes, LEAs perform a variety of activities that affect civilians' privacy. Video surveillance, audio surveillance, technical monitoring and tracking are a few to mention amongst many other activities. In various instances, law enforcement has sought more control rights, which increases concern amongst citizens and also the level of open debate on the topic. Earlier research has concentrated on either privacy issues from the citizens' point of view or on developing new forensic technologies for LEAs. Alternatively, Study II provides an improved understanding about why transparency is a crucial factor for the success of LEAs' technical surveillance. This research work also presents examples of current technological possibilities to create transparent and plausible monitoring for surveillance activities. Trust in LEAs has always been high in Finland. Nevertheless, there are a number of people in society who do not have any confidence in the authorities, especially in police forces and their expanded control. However, there is empirical and factual evidence pointing to the fact that civilians are willing to give authorities expanded rights to use intrusive means in extremely critical situations. In such cases, people are more open to the idea and expect authentic and timely information.

Study III shows that when investigating the identity of criminals, LEAs may apply technical tools that are totally different from those used when gathering evidences for charge because the data provided by their investigations may not be valid in court. For this reason, a new monitoring system that goes beyond the state–of-the-art is needed. Three organizational layers need attention: (1) LEA—the people that actually retrieve and store the information, (2) Prosecutors and their offices—how they get access to the information and (3) Courts—the final destination of the retrieved information. Until now, the LEAs' information gathering tools have been engineered focusing only on the best way to retrieve information from the target. The attention paid to the legal, integrity and chain-of-custody requirements, and to social acceptance and legal oversight in connection with retrieving information, has been inadequate, and guidance on the matter has existed only in manuals written by legal departments.

The activities of organized crime networks are more complex, diverse and international in scope than ever before, requiring LEAs to have better electronic equipment for technical surveillance of their activities. Study IV belongs to the first stage of the systems engineering (SE) life-cycle. This multiple case study analysis of four public safety-related research and development projects explores novel satellite-based tracking systems for better LE. The system-of-interest (SoI) includes small, low-power and smart sensors as well as the monitoring system and its associated communication channels. The research findings emphasized the transparency of LE. The integration of technical surveillance and legality control to the same SoI will improve the satisfaction of both the chain-of-custody requirements and their social acceptance. SE is a technical and technical management process widely used in the military sector, and research articles exist in this field. However, research papers on applying SE in law enforcement sector do not exist as of yet.

Study V focuses on the future requirements of broadband data transmission of public protection and disaster relief, critical infrastructure protection and the military, and presents the concept of redundant and secure data communication network systems in the multi-organizational environment. Much research exists in this field. However, Study V proposes a new fully decentralized architecture with optimized critical communication channels. 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 will be highly fault-tolerant in routine as well as crisis operations. The software-based approach will be independent of heterogeneous data communication technologies, IP networks and telecommunication operator services. The solution will enable 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.

LEAs endure intense human interaction. Due to the economic situation, the main need of LEAs is to maintain their core services with significantly reduced budgets. According to Study VI, the only realizable solution is the piggybacking of information and communications technology (ICT) and digital services. This also means infield operations, and thus emergency response vehicles (ERV), ICT applications and digital services will play an increasingly important role. Study VI presents a new layered approach for standardizing the electrical, electronic and ICT devices of ERVs. Thus, on the basis of this infrastructure, future mobile digital services, such as for the tracking of criminals, could be supplied.

Much research is carried out on how to develop a better police car, fire truck or ambulance. Instead of these silo approaches, Study VII aims to create a common ICT infrastructure for all ERVs. The approach is to divide ERVs' ICT systems into four layers (a vehicle infrastructure and power management layer, a communications layer, a service platform and common services layer and an actor-specific services layer) between which there are standardized interfaces. In addition to cost savings, interoperability and the availability of new PPDR ICT services will also improve.

Cloud sourcing and multi-sourcing are growing rapidly and are a part of the success criteria for today's IT departments. IT services are often operated by multiple suppliers, but only very few of the client organizations are getting planned savings and service quality within multi-supplier environments. The Information Technology Infrastructure Library (ITIL); Service Level Agreements (SLA) Management; Enterprise Service Management (ESM); Responsible, Accountable, Consulted and Informed (RACI) matrix and selective sourcing practices have been created to respond to this problem but have not been aligned to be jointly used during the service life-cycle. Study VIII presents a new model, describing how multi-supplier environments should be managed. The new method shows how existing frameworks should be aligned from a service management point of view. Attention is paid to how Public Protection and Disaster Relief (PPDR) organizations should choose their service delivery model. When service delivery is a mixture of in-house, outsourcing and cloud sourcing services, the operating model, responsibilities and scorecards between suppliers must be clarified.

A GNSS-based tracking system for law enforcement is a complex system of software-intensive systems that consists of different socio-digital systems, such as law enforcement, GNSS-based tracking systems, communication systems and command, control and monitoring systems. The application of systems engineering principles has a long history in the military sector, and SE could also have benefits for developing new law enforcement systems and services. However, today's ICT systems involve a complexity that extends beyond what can be addressed by traditional design approaches (Hanseth & Lyytinen

2010). The cross-case conclusions of this dissertation provide an addition to the knowledge base of systems engineering of complex software-intensive systems in respect to law enforcement technology services. With regard to GNSS-based tracking systems for law enforcement, a SE-based approach is practical for designing command, control and monitoring systems because LEAs have the full governance of these systems. On the other hand, GNSS and communication systems are governed by service operators, and law enforcement is a system of human actions supported by ICT and other technologies. Because II theory tackles IIs' dynamic complexity (Hanseth & Lyytinen 2010), it should be applied to supplement the SE approach. An implication of the cross-case conclusions is the new model for multi-use of law enforcement forensic sensor data that could be a part of the command, control and intelligence system of overall law enforcement, including criminal investigations, chain-of-custody requirements and monitoring-of-legality.

4.2 Applications in the appropriate environment

Table 2 lists the 1 artifacts that were developed within the whole DSR. For improving law enforcement, different functions are needed, such as criminal investigation, chain-of-custody and monitoring-of-legality. All these systems and sub-systems have many stakeholders with different requirements. This dissertation presents a PoC model for the multi-use of surveillance sensor data. A modular approach (sensors, monitoring systems, communications) means that new technologies are easy to apply, and new types of sensors can be easily included to the system. The integration of (1) investigation data, (2) digital evidence (=chain-of-custody requirements) and (3) monitoring-of-legality into the same system of SIS will provides multiple applications and benefits for many stakeholders, and no triplicate work is needed. Table 10 summarizes the main stakeholder needs, benefits and applications of the new types of GNSS-sensors, (mobile) monitoring stations and their associated communication channels for LEA operation in the field, taking into account the chain-of-custody requirements and the societal acceptance of these solutions.

TABLE 10 Stakeholders and their needs/benefits/applications

Stakeholder	Needs/benefits/applications
Citizens	Transparency of surveillance. Balance between surveillance and privacy. Efficient law enforcement; Value for money.
Targets	Fair, lawful, proportional and accountable surveillance.
LEAs	Better tools for the recording, retrieving and monitoring of

	criminal activities. Better tools and processes for cross-border operations and cooperation.
Prosecutors	Chain-of- evidence requirements.
Court of law	Chain-of-custody requirements.
Legal officers	Tools for legality control.
Legislators	Commonly agreed upon balance level between surveillance and privacy. Identification of the legal barriers to the EU-wide deployment of the system of interest.
Manufacturers and private service providers	More business opportunities by, for example, less fragmented markets and international standards.
Public service providers	More users of their services providing business continuity.
Funding agency	An efficient return on investment ratio.

4.3 Audit of the study

The method of study (Miles & Huberman 1994) used for auditing and judging the quality of this research consisted of asking and answering a set of questions during the eight studies. This study integrates multiple case study research into design science research and is primarily qualitative in nature. In qualitative design, the researcher is the principle instrument for collecting and analyzing data, and this lends itself to certain inherent strengths and limitations (Merriam 1998). The intimate relationship that the qualitative researcher establishes with the central phenomenon, the data collection, and the data analysis lends a very human element to the research conducted in any qualitative study. It is critical for the researcher to position him or herself within the study context such that biases, beliefs, and assumptions about both the central phenomenon and the research process are clarified.

It is not always a problem that the researcher comes equipped with biases, beliefs and assumptions because they allow the researcher to make meaning of the data. According to Miles and Huberman (1994), a problem arises when these crucial underpinnings of analysis remain mostly implicit and are explained only allusively. We need to make explicit the procedures and thought processes that qualitative researchers actually use in their work (Miles & Huberman 1994).

In this study, a conscious effort was made to position the researcher himself in relation to the research approach and the central phenomenon for this study. According to Merriam (1998), a qualitative study is only as good as the individuals conducting the study, and qualities such as tolerance for ambiguity, being highly intuitive, and having good communication skills are critical if one intends to maximize results. I trust with my skills in these areas mentioned by Merriam. The job assignments of the researcher as the scientific supervisor of the research projects may raise the question of the researcher's objectivity. However, the role of the researcher—arising from job assignments in all research projects—has been the role of expert, with the conscious aim of collecting objective results. The results of this study are based on the interviews with end-users and the additional material provided by other sources of information, thus enabling a triangulation of the information.

4.3.1 Design science research quality

Hevner et al. (2004) have established the seven guidelines (see Chapter 1) for assisting the researcher, reviewers, editors and readers to understand the requirements for effective DSR. In this dissertation, the guidelines are qualified as following:

1) Design as an artifact: A proof-of-concept model is developed.
2) Problem relevance: The objective of the study is to develop technology-based solutions to important and relevant LE problems dealing with criminal investigations, chain-of-custody and monitoring-of-legality.
3) Design evaluation: The PoC model is evaluated through eight case studies.
4) Research contributions: See section 4.1.
5) Research rigor: The eight included publications are quality-classified by the Publication Forum initiative of the Universities Finland UNIFI. All eight of the articles include a double review process by international reviewers with expertise in the relevant subject area; furthermore, the related parts of the studies have been presented at international conferences.
6) Design as a research process: The search process and path is documented via the "other publications" listed on pages 18–20 of this dissertation.
7) Communication of research: The results have been presented at 65 conferences to both technology-oriented and management-oriented audiences.

In this study, the main limitation is related to the difficulties of identifying and measuring the constructs that refer to the relationships among the phenomena being studied, such as "transparency," "security" and "privacy." The general delimitation of qualitative analysis is that it applies to presenting a study where the results lack statistical reliability, and they cannot be generalized without a deeper quantitative analysis, or that additional multi-methodological and multidisciplinary research and analysis is needed for proofing the research results in the future (Gummesson 2000, Robson 2002, Locke, Spirduso & Silverman 2007, Winter 2010).

4.3.2 Validity and reliability of case study research

Yin (1994) presents four tests to ensure the quality of case study research:

- Construct validity (establishing correct operational measures for the concepts being studied)

- Internal validity (establishing a causal relationship, whereby certain conditions are shown to lead other conditions)

- External validity (establishing the domain to which a study's findings can be generalized)

- Reliability (demonstrating that the operations of a study can be repeated with the same results).

4.3.2.1 Construct Validity

Construct validity can be met by the use of multiple sources of evidence. This study has used documents, interviews, direct observation, participant observation and physical artifacts as sources of evidence. The documentary information consisted of six collected themes of data created within four R&D projects: books, research articles, theses, project reports, board meetings data and seminar data (see Table 4). An effort to minimize potential limitations was sought through the collection of a variety of data sources from multiple perspectives, feedback and direction from experts and thorough self-exploration prior to entering into the context of the study. Feedback was given by numerous experts on the conclusions and verifications of the collected data. The validating procedures also include 65 presentations at international conferences and comments and suggestions from conference participants regarding the research issues (see the list of publications in pages 15, 17–18). The included articles of this dissertation included a double review process by international reviewers with expertise in the relevant subject area.

In this research, "construct validity" refers to the correct operational measures for the integrative theme (surveillance data = digital evidence = data for monitoring-of-legality) being studied. Construct validity was addressed to the extent of "what was to be measured was actually measured" or "does it measure what you think it measures?" as Robson (2002) proposes. As Robson states, there is no easy, single way to determine construct validity. Yin (2003) cautions novice researchers integrating embedded units into a case study design, noting that novices tend to conduct analyses at the subunit level and fail to return to the global phenomenon central to the research study. This is a valid concern, especially considering the complexities inherent to the phenomena of tracking sensors and communication and command, control and intelligence systems explored in this embedded case study design. In an effort to not lose site of the global issue at the heart of this study, the cross-case conclusions of results for this study returned to the global level of the phenomena central to this CSR.

4.3.2.2 Internal Validity

Yin (1994) states that that the internal validity can be extended to the broader problem of making inferences. The inferences have to be correct, and all the rival explanations and possibilities should be considered. This study involved a number of decision-makers (advisory board members), researchers and other experts in all four research projects with whom the research findings, rival explanations and possibilities were discussed.

In this research, the internal validity and authenticity, as well as credibility, refer to the establishment of casual relationships; the targets of the studies aim to increase the trustworthiness of and understanding that studies make sense and are credible enough for audiences (Miles & Huberman 1994). The design of the research was based on a combination of a thorough understanding of the theoretical framework and on wide experimental knowledge, for example, of the concepts and their relationships that were used to explain actions and meaning concerning the research questions. The internal validity of the results produced by the newly created models is in the realizations, both parallel with and in addition to the analyses and methods, models and new processes. The objective was to ensure that the new propositions are logical, authentic and internally valid from the perspective of IS, SE, SIS, II, security and services in the context of crime investigation, chain-of-custody and monitoring-of-legality.

From the perspective of authenticity, the transparency of data displays inspired the author's thinking and led to new ideas as well as the emergence of new models and new information systems. The analysis was carried out in collaboration with colleagues involved in the research projects. The data were reduced and understood first separately and then discussed, compared and combined with the displays, categories and models. In addition to increasing the internal validity, such researcher triangulation facilitated the emergence and elaboration of different theoretical views and concepts before the final categories, and a proof-of-concept model of the multi-use of surveillance data was created. I started the data reduction and data coding in accordance with the sampling technique and continued data collection in all eight studies. I compared the results and interpretations, which correlated with each other. As described in the chapter on methodology, the data were reduced and analyzed collaboratively in a setting that reinforced the internal validity of all eight studies. According to Corbin and Strauss (2008), the term "FIT" pertains to the validity of the study and means that the theory must fit the substantive area to which it will be applied. The term "FIT" also indicates that the data categories should not be chosen from pre-established theoretical points of view. In the propositions of the studies, the proof-of-concept model was developed as an inductive and constructive design-stream from the empirical data, as described earlier in the methods section (Patton 1990, Miles & Huberman 1994, Robson 2002, Brannen 2004, Corbin & Strauss 2008, RW.ERROR - Unable to find reference:134).

4.3.2.3 External Validity

The test of external validity deals with the problem of knowing whether a study's findings are generalizable beyond the immediate case study. According to the Contingency Theory of Organizations (Lawrence, Lorsch & Garrison 1967), no single action or model suits all intensive actors. Lawrence et al. state that an actor's environmental and cultural requirements should determine the appropriate creation structure for a realization model and its implementation. Yin (1994) notes that it is difficult to generalize from one case to another. In this study, the eight cases have several things in common but also a lot of differences. The universal "recipe" approach to the design and implementation of law enforcement technologies is not supported by this study. Every country is unique, but there are certain common features for comparison. According to Yin, analysts fall into the trap of trying to select a "representative" case or set of cases. Yin advises researchers not to generalize to other case studies but to generalize findings to a theory. Then, the propositions of this research, the multi-use of surveillance data concept, can work as an interoperative theory, guideline or structural reference for improving law enforcement.

4.3.2.4 Reliability

The final test of the quality of the CSR is reliability: If a later researcher followed the same procedure as described by the earlier researcher and conducted the study all over again, would the researcher arrive at the same findings and conclusions? In this study, the reliability is ensured by extensive documentation of the research data and results. Most of the documented evidence (see Table 4) is publicly available via the Internet. Each interview and observation situation is unique, making it impossible to obtain the exact same data with different researchers. The interviews did, however, provide information about the units of analysis that the researcher could interpret in a coherent way. The information gathered from the case studies reached saturation in all three units of analysis (sensors, communication channels and CCI); that is, additional case studies would not have provided any significant new information from the viewpoint of the research objectives.

4.4 Recommendations for future research

The proof-of-concept model designed in this dissertation deserves future designed science research. The scope of DSR should be to develop a requirement specification and interface specification for a complex SIS that integrates criminal investigation, chain-of-custody and monitoring-of-legality. Another important DSR/action research target is to develop a holistic operational procedure from beginning to end that enables the use of the new tools for all these three tasks.

The framework designed within Study VIII does not look at the dependencies between the different IT Services for the multi-supplier service base but rather from a single IT service perspective only. Synergies and/or conflicts between the IT services need to be studied in the multi-supplier service base also. Additionally, it should be investigated how governance practices for traditional outsourcing methodology differ from cloud-sourcing governance methodology where the services are more fixed for multi-tenants, especially in public cloud services.

Study VIII was written from an IT Service strategy perspective looking at the overall picture of IT Services. The methodologies in multi-supplier management in ITIL core processes have not been studied. A multi-supplier operating framework for some of the ITIL main processes, such as change management, incident management and problem management, is important to study to provide organizations with a more practical approach in operational duties. Each organization has its own requirements for IT services. When external suppliers are providing IT services, there might be inflexibility in standard services in the multitenant service base. Suppliers' standard services might not respond to client requirements. The ways organizations could manage the gaps between the suppliers' standard services and clients' requirements are vital to understand and study.

Study IV states that one target of the future monitoring system would be to support broader European goals in recognizing the needs for regulation and harmonization, promoting the use of other European technologies and systems such as Galileo and EUROSUR and creating the interfaces required. By no means are GNSSs everlasting, stable systems: old satellites die, and new systems are launched while international competition in space is going on. In Europe, "smart borders legislation" is under development, and it is creating new challenges to cross-border activities. Registering all people coming into and leaving the Schengen area creates billions of cases. How to track the movement of criminal cases under investigation in the Schengen and its borders? How to exchange information between LEAs of different countries? The SATERISK and MACICO projects started to explore these challenges. Whether EU legislation will tackle these problems remains to be seen. Mature research results might assist the legislators and are welcomed by them.

The results of Study VII will enable us to build new business models answering the question: How can a developed overall solution or a part of it be marketed as a compatible set? The industry's market and volumes and the relationships between international, national and public-private partnerships' regulations in different countries will be examined. One task is to monitor the development of the markets in the EU in that area. The objective is to create scenarios out of the business models to clarify who should be responsible for the integration work and further equipment acquisitions and administration. Within this work, the Finnish model is being developed and documented as a basis for creating RFQ documents. Development in the EU is contingent on the European surveillance system, EUROSUR, forming in the future a part of the EU's wider Common Information Sharing Environment (CISE), under which information may be shared with a whole range of third actors, including police agencies and defense forces. This development will have effects on the future mobile and vehicular systems that LEAs will be using in their everyday duties.

To bring new technologies into covert operations, a lot of further technological and socio-technical research and development work is needed. This research should go beyond the SE and DSR principles, because, for example, cultural effects are prominent, and other methodologies such as the critical research bricolage should be applied.

YHTEENVETO (FINNISH SUMMARY)

Lukuisten elektronisten seurantalaitteiden hallinta monissa yhtäaikaisissa rikostutkinnoissa on osoittautunut vaativaksi tehtäväksi lainvalvontaviranomaisille. Ongelmat ovat poikineet useita oikeusjuttuja sekä julkisuutta, joka ei ole lisännyt kansalaisten luottamusta oikeusvaltioon. Osallistuvan havainnoinnin keinoin on voitu todentaa, että poliisiorganisaatioilla on tendenssiä luoda kahden tason järjestelmiä: yhdet toimintaan kadulla ja toiset asian esittämiseen oikeudelle; joissakin Euroopan maissa tällainen kehitys on yllättävän pitkällä. EU:n kaikessa hallinnossa korostetaan läpinäkyvyyden merkitystä, kuitenkin viranomaiset keskittyvät edelleen vain tiedon hankintaan sen sijaan, että pyrittäisiin tekemään käytetyistä prosesseista läpinäkyviä. Yksityisyyden suojan vuoksi poliisin tiedonhankinta ei voi olla julkista, mutta se voi olla niin läpinäkyvää että kansalaisten kritiikin ja kontrollin on mahdollista toteutua valtiovallan suhteen.

Tämän väitöstutkimuksen tavoitteena on (a) syventää ymmärrystä siitä, miten satelliitteihin pohjautuvilla paikannuslaitteilla, mobileilla valvonta-asemilla ja näiden tarvitsemilla tiedonsiirtoyhteyksillä voidaan parantaa lainvalvontaa sekä (b) kehittää malli/tavoitetila tällaisesta kompleksisesta ohjelmistointensiivisestä järjestelmästä. Tässä laadullisessa tutkimuksessa on sovellettu suunnittelutieteellistä viitekehystä, jossa tavoitetilan määrittely on toteutettu usean tapauksen tapaustutkimuksella. Tutkimuksen pohjana ovat neljän Tekesin rahoittaman tutkimushankkeen tutkimusaineistot sekä -tulokset tarkasteltuna lainvalvonnan näkökulmasta. Väitöstutkimuksen mukaan seurantalaitteiden käytön suurimmat ongelmat ovat: (1) saatavilla olevat sensorit eivät täytä lainvalvontaviranomaisten vaatimuksia; mm. toiminta-aika ja piilotettavuus (koko), (2) rajat ylittävä toiminta; organisoitunut rikollisuus on kansainvälistä, kun taas lainvalvontaviranomaiset ovat kansallisia organisaatioita, (3) järjestelmien tarvitsemat tietoturvalliset tietoliikenneyhteydet eivät ole riittävät, (4) ei ole ratkaistu, miten kerättävä data täyttää digitaalisen todisteaineiston vaatimukset oikeudessa sekä (5) laillisuusvalvonnan toteuttaminen on puutteellista. Lisäksi on huomioitava nykyinen taloudellinen tilanne, jossa lainvalvonnan resurssit eivät ainakaan lisäänny. Tämä tarkoittaa että uusilla järjestelmillä tulee olla pitkä käyttöikä ja että vanhoja laitteita on voitava kytkeä niihin.

Hyödyntämällä tekoälyä sensoreiden toimintaa voidaan parantaa monella tavoin sekä niiden energiankulutusta pienentää; koska akku on sensoreiden suurin komponentti, tällöin myös sensoreiden kokoa voidaan pienentää toiminta-ajan siitä kärsimättä. Nykyiset tekniset ja operatiiviset järjestelmät eivät tue lainvalvojien rajat ylittäviä operaatioita, kuitenkin teknisistä puutteista huolimatta suurimman ongelman muodostaa eri organisaatioiden välinen luottamuspula. Lainvalvonnan tarvitsemat tulevaisuuden kyber-turvalliset tietoliikenneyhteydet kannattaa toteuttaa hajautetulla arkkitehtuurilla hyödyntäen useita rinnakkaisia teknologioita ja reittejä, mutta yhteensopivasti tai jopa yhdessä muiden turvallisuuskriittistä tietoliikennettä tarvitsevien tahojen kanssa, kuten palo ja pelastus, armeija ja kriittisen infrastruktuurin turvaajat. Nykyisen tekniikan avulla on mahdollista luoda tietojärjestelmä, johon voidaan kerää rikosten selvittämiseen käytettävä data niin että se täyttää digitaalisen todistusaineiston vaatimukset. Tähän kompleksiseen ohjelmistointensiiviseen järjestelmään voidaan yhdistää laillisuusvalvonnan mahdollistavat toiminteet.

Viranomaisten ajoneuvoihin on vuosikymmenten kuluessa lisätty kymmenittäin erillisiä teknisiä laitteistoja, jotka vaativat huomattavasti tilaa ja joilla on omat käyttöliittymänsä ajoneuvon ohjaamossa. Tämä on johtanut ajoittaisiin toiminnallisuusongelmiin (esimerkiksi turvatyynyn toimintatilan supistuminen) ja teknisiin ongelmiin sähkönsaannissa ja kaapeloinneissa. Monet laitteistot olisikin järkevää yhdistää yhdeksi fyysiseksi tai ainakin toiminnalliseksi kokonaisuudeksi, jonka käyttöliittymänä toimisi yleinen kenttäjohtojärjestelmä. Lainvalvontaviranomaisten osalta on käynnissä kehityssuunta, jossa toimistossa istumista vähennetään ja kentällä oloa lisätään. Tällöin myös rikosteknisten järjestelmien mobiilit ohjaus- ja valvontatarpeet lisääntyvät. Myös näiden uusien järjestelmien ohjaus- ja valvontafunktiot tulisi integroida yleiseen kenttäjohtojärjestelmään. Koska nykyiset tietojärjestelmät toimivat monitoimittaja-ympäristössä, vaaditaan viranomaisilta uudenlaista hankinta- ja ylläpito-osaamista.

Tämän väitöstutkimuksen johtopäätöksenä todetaan, että rikosten torjuntaa voidaan huomattavasti tehostaa yhdistämällä lainvalvontaviranomaisten teknisen tarkkailun tietojärjestelmät, tuomioistuinten digitaalisten todistusaineistojen käsittelyn tietojärjestelmät sekä laillisuusvalvontaorganisaatioiden tietojärjestelmät yhdeksi toiminnalliseksi ohjelmistointensiiviseksi järjestelmäksi. Jatkotutkimuskohteena tulisi kehittää laillisuusvalvontaohjelmiston vaatimusmääritykset sekä rajapinta, joka yhdistää laillisuusvalvonnan järjestelmän olemassa oleviin rikollisuuden teknisen seurannan tuotteisiin. Toisena tärkeänä jatkotutkimuskohteena olisi luoda näiden välineiden käyttöön alusta loppuun laillisuusvalvonnan mahdollistava käyttöprosessi. Käytännössä tämä tarkoittaisi, että tekniseen tarkkailuun ei tulevaisuudessa enää rakennettaisi ja käytetäisi yksittäisiä laitteita, joiden tuottamasta tiedosta vain jotain osaa käytettäisiin oikeudessa. Sen sijaan luotaisiin kokonaisjärjestelmä, joka synnyttäisi auditoitavan lokin prosessin jokaisesta vaiheesta. Tämä parantaisi lainvalvontaprosessien läpinäkyvyyttä vaikka tekninen tarkkailu lisääntyisi.

REFERENCES

Aanestad, M. & Jensen, T. B. 2011. Building nation-wide information infrastructures in healthcare through modular implementation strategies. The Journal of Strategic Information Systems 20 (2), 161-176.

ABI Research 2011. High Precision GNSS Market Set to Increase Almost 100% by 2016.

Akella, R., Tang, H. & McMillin, B. M. 2010. Analysis of information flow security in cyber–physical systems. International Journal of Critical Infrastructure Protection 3 (3), 157-173.

Ameyugo, G., Art, M., Esteves, A. S. & Piskorski, J. 2012. Creation of an EU-Level Information Exchange Network in the Domain of Border Security. European Intelligence and Security Informatics Conference (EISIC), 356-358.

Andreas, P. 2013. Smuggler nation: How illicit trade made America. Oxford University Press.

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.

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

BBC News 2013. Cybercriminals 'drained ATMs' in $45m world bank heist. (9. May edition) BBC News US & Canada,.

BBC News US & Canada 2013. Cybercriminals 'drained ATMs' in $45m world bank heist. Available in: http://www.bbc.co.uk/news/world-us-canada-22470299. Accessed: Dec 19, 2013.

Benbasat, I., Goldstein, D. K. & Mead, M. 1987. The case research strategy in studies of information systems. MIS Quarterly 11 (3), 369-386.

Benson, Y. 2011. *Authority IT serving national security*, VIRVE Day -seminar.

Betts, S. C. 2011. Contingency Theory: Science Or Technology? Journal of Business & Economics Research (JBER) 1 (8).

Bolkcom, C. 2004. Homeland security: Unmanned aerial vehicles and border surveillance. DTIC Document.

Brady, M. 2000. Use of entity or relationship diagramming as a technique in the grounded theory approach to social science research. In proceedings of the Irish Academy of Management Annual Conference.

Brannen, J. 2004. Working qualitatively and quantitatively. In C. Seale, G. Gobo, J. F. Gubrium & D. Silverman (Eds.) Qualitative Research Practice.London: Sage Publications, 312-326.

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

Carty, A. 2006. A Practical Guide to PPP in Europe. City & Financial .

Casey, E. 2011. Digital evidence and computer crime: Forensic science, computers, and the internet. Access Online via Elsevier.

Coenen, T. L. 2009. Expert fraud investigation: a step-by-step guide. Wiley.com.

Corbin, J. & Strauss, A. 2008. Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Saga Publications.

Coudert, F. 2010. When video cameras watch and screen: Privacy implications of pattern recognition technologies. Computer Law & Security Review 26 (4), 377-384.

Council of the European Union 2012. Results of the ENLETS meeting held on the 18-19 September 2012 in Cyprus. DG D 2C 16004/12. Brussels.

Daniel, L. E. 2011. Digital forensics for legal professionals: understanding digital evidence from the warrant to the courtroom. Access Online via Elsevier.

Drazin, R. & Van de Ven, Andrew H 1985. Alternative forms of fit in contingency theory. Administrative Science Quarterly , 514-539.

Driessen, B. 2012. Eavesdropping on Satellite Telecommunication Systems. IACR Cryptology ePrint Archive 2012, 51.

Echaore-McDavid, S. & McDavid, R. A. 2009. Career Opportunities in Forensic Science. Infobase Publishing.

Edwards, L. 2011. New 4G network could cause widespread GPS dead zones. Available in: http://phys.org/news/2011-02-4g-network-widespread-gps-dead.html. Accessed: Aug 12, 2014.

Edwards, P. N., Bowker, G. C., Jackson, S. J. & Williams, R. 2009. Introduction: an agenda for infrastructure studies. Journal of the Association for Information Systems 10 (5), 364-374.

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

El-Bakry, H. M. & Mastorakis, N. 2009. Design of anti-GPS for reasons of security. CIS 9, 480-500.

El-Haram, M. A., Marenjak, S. & Horner, M. W. 2002. Development of a generic framework for collecting whole life cost data for the building industry. Journal of Quality in Maintenance Engineering 8 (2), 144-151.

Elvy, D. 2011. Terrorism, Threat and Time: The Mediating Effect of Terrorist Threat on Public Willingness to Forego Civil Liberties. European Intelligence and Security Informatics Conference (EISIC), 52-57.

Erling, T. 2012. Preface–Technology Develops Taking International Cooperation to New Level. In J. Rajamäki, R. Pirinen & J. Knuuttila (Eds.) SATERISK - Risks of Satellite Based Tracking.Vantaa: Laurea University of Applied Sciences, 7-8.

European Commission 2013a. Communication from the Commission to the European Parliament and the Council: Second Report on the implementation of the EU Internal Security Strategy.

European Commission 2013b. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace COM(2013)48 final.

European Commission 2012. Work Programme 2013., Cooperation, Theme10, Security. (C (2012)4536 edition) European Commission.

European Commission 2011. Horizon 2020: Commission proposes €80 billion investment in research and innovation, to boost growth and jobs. Available in: http://europa.eu/rapid/press-release_IP-11-1475_en.htm. Accessed: 4 Dec. 2013.

European Commission 2009. GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, COM(2009) 624 final. Brussels: Commission of the European Communities.

Fiadeiro, J. L. 2007. Designing for software's social complexity. IEEE Computer 40 (1), 34-39.

Fox, V. 2013. How Do Banks Handle Credit Card Fraud? Available in: http://smallbusiness.chron.com/banks-handle-credit-card-fraud-12537.html. Accessed: Dec 20, 2013.

Frost & Sullivan 2010. Satellite phone comparison Iridium and Inmarsat.

Fuller, S. & Petersen, S. 1996. Life-cycle costing manual for the federal energy management program, 1995 Edition. NIST handbook 135.

Gallivan, M. J. & Wonseok Oh 1999. Analyzing IT outsourcing relationships as alliances among multiple clients and vendors. Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences (HICSS-32).

George, A. L. & Bennett, A. 2005. Case studies and theory development in the social sciences. Massachusetts: MIT Press.

George, R. 2008. Critical infrastructure protection. International Journal of Critical Infrastructure Protection 1, 4-5.

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

Goldstein, M. L. 2012. Emergency Communications: Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network. United States Government Accountability Office GAO-12-343. Washington, D.C.

Guinness, R., Pitsinki, H. & Penttinen, J. 2012. 3 Technical Risks. Risks of Satellite-Based Tracking. In J. Rajamäki, R. Pirinen & J. Knuuttila (Eds.) SATERISK - Risks of Satellite Based Tracking.Vantaa: Laurea University of Applied Sciences.

Gummesson, E. 2000. Qualitative methods in management research. Sage.

Haack, S. 1976. The pragmatist theory of truth. British Journal for the Philosophy of Science , 231-249.

Haddock, P. C., Hatley, J. W., Morse, W. D. & Tooley, R. D. 2012. Integrated communications and navigation module. IEEE International Carnahan Conference on Security Technology (ICCST).

Hallinan, D., Friedewald, M. & McCarthy, P. 2012. Citizens' perceptions of data protection and privacy in Europe. Computer Law & Security Review 28 (3), 263-272.

Hanseth, O. 2002. From systems and tools to networks and infrastructures-from design to cultivation. Towards a theory of ICT solutions and its design methodology implications. Unpublished manuscript .

Hanseth, O. & Lyytinen, K. 2010. Design theory for dynamic complexity in information infrastructures: the case of building internet. Journal of Information Technology 25 (1), 1-19.

Happonen, M. 2010. Recognising Risks Of Satellite-based Tracking.

Happonen, M., Viitanen, J., Kokkonen, P., Ojala, J. & Rajamäki, J. 2009. Jamming detection in the future navigation and tracking systems. Proc. 16th Saint Petersburg International Conference of Integrated Navigation Systems, 314-317.

Haskins, C., Krueger, M., Walden, D. & Hamelin, R. D. 2011. Systems Engineering Handbook: A guide for systems life cycle processes and activities. (v. 3.2.2 edition) San Diego, CA: International Council on Systems Engineering (INCOSE).

Hätönen, S. 2012. Police Field Commanding: The Role and Supportive ICT & Communication System. PSCE Forum Conference.

Herz, T. P., Hamel, F., Uebernickel, F. & Brenner, W. 2011. Mechanisms to implement a global multisourcing strategy. In New Studies in Global IT and Business Service Outsourcing. Springer, 1-20.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design Science Research in Information Systems. MIS Quarterly 28 (1), 75-105.

Hevner, A. & Chatterjee, S. 2010. Design science research in information systems. Springer.

Holland, J. 1996. Hidden order: how adaptation builds complexity. Redwood City, CA: Addison Wesley Longman Publishing Co., Inc.,.

Holmström, J., Rajamäki, J. & Hult, T. 2011. The future solution and technologies of public safety communications–DSiP traffic engineering solution for secure multichannel communication. International Journal of Communication (3), 155-122.

ICD, O. 2010. European GNSS (Galileo) open service.Signal in space.Interface control document.Issue 1.1 .

Ilander, T., Toivonen, H., Meriheinä, U. & Garlacz, J. 2010. Indoor Positioning for Nuclear Security. Proceedings of Third European IRPA Congress.

Jackson, J., Hough, M., Bradford, B., Pooler, T., Hohl, K. & Kuha, J. 2011. Trust in justice: topline results from round 5 of the European Social Survey.

Jahyun Goo & Kichan Nam 2007. Contract as a Source of Trust--Commitment in Successful IT Outsourcing Relationship: An Empirical Study. HICSS 40th Annual Hawaii International Conference on System Sciences, 239a.

Kämppi, P. & Guinness, R. 2010. Technical Risk Analysis for Satellite Based Tracking Systems. Integrated Communications, Navigation and Surveillance conference, M3-1.

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

Kaplan, E. D. & Hegarty, C. J. 2005. Understanding GPS: principles and applications. Artech house.

Kincheloe, J. L., McLaren, P. & Steinberg, S. R. 2011. Critical pedagogy and qualitative research. The Sage handbook of qualitative research , 163-177.

Kinzig, B. 2010. Global Hawk Systems Engineering: Case Study. Issue 1115. Virginia.

Kivimäki, A. 2007. Wireless telecommunication standardization processes : actors' viewpoint. Oulu: Oulun yliopiston kirjasto. Acta Universitatis Ouluensis.

Klinker, F. & Pietersen, O. 2000. Interference of GPS signals: Influence of Licensed Transmitters on the GPS Signal Quality in the Netherlands' Airspace. National Aerospace Laboratory NLR.

Kokkonen, P. 2010. Paikannus merellä lain ja tekniikan näkökulmista. Master thesis. Theseus. Espoo:Laurea.

Kosta, E., Dumortier, J., Graux, H., Tirtea, R. & Ikonomou, D. 2012. Study on data collection and storage in the EU. European Network and Information Security Agency (ENISA) Deliverable – 2012-02-08.

Lacity, M., Willcocks, L. & Feeny, D. F. 1966. The value of selective IT sourcing. MIT Sloan Management review.

Laine, M., Bamberg, J. & Jokinen, P. 2007. Tapaustutkimuksen taito. Helsinki: Helsinki University Press.

Laitinen, I. 2011. Role of Border Control in the new EU security architecture and an update on Frontex activities. Situation Scope seminar.

Lapierre, G. 2011. Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU? (Presentation in PSC Europe Conference edition) Brussels: PSCE.

Lawrence, P. R., Lorsch, J. W. & Garrison, J. S. 1967. Organization and environment: Managing differentiation and integration. Division of Research, Graduate School of Business Administration, Harvard University Boston, MA.

Lee, D. 2012. AA to launch sat-nav tech tracked insurance policy.

Lehti, M., Pursiainen, H., Volanen, R., Luoma, R., Timonen, P., Hagman, R. & Kanane, I. 2009. Promoting the availability of secure telecommunications networks. Helsinki.

Lehto, J., Rajamäki, J. & Rathod, P. 2012. Cloud computing with SOA approach as part of the disaster recovery and response in Finland. International Journal of Computers and Communications 6 (1), 175-182.

Leroux, O. 2004. Legal admissibility of electronic evidence 1. International Review of Law, Computers & Technology 18 (2), 193-220.

Lincoln, Y. S. & Guba, E. G. 1985. Naturalistic inquiry. Beverly Hills: Sage Publication.

Locke, L. F., Spirduso, W. W. & Silverman, S. J. 2007. Proposals that work: A guide for planning dissertations and grand proposals (5th edition) Thousand Oaks: Sage Publications.

Mager, B. 2004. Service design: A review. Köln International School of Design.

Mannermaa, M. 2008. Jokuveli: elämä ja vaikuttaminen ubiikkiyhteiskunnassa. WSOYpro.

Manni, K. 2011. Security communications – possibilities and challenges. VIRVE Day -seminar.

Manning, G. A. & CFE, E. 2010. Financial investigation and forensic accounting. CRC Press.

Manning, P. K. & Van Maanen, J. 1978. Policing: A view from the street. Goodyear Publishing Company Chicago, IL.

Markus, M. L., Majchrzak, A. & Gasser, L. 2002. A Design Theory for Systems That Support Emergent Knowledge Processes. Mis Quarterly 26 (3).

Marques, F. T., Sauve, J. P. & Moura, A. 2007. Service Level Agreement Design and Service Provisioning for Outsourced Services. Network Operations and Management Symposium, 2007. LANOMS 2007. Latin American, 106.

Marttila, J., Heikura, P. & Käyhkö, E. 2013. Poliisibarometri 2012 Sisäasiainministeriön Julkaisuja 47/2012. Helsinki.

Merriam, S. B. 1998. Qualitative research and case study applications in education.

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

Monteiro, E. & Hanseth, O. 1996. Social shaping of information infrastructure: on being specific about the technology. Information technology and changes in organizational work, 325-343.

Niemi, J. & de Godzinsky, V. 2009. Telecommunications Surveillance and Legal Protection in Finland. National Institute for Legal Policy. Tech. Rep. 243.

Nordman, M., Lehtonen, M., Holmström, J., Ramstedt, K. & Hämäläinen, P. 2003. A TCP/IP based communication architecture for distribution network operation and control. Proceedings, 17th International Conference on Electricity Distribution (CIRED), Barcelona.

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.

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).

Ojala, J. 2010. Technical tracking as covert coercive measure for police to collect information. Master thesis. Vantaa: Laurea University of Applied Sciences.

Ojasalo, J., Turunen, T. & Sihvonen, H. 2009. Responsibility and decision making transfer in public safety and security emergencies - A case study of school shootings. IEEE Conference on Technologies for Homeland Security, 358-365.

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.

Paajanen, R., Kuosmanen, P., Talvitie, J. & Juopperi, J. 2013. Digital services – The next boom. (White paper edition) Helsinki: Tieto- ja viestintäteollisuuden tutkimus TIVIT Oy.

Padding, P. 2013. Security and Safety. ENLETS. Conference on Innovation Procurement. Kraków: European Commission.

Parkinson, P. 2010. Conference plenary, Never Lost Again. 61st International Astronautical Congress, Prague, Czech Republic.

Patrascu, A. C. 2007. Optimizing distributed sensor placement for border patrol interdiction using microsoft excel.

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

Pelhe, A., Kozomora, N., Kun, A. L. & Miller, W. T. 2004. Distributed components in the Project54 system. Proceedings of the winter international synposium on Information and communication technologies. Trinity College Dublin, 1.

Petersen, R. R. & Wiil, U. K. 2011. CrimeFighter Investigator: A Novel Tool for Criminal Network Investigation. European Intelligence and Security Informatics Conference (EISIC), 197-202.

Pickett, K. S. & Pickett, J. M. 2002. Financial crime investigation and control. Wiley. com.

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.

Pirinen, R., Rajamäki, J. & Aunimo, L. 2008. Rescuing of Intelligence and Electronic Security Core Applications (RIESCA). WSEAS Transactions on Systems 7 (10), 1080-1091.

Popper, K. 2009. Conjectures and Refutations: The growth of scientific knowledge. London: Routledge Classics.

Pyster, A. & Olwell, D. H. 2013. The Guide to the Systems Engineering Body of Knowledge (SEBoK). (v. 1.1.2 edition) Hoboken, NJ: The Trustees of the Stevens Institute of Technology.

Rajamäki, J., Pirinen, R. & Knuuttila, J. (Eds.) 2012. SATERISK - Risks of Satellite-Based Tracking: Sample of Evidence Series. Vantaa: Laurea-University of Applied Sciences, Leppävaara Unit.

Rajamäki, J. & Viitanen, J. 2013. Law enforcement authorities' special requirements for GNSS. Proceedings of the 6th GNSS Vulnerabilities and Solutions Conference., 135-146.

Rajamäki, J., Knuuttila, J., Suni, O., Silanen, H., Tuomola, A. & Meros, P. 2014a. 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., Timonen, T., Nevalainen, J., Uusipaavalniemi, H., Töyrylä, T. & Arte, E. 2014b. Human-machine Interactions in Future Police Vehicles: Applying Speech User Interface and RFID Technology. International Journal of Systems Applications, Engineering & Development 8, 163-170.

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), 1-8.

Rajamäki, J., Tervahartiala, J., Tervola, S., Johansson, S., Ovaska, L. & Rathod, P. 2012. How Transparency Improves the Control of Law Enforcement Authorities' Activities? European Intelligence and Security Informatics Conference (EISIC), 14-21..

Rajamäki, J., Rathod, P. & Kämppi, P. 2013. A New Redundant Tracking System for Emergency Response. European Intelligence and Security Informatics Conference (EISIC), 218.

Ramakrishnan, M. & Pro, V. M. 2008. IT Program Governance in Multi-vendor Outsourcing. SETLabs Briefings 6 (3), 19.

Rathod, P. & Kämppi, P. 2013. User requirements specification: MOBI work package 2 (version 1.0, May edition) Vantaa: Laurea University of Applied Sciences.

Reivo, J., Vuoripuro, J. & Pelkonen, N. 2010. Communication and security management cooperation in large events - Case: IAAF World Chanpionships 2005 in Helsinki. In R. Pirinen & J. Rajamäki (Eds.) Integrative student-centred research and development work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA).Vantaa: Laurea Publications, 119-136.

Riippa, H. 2012. Procurement at the Finnish Police. Tekes Safety and Security Programme's Annu. Seminar.

Riippa, H. 2011. The future of PPDR networks in Finland – Requirements and options.

Roan, J. 2011. Battery tech improving as demand soars.

Robbin, A. 2001. The loss of personal privacy and its consequences for social research. Journal of Government Information 28 (5), 493-527.

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

Ross, J. W. & Westerman, G. 2004. Preparing for utility computing: The role of IT architecture and relationship management. IBM Systems Journal 43 (1), 5-19.

Ruoslahti, H., Guinness, R. & Viitanen, J. 2010. Airborne Security Information Acquisition Using Micro Air Vehicles: Helping Public Safety Professionals Build Real-Time Situational Awareness HICSS.

Samuel, A. L. 1959. Some Studies in Machine Learning Using the Game of Checkers. IBM Journal of Research and Development 3 (3), 210-229.

Sauser, B., Verma, D., Ramirez-Marquez, J. & Gove, R. 2006. From TRL to SRL: The concept of systems readiness levels. Conference on Systems Engineering Research, Los Angeles, CA.

Shiyue Fan, Lijun Zhao, Wenjun Xiao & Zhenghang Li 2012. Performance analysis and simulation of Iridium navigation satellite based on STK. Second International Workshop on Earth Observation and Remote Sensing Applications (EORSA), 291-295.

Shostack, G. L. 1982. How to design a service. European Journal of Marketing 16 (1), 49-63.

Simon, H. 1978. The science of the artificial. Cambridge: MIT Press.

Smith, A. 2011. Law Enforcement Use of Global Positioning (GPS) Devices to Monitor Motor Vehicles: Fourth Amendment Considerations. R41663.

Snyder, J. & Mattingly, P. 2013. *U.S* Lawmakers Warns for Security Threats from Cyberattacks. Bloomberg Technology.

Sprague, R. 2008. Orwell was an Optimist: the Evolution of Privacy in the United States and its De-evolution for American Employees. John Marshall Law Review 42, 83-134.

Srimoolanathan, B. 2012. World Security Market Outlook Tekes Safety and Security Programme's annual semina. Helsinki: Tekes.

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

Star, S. L. & Ruhleder, K. 1996. Steps toward an ecology of infrastructure: Design and access for large information spaces. Information systems research 7 (1), 111-134.

Stigell, P. 2012. Preface–GNSS; from Security Applications to Secure Evereday Use. In J. Rajamäki, R. Pirinen & J. Knuuttila (Eds.) SATERISK - Risks of Satellite Based Tracking.Vantaa: Laurea University of Applied Sciences, 9-12.

Sun, Z., Wang, P., Vuran, M. C., Al-Rodhaan, M. A., Al-Dhelaan, A. M. & Akyildiz, I. F. 2011. BorderSense: Border patrol through advanced wireless sensor networks. Ad Hoc Networks 9 (3), 468-477.

Syrjänen, K. 2010. Information Technology (IT) perspective on Maturity Modelling and Continuity Management: an Action and Design Research. In R. Pirinen & J. Rajamäki (Eds.) Integrative student-centred research and development work: Rescuing of Intelligence and Electronic Security Core Applications (RIESCA).Vantaa: Laurea Publications, 68-111.

The Gallup Organization 2008. Data Protection in the European Union: Citizens' perceptions. Flash Eurobarometer Series 225. European Commission.

The Information Technology Infrastructure Library 2007. ITIL v.3 Service Design.

Tikanmäki, I., Rajamäki, J. & Pirinen, R. (Eds.) 2014. Mobile Object Bus Interaction - Designing future emergency vehicles. Vantaa: Laurea.

Tuohimaa, T., Tikanmäki, I., Rajamäki, J., Viitanen, J., Patama, P., Knuuttila, J. & Ruoslahti, H. 2011. Is Big Brother Watching You? International Journal of Systems Engineering, Applications and Development 5 (5), 602-609.

U.S. Department of the Treasury 2011. Terrorist Finance Tracking Program (TFTP). Available in: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx. Accessed: Dec 19, 2013.

Van Haren Publishing 2007. IT service management: an introduction. Van Haren Publishing.

Viikari, L. (Ed.) 2011. SATERISK: Tutkimusraportti 2008-2011. Rovaniemi: Lapin yliopistopaino.

Viitanen, J., Happonen, M., Patama, P. & Rajamäki, J. 2010a. Near border procedures for tracking information. WSEAS Transactions on Systems 9 (3), 223-232.

Viitanen, J., Patama, P., Knuuttila, J., Rajamäki, J. & Ruoslahti, H. 2010b. Is there a choice for Big Brother. Presented at The 12th annual Conference of the Finland Futures Research Centre and the Finland Futures Academy: Security in Futures - Security in Change. Turku, Finland.

Viitanen, J., Patama, P., Rajamäki, J., Knuuttila, J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. 2012. How to create oversight in intelligence surveillance. Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE'11) , 52-56.

Walsham, G. 2006. Doing interpretive research. European Journal of Information Systems 15, 320-330.

Wardley, S. 2009. Cloud Computing-Why IT Matters. OSCON (Open Source Convention).

Waterman, S. 2007. UAV tested For US border security Washington: UPI.

Wernick, M. N., Yongyi Yang, Brankov, J. G., Yourganov, G. & Strother, S. C. 2010. Machine Learning in Medical Imaging. Signal Processing Magazine, IEEE 27 (4), 25-38.

WIMAX Forum 2011. WiMAX™ on Track to Cover One Billion by EOY 2011.

Winter, R. 2010. Interview with Jay F. Nunamaker, Jr. on "Toward a broader vision of IS research". Business & Information Systems Engineering 2 (5), 321-329.

Wood, D. M., Ball, K., Lyon, D., Norris, C. & Raab, C. 2006. A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network.

Yates, P. 2012. Successfully manage multiple suppliers: Achieve effective IT service delivery. (Rev. 3 edition) Hewlett-Packard Development Company.

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

Yin, R. K. 1994. Case Study Research, Design and Method. (2nd edition) Thousand Oaks: Sage Publications.

APPENDIX A. RESEARCH AND DEVELOPMENT PROJECTS

THE RIESCA PROJECT

The RIESCA (Rescuing of Intelligence and Electronic Security Core Applications) project was a Tekes (Finnish Funding Agency for Technology and Innovation) Safety and Security Programme-funded project, which began on October 1st, 2007 and ended on March 31st, 2010. The RIESCA project's focus areas were on the following Tekes Safety and Security Programme points: (1) National safety and security covers items in the defense, border guard, police, first response and firefighting as well as customs operations, and (2) Industrial safety and security deals with the full agenda of corporate needs and particular solutions.

Finnish society is highly dependent on the various critical information systems that support society. Business secrets, patient records and the credit card data of citizens, to name but a few, are kept in electronic form, and it is obviously important that such information is kept confidential and protected from unauthorized access. Therefore, information systems and software applications should function in the correct way even in cases of attempted hacking or human error. Successful hacking or even coffee spilt on a computer may result in a system not functioning as required (Pirinen & Rajamäki 2010).

There are a number of systems, such as transportation, water, power, financing and law enforcement, which are critical for the functioning of society in Finland. When assessing possible risks, it is only seldom taken into account that, for example, law enforcement is critically dependent on the reliability and security of information systems. Information security is often enhanced by technical solutions without any systematic planning and knowledge of how to protect the different segments of the system. Here, the risk is not only the investing of information security resources in the wrong targets but that the unplanned integration of systems and the related information security components may even create new security risks. In consequence, systems that are critical for society may not work as they should.

The RIESCA project aimed to solve this problem. The research project developed information security management techniques that can be used to ensure the proper functioning of critical systems in all circumstances. The research partners in the project were the University of Oulu, the University of Eastern Finland and the Laurea University of Applied Sciences. The project's budget was over 950.000 EUR from 2007 to 2010.

The work package of Laurea aimed at developing further evaluation methods of systems that were critical for the functioning of the society. To reach this aim, there was an analysis of the methods that evaluate these systems' continual development (Pirinen, Rajamäki & Aunimo 2008) and maturity-based continuity management (Syrjänen 2010). Particular attention was paid to the situation of moving from normality to a crisis situation and recovering from the crisis to a normal state. The other aim was to develop different security management and communication systems for critical events, including mass events (Reivo, Vuoripuro & Pelkonen

2010), high-level political meetings (Ilander et al. 2010) and crisis situations (Ojasalo, Turunen & Sihvonen 2009), and to assess methods for evaluating their functionality.

THE SATERISK PROJECT

The SATERISK (SATEllite-based tracking RISKs) project (started 9/1/2008, ended 12/31/2011) studied risks associated with satellite-based tracking, specifically whether the use of tracking generates additional risks (Rajamäki, Pirinen & Knuuttila 2012). The project, led by the Laurea University of Applied Sciences, had partners and other participants from the whole value-chain of satellite-based tracking, from network operators to companies that offer information-gathering devices and tracking software and, finally, to the users, such as the police and customs, of these tracking systems. The project analyzed risks by applying different approaches: legal, technical and operational and how the tracking is used. Operational risks were widely researched from different points of view as all end-users of tracking devices and systems face some risks when they use tracking. The legal aspects of satellite-based tracking were studied at the University of Lapland in its own SATERISK co-project (Viikari 2011).

The SATERISK project aimed to answer the following questions: Does satellite-based navigation and tracking involve risks? Do we know what the risks are now and what they will be in the future? Often new technologies will present opportunities for increased safety and security—and this is certainly true with satellite-based navigation and tracking—but they can also create new risks. It is important for the technology developers and end-users to clearly understand these risks and take steps to mitigate them. The project aimed at a situation where laws on positioning and tracking allow the use of machine to machine (M2M) tracking devices across state and union borders. The project aimed to bring new know-how at the international level to the European security field. The project created new methods and development paths for positioning and tracking systems. The widely used US-based Global Positioning System (GPS) and Russian-based Globalnaja navigatsionnaja sputnikovaja sistema (GLOSNASS) satellite positioning systems will soon get an EU counterpart and rival from Galileo. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. The SATERISK project also offered technological solutions to issues that arose while the project was under way.

SATERISK also aimed to bring new know-how to the safety and security field in Europe. The project created new methods and development paths for positioning and tracking systems that address the risks and limitations that have been discovered. These methods related to information security, signal interference and legal restrictions on tracking. Amongst safety and security professionals—both in the public and private sectors—where the risks could be high if they were not properly addressed—a special emphasis has been placed on the use of satellite-based tracking.

THE MOBI PROJECT

LEAs ought to have forensics technology for investigations and field work in their vehicles. These kinds of technologies include advanced GNSS-based tracking systems to track criminals and vehicles that have been tagged.

The recent ICT development has brought much new technical equipment and many new digital services into LEA vehicles. All this has produced entirely novel problems with the sufficiency of power supply, ergonomics, cabling routes, electromagnetic compatibility and the functioning of vehicles' safety devices, such as air bags. Documentation of applied solutions varies, and standards are lacking. Particularly, standardization is needed because of the diversity of the equipment suppliers.

Figure 23 shows what kinds of research and development activities are ongoing in Finland with regard to emergency response vehicles (ERVs). When looking at 'technology push' side, the Finnish research coalition includes two enterprise projects. An enterprise project, led by Insta DefSec Ltd., developed secured software services. The project utilized the results of the related research project and aimed to develop product concepts that have potential in both domestic and export markets. Additionally, Insta DefSec Ltd. will further develop its business model in order to be able to utilize the growth potential of their product concepts. The project started in June 2010 and ended in December 2012 [24]. Another enterprise project, led by Cassidian Finland Ltd., implements a vehicle-installed professional mobile radio (PMR) concept for law enforcement and for fire and rescue operations. The project started in January 2010 and ended in May 2013 [25]. When looking at market pull, the end-user and customer side, the Police Technical Center is leading a pre-commercial procurement project (the PARVI project) for a new type of a law-enforcement patrol car (Riippa 2012). The Ministry of the Interior's ICT Agency HALTIK and the National Police Board are developing a common Field Command System for all public safety actors. This KEJO project started in January 2013 and will end in December 2016 [26].

The objective of the MOBI project (Mobile Object Bus Interaction, http://mobi.laurea.fi, duration: September 2010–March 2014) is to enhance information and communication technology (ICT) integration of ERVs and create a base for ERVs' ICT concept suitable for commercializing. It will address the above issues through a user-centered program of research that will culminate in new recommendations and designs for an integrated platform for use in ERVs. The MOBI research project generates research data for enterprise and governmental projects by researching and documenting the needs and requirements of the users, power generation and supply and specifying the existing solutions. The MOBI project also equips a demo vehicle.

---

24 (2013, Dec. 3). Secure software services [online]. Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10210602.

25 (2013, Dec. 3). Vehicle installed professional mobile radio concept for law enforcement and fire & rescue operations. [Online]. Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10201742.

26 (2013, Dec. 3). Projektipäällikkö – Kejo-hanke (Project Manager – Kejo Project). [Online]. Available: http://www.poliisi.fi/poliisi/bulletin.nsf/PFC/ 6FA46AF5EF825F98C2257AF3

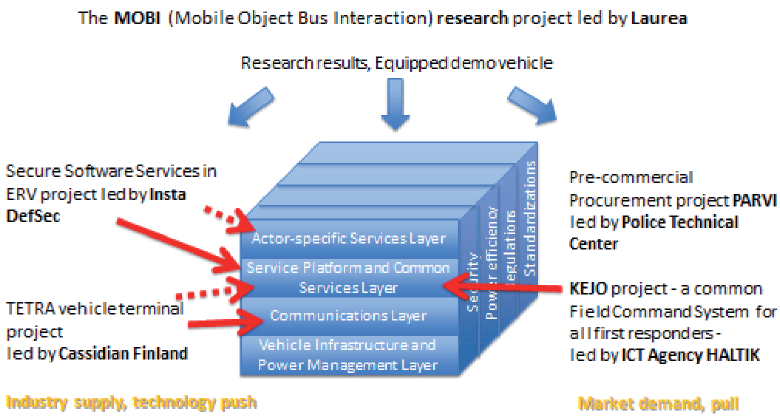


FIGURE 23 Finnish ERV-related R&D projects

THE MACICO PROJECT

The MACICO project (Multi-Agency Cooperation In Cross-border Operations, http://macico.com, duration: Dec 2011 – Dec 2014) will develop a concept for the interworking of security organizations in their daily activities (Aro & Rajamäki 2014). It deals with cooperation of security organizations that do not use in their day-to-day job the same public safety communication (PSC) network but in some missions could benefit from a share of their respective infrastructure. In addition, the concept of decentralized fully redundant cyber-secure governmental communications will be developed. Some use cases, such as the pursuit of criminals across the border or close support for vehicles going through the border, require that security organizations from both countries communicate together and continue to communicate with their control rooms as well. Moreover, cross-border M2M communication is needed between sensors and control systems.

The way to organize this foreign use of a radio network is to be defined and validated by security organizations. The work of the project is carried out in cooperation with public safety authorities, such as LEAs and fire, rescue and emergency medical services. Requirements for these communications are spearheaded by concrete use cases. Interworking at the border will then address the interoperability of different PSC networks and technologies, such as Tetrapol and terrestrial trunked radio (TETRA). From these requirements, the definition of the way to deploy terminals to foreign organizations, the way to organize and to deploy the solutions, including gateways, will be defined in all of the interworking cases. The project addresses not only the interoperability issue, but also the complete procedure that accepts foreign users on a security radio network and looks for a solution that keeps the intrinsic security mechanisms of such networks.

ORIGINAL PAPERS

I

MOBILE COMMUNICATIONS CHALLENGES TO CROSS-BORDER TRACKING OPERATIONS CARRIED OUT BY LAW ENFORCEMENT AUTHORITIES

by

Jyri Rajamäki & Pasi Kämppi, 2013

Proceedings of The International Conference on Information Networking (ICOIN), 2013, 560-565

Mobile Communications Challenges to Cross-border Tracking Operations Carried out by Law Enforcement Authorities

Jyri Rajamäki and Pasi Kämppi
Laurea SID Leppävaara
Laurea University of Applied Sciences
Espoo, Finland
{jyri.rajamaki, pasi.kamppi} @laurea.fi

***Abstract*— Organised crime is a real cross-border threat with the emergence of international warehouses of crime. For improving their evidence-gathering abilities, law enforcement authorities (LEAs) are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organisations. The criminals' counter measure activities, such as electronic counter-surveillance, jamming and constant changes in behaviour for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new intelligent technologies, which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive, is emerging and is a high-priority task. The aim of this study is to provide an improved understanding of the structural characteristics and the dynamic evolution of mobile communication challenges to cross-border satellite-based tracking operations carried out by LEAs. The study is based on the results and lessons learned from the SATERISK research project executed 2008-2011. The study results will be exploited in the ongoing 2.5 years research project Multi-Agency Cooperation In Cross-border Operations (MACICO).**

Keywords- GNSS; law enforcement; law enforcement authorities; technical surveillance; tracking

I. INTRODUCTION

Satellite-based navigation and tracking have become routine features of modern society and everyday life. Their use is still growing—a recent market research report predicts that the Global Navigation Satellite System (GNSS) market will likely double by 2016 [1]. The European Commission launched its first two operational satellites for the Galileo positioning system in October 2011.

The use of satellite-based tracking in a national and international operating environment has been widely studied within the framework of the SATERISK (SATEllite positioning RISKs) project; and a lot of attention has been justifiably and meritoriously devoted to the requirements and risks for the reliability, legal safeguards, data protection and legislation associated with advanced techniques. The SATERISK project aimed to answer the following questions: Does satellite-based navigation and tracking involve risks, especially in cross-border operations? Do we know what the risks are now and what they will be in the future? Often new technologies will present opportunities for increased safety and security—and this is certainly true with satellite-based navigation and tracking—but they can also create new risks. It is important for the technology developers, end-users, and authorities to clearly understand these risks and take steps to mitigate them. The ambitious objective of the project was to create new and better operational models by recognizing the risks, and to support the research and development of positioning branch and hardware and system suppliers. [2], [3].

SATERISK also aimed to bring new know-how to the European field of security. The project created new methods and development paths for positioning and tracking systems that address the risks and limitations that had already been discovered. These include methods related to information security, signal interference, and legal restrictions on tracking. A special emphasis had been placed on the use of satellite-based tracking amongst security professionals in the public sector where the risks could be high if they were not properly addressed. [2], [4].

From time to time, international organized crime organizations have used satellite positioning more effectively than the law enforcement authorities (LEAs), e.g. for the concealment of drug trafficking. Often, effective international activities of LEAs are prevented e.g. by slow communication processes and lack of common regulation. The SATERISK project has proved that the technical preconditions for the improvement of international activities of the authorities exist. A process should be established in the framework of both the World Customs Organization (WCO) and the European Union (EU) and the European Space Agency (ESA) as a result of which LEAs could seamlessly and reliably exchange tracking information of cargoes of special interest. [3].

The MACICO project [15] will develop a concept for interworking of security organizations in their daily activity. It deals with cooperation of security organizations that do not use 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 require security organizations from both countries to communicate together and to continue to communicate with their control room.

II. Challenges to Cross-border Tracking Operations

LEA officers need to have an easier access to all investigation data, independently from place and time and attention has to be paid to public awareness and concern on the use of surveillance equipment. However, cross-border operations are very challenging ones for LEAs, because they are national organizations.

A. *Operational Environment*

Organized crime is a real threat in Europe with the emergence of international warehouses of crime. For improving their evidence-gathering abilities, the law enforcement authorities are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. The criminals' counter measure activities like electronic counter-surveillance, jamming and constant changes in behaviour for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new, harder to detect, more strongly encrypted, longer-lasting and quicker to install and more adaptive intelligent technologies, is emerging and a high priority task. Respecting the accountability and integrity requirements and smooth utilization of data in different phases of chains-of-custody is of utmost importance. In the current situation the chain of custody is difficult to maintain due to different techniques that operate on their own and are connected to different monitoring systems. This makes LEA work very labour-intensive so the use of new state-of-the-art technologies should enable the optimization of the use of human resources. Fig. 1 shows the operational environment where LEAs use tracking.

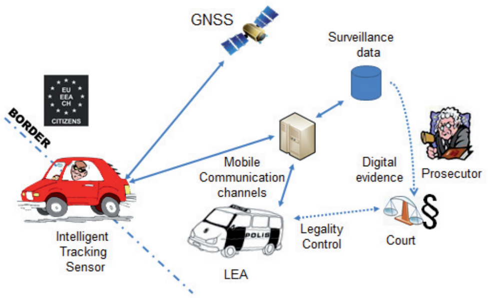


Fig. 1 Operational environment

For pinpointing the major deficiencies in existing surveillance technologies, in the discussions between researchers and industrial and LEA experts, the following major needs or gaps related to everyday investigation and monitoring technologies and the context they are deployed were highlighted:

- Current tracking and monitoring systems are lacking in performance, old equipment is too big in size, hard to disguise and energy consuming.
- Most devices produced for LEAs take account their needs, but commercial interests are sometimes stronger incentive. This situation means that the best solutions are not always for sale and the manufacturers sell out the first generation products before bringing the next generation. This means that LEAs end up with having several inefficient systems lacking integration. This requires a lot of support and logistics. The open IT solutions launched on the markets should be adaptable with new (experimental) sensors.
- Counter measures by criminals are posing new challenges as criminals use advanced detection and signal jamming technologies. Because of this the technologies used by LEAs have to be concealed in better ways, e.g. by size and appearance and have the jamming detection capabilities.
- Operational models of LEAs' information gathering do not comply with the legal and societal requirements and expectations in the needed level, neither with the possibilities the modern technology would allow. Harmonizing by implementing legal requirements into a new system that is useful for all LEAs in Europe is a first step.
- Safety, encryption and access control are very important. For investigation data has to be protected so that no unpermitted access will be possible and the content will not be revealed. Encryption safeguards privacy; tampering will be recognized and encrypted files will guarantee a strong chain of custody.
- New alternative positioning system is required; Galileo becoming operative will give new interdependence possibilities and advantages for tracking.

III. Technical Vulnerabilities of Tracking Systems

A satellite-based tracking system combines navigation and telecommunication technologies. The system is relatively complicated and consists of many technical segments, including the control, space, tracking, communication, data processing, application interface for external applications and end-user segment, as shown in Fig. 2. The basic principle is that a tracked device is positioned by Global Navigation Satellite Systems (GNSS) and positioning data is delivered for post-processing via mobile networks, the Internet or a secure network. The end-user segment might be e.g. an office-based Geographic Information System (GIS) for emergency management. The manner in which GNSS used with GIS is wide and varied allowing users to determine the way GIS and GNSS are used together to best meet their needs.

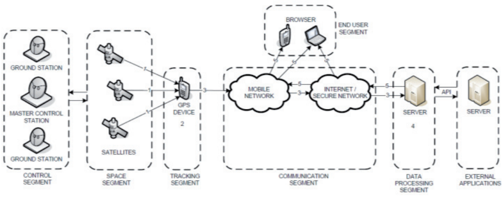


Fig. 2 Principle of a satellite-based tracking system

GNSS-based tracking devices are able to calculate and deliver position information for post processing. Today many mobile phones (smart phones) include GPS receivers and phones are easy to turn into tracking devices by client software. For professional services like emergency management, TETRA clients and tracking-only clients without communications functionality are available. New positioning devices expected to support all four major systems (GPS, GLONASS, Compass and Galileo) so that several techniques can be used simultaneously to guarantee better positioning accuracy and availability. GNSS-based tracking is used in many applications, e.g. in logistics, fleet management, road tolls, traffic signal management. Also, emergency management is using them e.g. for following troop's location.

Very often only the benefits of the satellite-based tracking solutions are advertised while the risks and weak points are forgotten. SATERISK project executed during 2008-2011, yielded information about the present and the future risks of satellite-based tracking systems. It showed that current GNSS-based tracking systems have serious vulnerabilities. The systems are complex and open to several kinds of data delivery problems, data losses and cyber-attacks. The systems are GPS and GSM dependent for positioning and communications. They include no cross-over possibilities; positioning is not based on parallel satellite systems, known WLAN networks, mobile phone cell location, RF/DF etc. Also, intelligence is lacking from the systems; they can be commanded but they do not have the capability of self-reacting and alerting. Furthermore, available commercial products are vulnerable to jamming without jamming detection possibilities and their power consumption is not always optimized.

A. Risk Analysis

Identifying threats of satellite-based tracking in order to avoid the problem of limited existing data or limited knowledge of the risk analysis team, it is necessary to investigate the requirements of the applications and operations/business. An application can have technical requirements that have not been levied on prior uses of the system. If the system cannot offer service with certain requirements, then it is a threat for the application. The requirements of the operations/business can create technical requirements, and the technical limitations of the system causes threats to those requirements being met. Using this approach, we were able to generate a model for identifying threats with regard to satellite-based tracking, shown in Fig. 3.

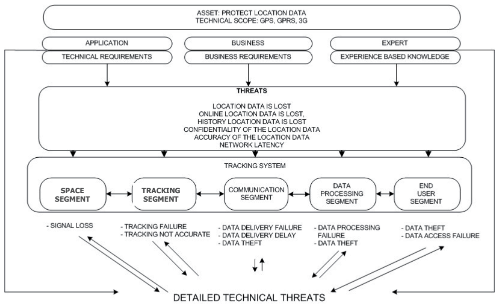


Fig.3 Model for identifying technical threats of satellite-based tracking

We started identifying threats by listing well known technical threats. The asset we chose to investigate was location data. First, we defined the segments of the system and then we group the threat according to the segments in which they occur. We discovered that a single technical threat can be the cause for some higher-level threat. For example, the cause of a tracking failure can be a technical problem in tracking device. The technical problem is the lower-level threat and the tracking failure is the higher-level threat. Also, we noticed that higher-level threats can help to find lower level threats. Data privacy threats are caused by certain technical reasons. The data privacy is higher level threat and the technical reason is the lower level threat. Next, we investigated if higher-level threat could occur in the other segments of the system. For example, privacy threats can be caused by many technical reasons in many segments. This cycle generated relations between all threats and segments.

When we had sorted all well-known threats we added operational/business requirements. Table I shows the threats resulting from this methodology grouped by system segments and categories.

TABLE I. TECHNICAL VULNERABILITIES IN SATELLITE-BASED TRACKING SYSTEMS

System segment	***Threats***
Control segment	Error in monitoring data, Error in adjustment commands
Space segment	Natural disasters (e.g. solar storms, ash cloud from volcano eruption), Collisions in the orbit, Unintended interface, Intentional interface, Atmospheric conditions, Multipath propagation, Selective availability, Total signal loss
Tracking segment	HW fault, SW fault, Power feed break-down, Clock drift, Signal attenuation, Information security diminution
Communication segment	Capacity, Radio coverage, Roaming, Latency, Information security diminution
Data processing segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution, Database corruption
End-user segment	HW fault, SW fault, Power feed break-down, Capacity, Information security diminution

IV. THREATS OF COMMUNICATION SEGMENT

The communication segment contains systems to deliver positioning data for post-processing and further to end-users. The Global System for Mobile Communications (GSM) is the second-generation mobile communications (2G) standard made by European Telecommunications Standards Institute (ETSI). The General Packet Radio System (GPRS) is an extension of GSM, which offers mobile packet-switched access. The data rate offered is 40-300 kbit/s, and the round trip time (RTT) is up to a few seconds. GSM offers connectivity in more than 200 countries covering over 80% of the world's population. Universal Mobile Telecommunications System (UMTS) is the successor to GSM, also called third-generation mobile communications system (3G). It offers voice, messaging and data services. UMTS' data rate is up to 14 Mbit/s and RTT shorter than in GSM. Radio coverage is continually expanding and UMTS currently covers the most populated areas. Short Message Service (SMS) is the messaging service of GSM and UMTS. It allows users to send and receive text messages on a mobile phone. The length of messages is 160 characters, and messages can be sent globally via different operators. Long Term Evolution (LTE) is a fourth-generation (4G) telecommunication standard. LTE offers a packet-optimized service without native support for voice communication. The data rate offered is up to 300 Mbit/s with low RTT. The first commercial networks were launched in Scandinavia in late 2009.

Terrestrial Trunked Radio (TETRA) has been developed for professional services, especially for public safety and security like police and fire departments. It offers voice, short data and packet data services. Strong security features and dedicated capacity are essential for professional use. The latest release of TETRA offers data rates up to 500 kbit/s.

Worldwide Interoperability for Microwave Access (WiMAX) is based on open 802.16 standards. WiMAX offers a packet-switched service and voice communication is not supported. 802.16m offers pick data rates of 1 Gbit/s for fixed line and 100 Mbit/s for mobile users. WiMAX is currently deployed in 149 countries with 621 million people covered [5].

A. Unintended Interferences

Unintended interference can be caused by other radio transmitters that are working nearby the frequencies used by the positioning satellites. Also, weakly shielded or faulty electronics can cause interference. All GNSS-system uses same frequency, which could cause interference problems if the systems are not designed properly [6]. Other lately reported case handled telecommunication system and GNSS interworking; 4G mobile communication network by LightSquared will cause interference for GPS signal in U.S because they are using almost same frequency. The results of simulation showed that the interference will start at 22.1 km for the aviation receiver and total signal loss occurred at 9.0 km from the transmitter. [7]

B. Intentional interference

Intentional interference can be caused by sending interfering signals on the same frequency band that the satellite systems are using. Equipment used for generating interfering signals is called a jammer. Multifunctional jammers can generate intentional interference for mobile radio network frequencies as well as for GPS. Prices for portable devices start at around $30 and the effective range is 2-20m, easy availability and minor cost causes frequent threat. Most of the tracking devices available today accept the false signals as real ones because they are stronger and easier to receive [8]. One way to spoof tracking system is to use dummy satellites, so called pseudo-satellites or pseudolites. Instead of jamming, pseudolites imitate satellite signals and corrupted satellite data causes wrong positioning for tracking devices [9].

C. Capacity

GPRS user plane capacity could be a problem in highly populated areas. Rapidly growing use of mobile Internet causes stress for mobile networks. Rural areas could have very limited GPRS capacity or there may not be GPRS capacity at all. High amount of mobility requires network signalling capacity. 3G offers higher data rates and more capacity than GSM, but usage is increasing due to the real mobile Internet experience that it provides. Networks can run out of capacity in highly populated areas, and there has already been cases reported of capacity problems [10]. SMS delivery does not reserve radio network user plane capacity like GPRS or normal speech, because SMS is delivered within signalling channel. However, high amounts of mobility require high network signalling capacity and SMS capacity is dependent on the operator. Internet capacity depends on access network capacity, core network capacity and current network load.

D. Latency

Latency**,** the measure of time delay experienced in a system, might be a problem. Round-trip time in GPRS can vary a lot, sometimes being greater than 1000ms. 3G offers much lower RTT than GSM; typically 200-300ms. Delivery time of SMS can be even 10 seconds depending on the operator and location. If an SMS is not delivered at first try, it will be buffered by the network for resending. In the Internet, delivery time of the data depends on the capacity of the access network as well as the current network load and distance between delivery points.

E. Information Security

Information security threats, various kind of threats at various level. Delivery of an SMS is encrypted only on the radio interface. An SMS is delivered without encryption in the core network and even between operators. GPRS offers data encryption only on the radio interface whereas data is delivered without encryption in the core network. 3G information security is built on GSM security adding many new security features. However, 3G has security problems; e.g. the International Mobile Subscriber Identity (IMSI) is sent in clear text when allocating the Temporary Mobile Subscriber Identity (TMSI) to the user; the transmission of the International Mobile Equipment Identity (IMEI) is not protected; hijacking of outgoing/incoming calls in networks with disabled encryption is possible. In the Internet, data is not encrypted as default, so unsecured and sensitive data can be a potential target for the hackers and criminals.

F. Radio Coverage

Although GSM offers wide connectivity, there are areas without GSM *radio coverage*. Some parts of USA, Canada, South America, Africa, Russia and Australia have their own 2G systems running till day. 3G has good radio coverage in North, West and South Europe. Other parts of the world are currently expanding their networks. There is lack of unified coverage across globe considering these technologies.

G. Roaming

Roaming is the situation when a device is moving outside of its home network. Roaming can cause a situation when the mobile device is not able to deliver location data via SMS, GPRS or 3G. Roaming between TETRA networks is not in operational use.

V. Discussion and Conclusions

Based on the identified deficiencies in the existing solutions, operational scenarios defined by the consortium LEAs and considerations of future challenges and issues that would be the most influential in European and international context, SATERISK has found to follow five main operational and technological challenges.

1. GNSS sensors; commercial sensor do not fulfil the needs of LEAs.
2. Cross-border operations; criminal nature has internationalised but LEAs are national organisations.
3. Secure mobile communications is more and more important in all operations.
4. Digital evidence; surveillance data LEAs collect should be valid in the court [11].
5. Legality control; LEAs' operations should be transparent [11].

A. Cross-border LEA Operations

Organized criminality does not respect national borderlines and international warehouses of crime involved in smuggling, drug and human trafficking and terrorism are becoming a stronger threat to the European security. Following this, there is an increased need for European collaboration and information sharing related to the investigation technologies; cross-border usability and interoperability of investigation tools have to be guaranteed. However, 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 to e.g. to slow or even hindered information exchange, endangering the success of entire investigations.

Viitanen et al. [12] focus on cross-border surveillance operations dealing with time critical data communication between multinational organizations. This problem is common between the LEAs. Criminals are working more often abroad due the European integration, but LEAs do not have common protocols and procedures, how to pass information between each other. Especially machine to machine (M2M) communication is not researched yet.

B. Secure Mobile Communications

Secure, uninterruptable communication is a pre-requisite in critical environments, for example in public safety applications and critical infrastructure telemetry. General purpose IP based communication links may not be adequate and sufficient. For example, capacity of communication links and cyber warfare may present problems. Methods for ensuring constant connectivity and maintaining unbroken communication in all circumstances are needed. Traffic engineering and multichannel communication may mitigate the aforementioned problems. The DSiP solution (Distributed Systems intercommunication Protocol ®) enables parallel use of different network technologies in a consistent and transparent way enabling communications services platforms to be created. For example in cross-border operations, this is a huge advantage [13].

Information security has at least five dimensions: Availability, authenticity, confidentiality, integrity and non-repudiation. Violating any of these may cause considerable harm or even damage. Identifying issues related to information security in satellite-based tracking systems is a huge topic. Kämppi et al. [14] open this playground in the SATERISK project introducing the technical architecture and data flow in General Packet Radio Service (GPRS) and points out vulnerabilities and unknown issues in information security. They conclude that applicable security solutions or satellite-based tracking systems are, however, available. The also study describe major technical vulnerabilities of such systems. The field is divided into four segments: the satellite and tracking segment, the communication segment, the data-processing segment and the end-user segment. Each of these segments has its own set of risks and threats, which can be reduced to an acceptable level. Preserving the confidentiality of data is seen as the most important issue.

C. Future Work

In order to bringing about the LEAs' special requirements for GNSS, technological and socio-technical research and development work is needed. Development of novel monitoring systems and miniaturized sensors improves LEAs' evidence-gathering abilities while respecting legal and ethical expectations of society. Also, tactical and technical mobile communication solutions to various high end security purposes need more research.

References

[1] "High Precision GNSS Market Set to Increase Almost 100% by 2016". ABI Research, 2011, 9, 29. Available at: http://www.abiresearch.com/press/3780-High+Precision+GNSS+Market+Set+to+Increase+Almost+100%25+by+2016

[2] J. Rajamäki, R. Guinness and S. Tiainen, "Introduction," in *SATERISK Risks of Satellite Based Tracking* (Sample of Evidence Series, vol. 2), J. Rajamäki, R. Pirinen and J. Knuuttila, Eds. Helsinki: Edita Prima, 2012, pp.13-16.

[3] T. Erling, "Preface – Technology Develops Taking International Cooperation to New Level," in *SATERISK Risks of Satellite Based Tracking* (Sample of Evidence Series, vol. 2), J. Rajamäki, R. Pirinen and J. Knuuttila, Eds. Helsinki: Edita Prima, 2012, pp.7-8

[4] J. Rajamäki, "Cross-border Satellite-based Tracking: Needs, Approach, Benefits and Competition", *Proc. of 2nd International Conference on Ubiquitous Positioning, Indoor Navigation and Location-Based Service*, UPINLBS2012, Helsinki, October 3-4, 2012.

[5] WIMAX Forum. [online]. *Monthly Industry Report*, February. Available at: http://www.wimaxforum.org/resources/monthly-industry-report.

[6] P. Parkinson, "Conference plenary, Never Lost Again", *61st International Astronautical Congress*, Prague, Czech Republic, September, 2010.

[7] L. Edwars, L. (2011) "New 4G network could cause widespread GPS dead zones", Available at http://www.physorg.com/news/2011-02-4g-network-widespread-gps-dead.html (Assessed 6.11.2011).

[8] H. M. El-Bakry and M. Mastorakis, M. "Design of Anti-GPS for reasons of security", *Proc. of the Int. Conference on Computational and Information Science,* 2009, pp. 480-500.

[9] M. Happonen, *et al.* "Jamming detection in the future navigation and tracking systems", *Proc. of the 16th Saint Petersburg International Conference of Integrated Navigation Systems,* St. Petersburg, Russia, May, 2009, pp. 314-317.

[10] D. Sarno (2009), Los Angeles Times. http://articles.latimes.com/2009/dec/10/business/lafi-iphone10-2009dec10

[11] J. Rajamaki, *et al.*, "How Transparency Improves the Control of Law Enforcement Authorities' Activities?," *Intelligence and Security Informatics Conference (EISIC)*, 2012 European , vol., no., pp.14-21, 22-24 Aug. 2012. doi: 10.1109/EISIC.2012.35. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6298881&isnumber=6298809

[12] J. Viitanen, *et al.*. Near Border Procedures for Tracking Information. *WSEAS TRANSACTIONS on SYSTEMS*. iss. 3. vol. 9, 2010. pp. 223 – 232.

[13] j. Rajamäki, J. Holmström and J. Knuuttila, "Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities," *Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, Twente, The Netherlands Nov. 24-25, 2010 and IEEE Xplore.

[14] P. Kämppi, J. Rajamäki and R. Guinness, R. "Information security risks for satellite tracking systems," *Int. Journal of Computers and Communications*, iss. 1, vol. 3, 2009.

[15] CELTIC-Plus, *Project Information - Multi-agency cooperation in cross-border operations* [Online]. Available: http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

II

HOW TRANSPARENCY IMPROVES THE CONTROL OF LAW ENFORCEMENT AUTHORITIES' ACTIVITIES?

by

Jyri Rajamäki, Jutta Tervahartiala, Sofia Tervola, Sari Johansson, Leila Ovaska & Paresh Rathod, 2012

Proceedings of The European Intelligence and Security Informatics Conference (EISIC), 2012, 14-21

2012 European Intelligence and Security Informatics Conference

How Transparency Improves the Control of Law Enforcement Authorities' Activities?

Jyri Rajamäki, Jutta Tervahartiala, Sofia Tervola, Sari Johansson, Leila Ovaska and Paresh Rathod
Laurea University of Applied Sciences
Espoo, Finland
{jyri.rajamaki, jutta.tervahartiala, sofia.tervola, sari.johansson, leila.ovaska, paresh.rathod}@laurea.fi

***Abstract*— When preventing and investigating crime the law enforcement authorities (LEAs) perform a variety of activities that affect civilians' privacy. Video surveillance, audio surveillance, technical monitoring and tracking are few to mention amongst many other activities. On various incidents, law enforcement is seeking more control rights that increases concern amongst citizens and also level of open debate increases steeply. The aim of this paper is to provide an improved understanding why transparency is a crucial factor succeeding in LEAs' technical surveillance. This research work also presents examples of current technological possibilities to create transparent and plausible monitoring for surveillance activities. The paper is based on the results and lessons learned from the Finnish SATERISK (SATEllite-based tracking RISKs) research project executed during 2008-2011. Trusts in LEAs have always been high in Finland. Even though number of people in society who do not have any confidence in authorities, especially for police forces and their extended control. However, there are empirical and factual evidences that civilians are willing to give extended rights to authorities if used in intrusive means for extremely necessary situation. In such cases, people are more open and expecting authentic timely information. The research work also discusses the challenges faced by LEAs during criminal investigations.**

***Index Terms*— Law Enforcement, Law Enforcement Authority, Surveillance, Surveillance technology, Transparency, Public Trust**

I. Introduction

Organised crime is a real threat in Europe with the emergence of international warehouses of crime. International terrorism has also evolved into a more threatening problem. According to the study done by Elyv in 2009, there is a strong relationship between public fear of terrorism, and the willingness of the public to allow to the authorities more rights for increasing security [1]. Data protection laws do not always offer a sufficient protection against threats stemming from the use of new technologies and modes. The importance of security increased dramatically due to fear caused by terrorist attacks. The cutting-edge security measures are in use without proper debate and study on social implications. The most efficient security practice is often regarded as a threat to the privacy and civilians are afraid of being suspect. It is common phenomena to think more security means less privacy, and more privacy means less security! Such insecurity feelings leads majority of citizens to give up their privacy in order to get more security [2]. Informational control requires high level of transparency regarding data gathering and information processing [3]. In criminal network investigations, there are four common problems: resources, information amount, information complexity and information sharing [4]. On other hand, law enforcement authorities (LEAs) are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. To help LEAs struggle against criminals, the European Union backed with an anti-terrorism legislation which requires telecommunication operators to preserve phone data and internet logs for a minimum of six months [5].

The issue in this case is trust. To prevent and investigate crimes, LEAs are able to conduct various operations which are affecting privacy of citizens. People fear that a LEA can abuse its power and intrude their privacy, even though retaining phone data is not as intrusive as technical tracking or eavesdropping. Modern systems have some features, for example if phone call or e-mail exchange data is traced, the operator's system and log files will have marks that the copy of the data has been delivered to the LEA.

At present, many LEAs are using old-fashioned stand-alone investigation tools and tracking systems which neither creates watermarks nor log-file marks. For that reason neither chain-of-custody nor social acceptance of transparency comes true [6]. For example, in Finland the oversight of police's coercive measures is based on a file system SALPA (Finnish acronym of electronic database system used by the Security Police (SUPO) and the National Bureau of Investigation (NBI)) [7]. The SALPA system guides how to make applications and notifications in correct manner. However, the question arise if information that police officers write down are not based on actual log files, can this system alone be a sufficient base for legally control system?

These non-transparent systems might be a hindrance to LEAs [8]. LEAs may also act according to law, but they are not able to prove it because methods cannot be audited by neutral outsider. The current state of affairs is neither efficient nor transparent. With lack of trust, there is also a lack of new legislation that allows usages of new crime fighting tools. In this situation, we all are compromising or losing our security. More advanced monitoring system is essential and required to provide faultless round-the-clock control of the surveillance equipment and procedure. At present, no process or instance is able to present publicly proven technical control methods involved in the chain.

This paper deliberates the importance of transparency of law enforcement authorities' (LEAs) technical surveillance and presents a system with improved transparency and efficient

978-0-7695-4782-4/12 $26.00 © 2012 IEEE
DOI 10.1109/EISIC.2012.35

IEEE computer society

surveillance operations that acceptable to citizens. The paper is based on the results and lessons learned from the Finnish SATERISK (SATEllite-based tracking RISKs) research project executed during 2008-2011 [9]. This paper has six sections. The second section briefly introduces the main terms and concepts applied in this paper. The third section examines related work. The forth section outlines the SATERISK research project and presents the findings with regard to social acceptance and transparency of surveillance carried out by LEAs. The fifth section describes an example of a technical solution that fulfills social acceptance demands of LEA operations. The last section concludes this paper.

II. Terms and Concepts

This section briefly describes the terms and concepts of surveillance authority process

A. *Law Enforcement Authority (LEA)*

Law enforcement broadly refers to any system by which some members of society act in an organised manner to promote adherence to the law by discovering and punishing persons who violate the rules and norms governing that society [31]. Law enforcement authority (LEA) is a national police, customs or other authority that is authorized by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities.

B. *Activities*

LEAs are working in order to prevent and investigate crimes. Some of the operations affect privacy of citizens. Video surveillance, audio surveillance and technical tracking are among those activities [6].

BBC News [10] listed some of the possible means for surveillance and tracking: CCTV cameras, automatic number plate recognition, radio frequency ID tags in shops, mobile phone triangulation, store loyalty cards, credit card transactions, satellites, electoral roll, NHS patients records, personal video recorders, phone-tapping, bugs and hidden cameras, worker call monitoring and cookies. Only LEAs can legally use the information from all these sources.

In addition to using gathered data LEAs share information with other authorities. European integration has increased transport of the illegal goods and criminals. Therefore, transmitting, tracking and other status information between nations and different organizations becoming everyday business. LEAs are using more tracking technology than ever before. The systems are network based (GSM&TCP/IP) and they can transmit information basically anywhere. These days, technical tracking is used in even nominal cases [9].

C. *Surveillance*

Surveillance is purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection [11].

Purposeful means the monitoring has a point that can be justified in terms of publicly agreed goal. Routine means it happens as we all carry on our daily business. Surveillance is also systematic because it is planned and carried out according to the rational schedule. Finally, surveillance is focused. While some surveillance depends on aggregate data, majority refers to identifiable persons. Their data are collected, stored, transmitted, retrieved, compared, mined and traded [11].

D. *Transparency*

The society is presented as “soft surveillance, knowledge and non-forgetting history data” says Finnish futurologist Mannermaa. He believes that every action of the authorities must be tracked, and surveillance should be commonly agreed upon and transparent [12]. The public feels they have lost control over their own data and they do not know who handles personal data, when and for what purpose. And 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 transparency of these operations [13].

The law enforcement surveillance operation which can be approved by the citizens must be transparent and possible to prove. Authorities are able to get more jurisdiction based rights, if citizens have more trust into the system. In ubiquitous networked society, it is important that single-sided enforcement changes to multi directional surveillance and develops transparent authority power. Transparency is needed because of the new legislation that meets LEA’s needs even when there is wide and good trust base. People must be assured that LEA is not abusing its power. Today transparency can be based on technology which supports operation’s legal processes firmly [6].

The principle of transparency is information should be shared while data is collected. Even extended information should be given to a person in subject including circumstances under which data collected and shared, protection measures and identity of officer in subject. Individuals and communities need to have an opportunity to control the use of the government and public allowances with the help of the openness of the authorities [15].

III. Related Work

A. *Security or Privacy*

The United States Department of the Treasury initiated the Terrorist Finance Tracking Program (TFTP) after the 2001 terrorist attacks in New York. The objective of TFTP is to identify, track and pursue terrorists and their networks worldwide. The U.S. Treasury Department issues subpoenas to a company that collects information on financial transactions worldwide, the Society for Worldwide Interbank Financial Telecommunication (SWIFT). The U.S. Government receives information from SWIFT as part of specific terrorism investigation and it is able to execute targeted searches against the records of SWIFT in order to track financial transactions that may be linked to terrorist activity. SWIFT data aid in tracing terrorist organizations and their networks. By following the money, the TFTP has enabled locating terrorists and their financiers and thus helped stop funding terrorism. Lives have been saved, thanks to the Terrorist Finance Tracking Program. Access to financial transaction data raises questions about privacy of citizens. SWIFT is overseen by a committee from several central banks, for example the U.S. Federal Reserve, the Bank of England and the Bank of Japan. The TFTP ensures it has precise safeguards and protocols regarding privacy. The program is regularly audited by an independent party [16].

Various surveys show that concerns about privacy have escalated during past few decades, at least in the U.S. A great increase in concerns about intrusions into personal life has been noted. People also feel anxious about using computer and this anxiety seems to be growing. The worry is greatest among people who do not use computers. Citizens are becoming more skeptical against allowing government agencies to post public records of personal information over the internet. The respondents would be more willing to allow posting public records if the agencies would have certain privacy guidelines [17].

In Europe, the general data protection according to the principle of conservation of information is "kept in a form which allows the identification for as long as is necessary for the purposes for which the data were collected or further processed". In 0155 the principle of interpreting and applying it to the case of traffic information that is collected and processed billing and interconnection principles (as defined in Article 6(2) the e-Privacy Directive), some countries consider three months as sufficient time for the storage of traffic data collected for billing and interconnection payments, while others, such as Romania, require a longer time. The choices made by the Member States during the storage of traffic data to reveal the fragmentation of necessity in relation to length of storage of the data and greatly varied approach to the protection and up to the principle of proportionality are concerned [18].

Recently, there is common agreement at European level about storage time identification, traffic and location data for law enforcement purposes. Directive 156 mentioned about the retention of data between six months to two years from communication. Directive 157 aims to harmonize the relevant provisions of the Member States concerning the obligations. Common recommendation to the electronic communications services or public communications networks to maintain the association of certain identification, traffic and location data that is produced or processed in order to ensure that the information is available for the detection, investigation and prosecution of serious crimes, as defined by each Member State under national law. Directive 158 shows, European Member States have made different choices as to store identification, traffic and location data for law enforcement choices, the framework provided by the Data Retention Directive [18].

B. *LEA's Powers versus Transparency*

The European Commission has been collating the perceptions, attitudes and views of the EU citizens on data protection issues. The wider survey and study conducted under the title, "Data Protection in the European Union: Citizens' perceptions". The survey reflects citizens' general feelings and concerns about data privacy and trust in different types of organizations that holds their personal data. The study also helps in awareness of their data protection rights and national protection authorities. According to this survey, the threat of international terrorism is an acceptable reason to restrict data protection rights. The opinion of the majority of respondents reflects that it should be possible to monitor passenger flight details (82%), telephone calls (72%) and internet and credit card usage (75% and 69%, respectively) when the matter was connected with the prevention of the terrorism. In this survey, it came to light that there was suspicion about any provisions that would allow authorities to relax data protection laws and it should be within clearly-defined limits. 27%-35% of the respondents said that only suspects should be monitored and 14%-21% of the respondents wanted even stricter safeguards [19].

The police is one of the organizations which had confidence in data protection, 80% of the respondents reported trusting the police to use their data properly. The respondents reported trusting in other public authorities such as associate security 74%, tax authorities 69% and local authorities 67%. 66% respondent shows trust in Banks and other financial institutions. The confidence was highest in Finland and Denmark and lowest in Latvia and Lithuania. Age and education played a role in the respondents' trust in specific organizations. Concerning the age of the respondents, there was a pattern that the older the respondents were, the less likely trusted any of the listed organizations. 84% of the 15-24 years old trusted the police that they protected their personal data, while only 78% of the over 55 years old believed so. Highly-educated respondents had more confidence in data privacy issue than less-educated respondents [19].

IV. Analytical Framework and Methods

A. *SATERISK Research Project*

The Finnish national SATERISK (SATEllite-based tracking RISKs) was a joint research project of universities, public organizations and private companies with regard to positioning, navigation and tracking systems on the whole tracking value chain, as shown in Fig. 1. The project started in September 2008 and ended in December 2011. The SATERISK project led by Laurea University of Applied Sciences, had partners and other participants from the whole value-chain of satellite-based tracking; starting from the network operators to companies that offer information-gathering devices and tracking software, and finally to the users of these tracking systems, such as Police and Customs. The legal aspects of satellite-based tracking were studied at the University of Lapland in its own SATERISK co-project. [9]

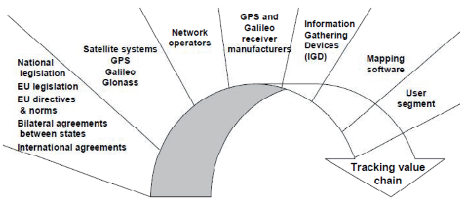


Figure 1. Sectors of the SATERISK project

The SATERISK project aimed to answer the following questions: Does satellite-based navigation and tracking involve risks? Do we know what the risks are now and what they will be in the future? Often new technologies will present opportunities for increased safety and security—and this is certainly true with satellite-based navigation and tracking—but they can also create new risks. It is important for the technology developers and end-users to clearly understand these risks and take steps to mitigate them. The project aimed at a situation where laws on positioning and tracking allow the use of machine to machine (m2m) tracking devices across state and union borders. The project aimed to bring new know-how on an international level to the European security field. The project created new methods and development paths for positioning and tracking systems. The widely used US-based GPS (Global Positioning System) and Russian-based GLOSNASS (Globalnaja navigatsionnaja sputnikovaja sistema) satellite positioning systems will soon get an EU counterpart and rival from Galileo. While most of the satellites are still on the ground, it is important that any problems and possibilities related to the new system are charted. The SATERISK project also offered technological solutions to issues that aroused while the project was on-going. Fig. 2 shows the research topics of the SATERISK project.

Figure 2. Research topics of the SATERISK project

The SATERISK project evaluated technical, operational and legislative risks of positioning and tracking. Studies of current risks were followed by producing risk scenarios for the future. Another interesting area was developing new service innovations that apply satellite-based tracking. The project also organised three annual "Situation Scope" seminars and the "Building Trust on Borders" seminar dealing with the situational awareness of international operations.

Students participated in many interesting projects related to SATERISK and gained over 1600 ECTS from that work. Thus far, the results of the SATERISK project mainly been featured in various publications, conferences, seminars, workshops and theses. More than twenty peer reviewed articles have been published, addressing various aspects of the project. Also, SATERISK has published two books [20], [21].

SATERISK also aimed to bring new know-how to the European field of safety and security. The project created new methods and development paths for positioning and tracking systems that address risks and limitations which already been discovered. Including methods related to information security, signal interference, and legal restrictions on tracking. A special emphasis have been placed on the use of satellite-based tracking amongst safety and security professionals—both in the public and private sectors—where the risks could be high if they were not properly addressed.

B. *Research Methodology*

Neither computer science alone with its technical solutions nor psychology or other behavioural disciplines is able to address the challenges of today's safety and security problems, especially in sufficiently integrated way. If we put innovative artefacts into action and analyse how they are used and how they perform, we will see things that cannot be seen in the laboratory [22]. Management information systems (MIS) involve three primary resources: people, technology, and information. The SATERISK project follows the basic development research in the MIS wheel diagram, first published in 1991 [23]. In the concept of Development Research (DR), the continuum of scientific method using each aspect to inform system design as Design Science Research (DSR) choices and using systems technology to inform the science [24], [25], [26]. DR and DSR are research approaches that can be combined with other social science methods such as grounded theory, action research and case study research.

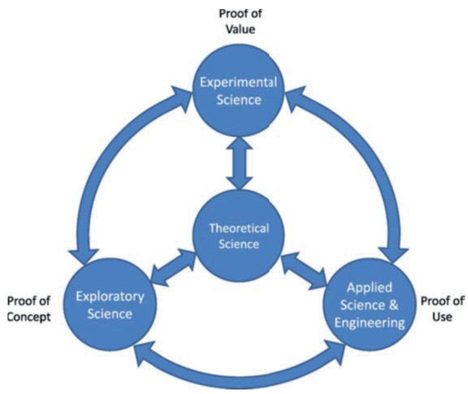


Figure 3. Integrated, multidisciplinary, multi methodological development research

According to the "going the last mile" approach [22], the starting point of research should be a real problem for real people. In the SATERISK project, this real problem came from Law Enforcement Authorities who had exploited GNSS-based tracking but who fretted about how it had been used. The creation of innovative artefacts includes three phases: proof of concept (POC), proof of value (POV) and proof of use (POU). This means designed artefact is not really understood and cannot really be evaluated before actually implemented. In addition to POC and POV, they should also strive for POU [22]. The SATERISK project integrated science both in the laboratory and in the field (see Fig. 3), including the theory, prototype and validation by experiments or field studies.

The SATERISK project has widely studied technical, operational and legislative risks from different points of view. All end-users of tracking devices and systems from both public and private side faces some risks when they use tracking; also being tracked by someone else is a problematic issue. This paper concentrates on the results with regard to the risks that LEAs faces when they exploit tracking, one being the social acceptance of applying these new technical systems.

C. *LEAs' Special Requirements for Tracking Systems*

Organised crime has been increased. For improving their evidence-gathering abilities, the LEAs are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. The criminals' counter measure activities like electronic counter-surveillance, jamming and constant changes in behaviour for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new, hard to detect, strongly encrypted, long-lasting and quick to install, and more adaptive intelligent technologies, is emerging. Respecting the accountability and integrity requirements and smooth utilisation of data in different phases of chains-of-custody is of utmost importance. In the current situation the chain of custody is difficult to maintain due to different techniques that operate on their own and connected to different monitoring systems. This makes LEA's work very labour-intensive hence the use of new state-of-the-art technologies should enable optimization of human resources. [27]

Fig. 4 shows the operational environment where LEAs use tracking.

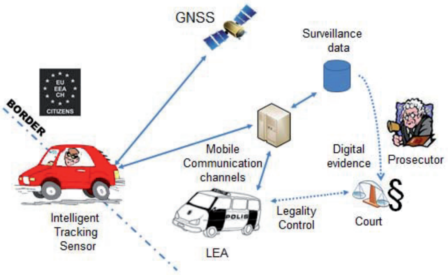


Figure 4. Operational environment

LEA officers need to have an easier access to all investigation data, independently from place and time. Special attention has to be paid to the public awareness and concern on the use of surveillance equipment. However, legal recording, retrieving and monitoring of criminal activities in a safe and silent way also raises two problems: (a) how to ensure accountability of law enforcement officer who uses intrusive techniques and (b) how to ensure sufficient implementation of privacy safeguards. That also ensures proper measures are used exclusively during overriding situation where interest prevail in a proportionate way.

Based on the identified deficiencies in the existing solutions, LEAs consortium has defined operation scenarios and considerations of future challenges and issues, which could be the most influential in Europe and International context. SATERISK has found the following five main operational and technological challenges:

1. GNSS sensors: Commercial sensors do not fulfil the needs of LEAs.
2. Cross-border operations: International nature of criminals where LEAs are national organisations.
3. Secure mobile communications: it is more and more important in all operations.
4. Digital evidence: LEAs collected surveillance data should be valid in the court.
5. Legality control: LEAs' operations should be transparent.

This paper concentrates on the fifth challenge; legality control and social acceptance of applying these new technical surveillance systems.

D. *Security or Privacy*

The surveillance methods used by LEAs are one of the most regulated areas in the society. It is important to build a safe and reliable system, mainly because majority people are particularly concern about unseen and what they also think uncontrolled and excessive surveillance. Fortunately, LEAs can legally obtain information from all these sources. Unfortunately, large-scale technological infrastructures are prone to large-scale problems. We read newspapers and on the web, also watch on TV and hear on the radio, news about some or other way of data leakage. The only relief is - fortunately, it is really difficult for a cracker to get all the information about one person.

Occasionally there are allegations about LEAs abusing surveillance. Because the cases and materials are mostly confidential hence publicly not available to use as counter argument, LEAs cannot prove that they are not abusing. LEAs argue that what is invisible, and the police under control, must be proportionate otherwise it would never be accepted. You must be free from defects surveillance equipment under control at all times in order to happen. How is this possible? And the real challenge is how can you prove it to the public? That shows dilemma about security or privacy [6].

E. *Technical Tracking as Covert Coercive Measure for Police to Collect Information*

The Finnish Coercive Measures Act (CMA) defines the methods and measures that pre-trial investigation authorities can use and entitles them to interfere in human rights protected by law. According to CMA, technical tracking means tracking of a vehicle or goods with an attached radio transmitter or other such device or mechanism. While according to the Finnish Police Act (PA), technical tracking means tracking of the movements of a vehicle or goods

Within the SATERISK project, the legislation in force regarding technical tracking as a part of technical surveillance has been clarified. The legislation is disordered and difficult to understand. It includes numerous partial reforms, references to other laws and as a whole it is hard to manage. What makes it especially difficult is a trouble of drawing the lines between those coercive measures which are prescribed in CMA and are used in a pre-trial investigation and those measures which are prescribed in PA and are used for information gathering purposes in a phase of crime prevention [28].

When the officers in charge of the investigation are dealing with technical tracking as a covert measure, they should take into consideration the following things: In addition to sections of law regarding technical tracking also human rights, general principles of police duties, such as relativity principle, and professional ethics should be taken into account. According to that evaluation of the functioning of legality control concerning covert coercive measures and especially technical tracking, the quality of legality control in Finland is good. However, an external legality control regarding technical tracking is quite insignificant which reflects to the internal control of the Police which is also on very small-scale [28].

With regard to the use of technical tracking, very little scientific research information is available. There is only small literature on evaluation of some methods of application available. It is very hard to find any description or legal rules on this item. Further, there are no comments available from Parliamentary Ombudsman or Deputy Ombudsman, neither legally valid decisions of Supreme Court nor Court of Appeal regarding technical tracking [28].

In Finland, the reform of legislation is in progress. The new Coercive Measures Act was signed in July 2011 and it comes into effect in January 2014. The new CMA would undermine possibilities of the Police to carry out efficient pre-trial investigation. At the same time it would increase the amount of work for officers in charge of investigation. It would also reflect especially to the execution of technical tracking of vehicles and to use of the extraneous information obtained by covert coercive measures to an offence other than that for which the investigation is carried out [27].

F. *LEA's Powers versus Transparency*

However, there are vague signs that citizens are willing to give more power to authorities if usage of these intrusive means is more transparent and better monitored by public. This presumption is based on a poll made within the SATERISK project and received significant response, results are shown in Fig. 5.

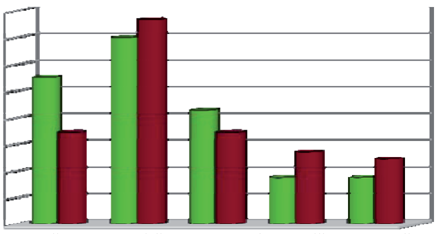


Figure 5. Poll on willingness of conceding more power to LEA

The red columns (on right) present those who want to give more jurisdiction based rights to LEA in current circumstances; where only 17.3% fully agreed. The green columns present those who are willing to give more jurisdiction based rights when given assurance that LEA is not abusing its power; there 27.5% fully agreed. From these columns, a shift can be seen to pro-more powers to LEA, if people can be sure that LEA is not abusing them and using for security of citizens [6].The fact which makes it even more noteworthy, that in the 2007 Police barometer (n=989), 48% of Finns trusted the police fully and 46% for most part [29]. So only 6% had not trust in police. Recent results of European Social Survey also backed the trust in police in Finland [32]. Police is by far the biggest law enforcement agency in Finland. Hence, even when there is wide and good trust base, there is still a need for more transparency. What we can see here is that citizens are more willing to give more jurisdiction based rights, if they have more trust in the system.

In November 2011, the student authors of this paper carried out another study. Four different age-groups' understanding were examined with regard to their knowledge about how much information is being collected from them and their approach to data collection. A significant positive signs from the result was - that the demand for privacy is blurred in case of an emergency situation, such as the disappearances. In emergency situations, law enforcement and rescue authorities are allowed to use all the means and people do not feel interference in private life. In such situation lives are at stake. When it comes to other issues, citizens are more critical about who has the right to receive the location information in hand. The basic demand for privacy is an important thing, namely that no one can, at least not forced to surrender their place to their knowledge. All the related technology will be adjustable so the person is in control of own needs.

V. Technical Solution

We are proposing a transparent surveillance system as a solution of above mentioned problems. Fig. 6 represents the system for transparent surveillance.

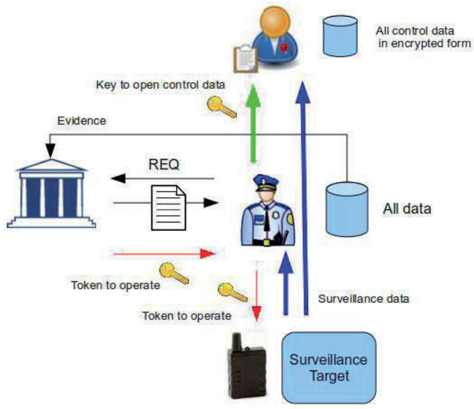


Fig. 6 System for transparent surveillance

The ‘surveillance data' is consumed by Police (blue line in Fig. 6). Surveillance data is also delivered to the oversight officer at the same time (blue line). The oversight officer can audit the conducted operations and related materials by contacting Police and asking for the accessing key for the data (green line and key), REQ(uest) and court order (black line between Police and court). Surveillance equipment accepts court issued statistical encryption token and sets parameters to operation as court has ordered (red line and key). The equipment collects data from surveillance target (blue area). All data is stored by Police and the oversight officer, but auditing the data contents requires operation decryption key from Police. Without the decryption key data cannot be accessed [30].

Nowadays, LEA can use publicly accepted authentication and cryptography functions in order to authorise and control equipment and the data they produce. The equipment may reduce the privacy of individuals. The technology and procedure used consist of several parts. The most significant improvement compared to the current situation is the new system is centralized, and parts are only working together and ad-hoc usage is not allowed. The process parts are

- Court (instance of permissions),
- Police (instance of cases and operations),
- Legal audit (monitoring, auditing and inspections of coercive means),
- Target (surveillance operation target).

The most intrusive parts used in surveillance operations are the surveillance equipment and the data they produce. No authenticated permission token is needed at the moment. If token is not required, simply the usage cannot be controlled. There is even no proof of correct usage of the equipment.

There is similar kind of problem with the data produced by processes. Some incidents where authentication is required- and patterns are recognised in both legal and technical terms. However, it cannot be determined when, where and by whom the data were produced. Also, it cannot be said whether the collected data is the same kind of data which has been authorised to be collected.

When coercive methods are used, the authority should be asked if the equipment is able to work without token, who knows about the operation, if the equipment can be used without authorization, if the amount of data can be identified and if the used equipment has been under control all the time.

Proof of Concept – implementation includes chain of trust between the process parties. Therefore it is possible to create a transparent and secure surveillance operation base. Systems transparency is based on technology. All legal processes are firmly supported. The surveillance material can be obtained only with technology authenticated to operation. For the supervision, all data from the source is sent in encrypted form to a trusted third party, which is a trustee of the public. This trusted third party sees real data only when LEA's representative is present with the decryption key. This way the information remains secret and they cannot be abused.

VI. Conclusion

The ideal situation would be to achieve a balance between surveillance and privacy. How is this balance going to be reached? The answer is to understand the threats to privacy, privacy enhancement mechanisms and the principles which make the balance possible. Surveillance should ensure that its exercise is fair, legitimate, proportionate, transparent and accountable [13]. Many countries want to improve law enforcement and general security. This leads to the fact that new surveillance technology as well as new legislation enabling its usage is needed. The people will be ready to give greater authority to LEA than before if they believe that it increases safety and security. And they can trust that the authorities do not abuse the power received by them. LEA officers have to understand that the systems must be linear and transparent so that the new legislation, which makes the utilizing of the new technology possible, will be obtained.

One important part of designing and developing the surveillance authoring process is creating open acceptance process for the technology. Both security and transparency are important in surveillance operations and they must be at a sufficient level.

References

[1] D. Elvy, “Terrorism, Threat and Time: The mediating effect of terrorist threat on public willingness to forego civil liberties” presented at the 9th Intelligence and Security Informatics Conference (EISIC), 2011 European, Athens, Greece, Sep. 12-14, 2011, ISBN 978-0-7695-4406-9, pp. 52 – 57.

[2] F. Coudert,” European perspective on surveillance,” Computer Law & Security Review vol. 26, pp.377-384, 2010.

[3] BBC. (2006). *A report on the Surveillance Society.* [Online]. Available: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf accessed on June 5, 2012.

[4] R.R. Petersen, and U. K. Wiil,” CrimeFighter Investigator: A Novel Tool for Criminal Network Investigation”, presented at the 9th Intelligence and Security Informatics Conference (EISIC), 2011 European, Athens, Greece, Sep. 12-14, 2011, ISBN: 978-0-7695-4406-9, pp. 197-202.

[5] Directive 2006/24/EC of the European Parliament and of the Council of 15 Mar. 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Directive 2006/24/EC.

[6] P. Viitanen, P. Patama, J. Rajamäki, J. Knuutila, H. Ruoslahti, T. Tuohimaa, and I. Tikanmäki, ”How to Create Oversight in Intelligence Surveillance”. [Online]. Available: http://www.wseas.us/e-library/conferences/2011/Meloneras/ACELAE/ACELAE-07.pdf accessed April 5, 2012.

[7] J. Niemi and V-M. de Codzinsky, “ Telecommunications surveillance and legal protection in Finland,” Finnish National Institute for Legal policy, research report 243, 2009. [Online]. Available: http://www.optula.om.fi/en/1247666990623 accessed on April 9, 2012.

[8] P. Viitanen, M. Happonen, P. Patama, and J. Rajamäki, “International and Transorganizational Information Flow of Tracking Data”. [Online]. Available: http://www.wseas.us/e-library/conferences/2009/tenerife/EACT-ISP/EACT-ISP-18.pdf accessed on April 5, 2012.

[9] Saterisk. [Online]. Available: http://www.saterisk.fi accessed on March 5, 2012.

[10] BBC news story, “How we are being watched?,” BBC London, Feb. 2006. [Online]. Available: http://news.bbc.co.uk/2/hi/uk_news/6110866.stm accessed on April 3, 2012.

[11] D. Wood, K. Ball, D. Lyon, C. Norris, and C. Raab,” A Report on the Surveillance Society,” 2006. [Online]. Available: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf accessed on April 7, 2012.

[12] M. Mannermaa, Jokuveli – Elämä ja vaikuttaminen ubiikkiyhteiskunnassa (Some brother society). Helsinki: WSOYpro, 2008, ch. 2.
[13] D. Hallinan, M. Friedewald , P. McCarthy, "Citizens' perceptions of data protection and privacy in Europe," ," Computer Law & Security Review vol. 28, pp.263-272, 2012.
[14] K. Aquilina, "Public security versus privacy in technology law: A balancing act?," Computer Law & Security Review, vol. 26, pp.130–143, 2010.
[15] Minstery of Justice, Finland, Act on the Openness of Government Activities. 14.04.2012 [Online]. Available: http://www.om.fi/Etusivu/Perussaannoksia/Julkisuuslaki/Uudistuksesta accessed on April 7, 2012.
[16] U.S. Department of the Treasury, Terrorist Finance Tracking Program (TFTP), 2011. Available: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Pages/tftp.aspx accessed on May 28, 2012.
[17] A. Robbin, "The loss of personal privacy and its consequences for social research". Available: http://eprints.rclis.org/handle/10760/11353, accessed on June 5, 2012.
[18] Enisa, European Network and Information Security Agency: Study on data collection and storage in the EU, 2012 .Available: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection, accessed on June 3, 2012.
[19] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf, accessed on June 6, 2012.
[20] J. Rajamäki, R. Pirinen and J. Knuuttila, Eds. *SATERISK Risks of Satellite Based Tracking* (Sample of Evidence Series, vol. 2). Helsinki: Edita Prima, 2012.
[21] L. Viikari, Ed.. SATERISK: Tutkimusraportti 2008-2011. University of Lappland. Rovaniemi: Lapin yliopistopaino, 2011. (in Finnish).
[22] Interview with J. F. Nunamaker, Jr. on "Toward a Broader Vision of IS Research", Business & Information Systems Engineering, May 2010.
[23] J. Nunamaker, M. Chan, and T. Purdin "Systems Development in Information Systems Research," Journal of Management Information Systems, vol. 7, no. 3, 1991.
[24] S. March, and G. Smith, "Design and natural science research on information technology," Decision Support Systems 15, 1995.
[25] J. VanAken, "Management research based on the paradigm of the design sciences: The quest for field-tested and grounded technological rules," Journal of Management Studies 41, no 2, 2004.
[26] A. Hevner, S. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quarterly 28, no 1, 2004.
[27] J. Rajamäki, "Law Enforcement Authorities Special Requirements for GNSS," presented in the 6th GNSS Vulnerabilities and Solutions Conference, 2012.5.21-24, Ba ka, Krk Island, Croatia.
[28] J. Ojala," Technical tracking as covert coercive measure for police to collect information", Master's Thesis, Laurea University of Applied Sciences, 2010.
[29] Finnish ministry of interior, Police barometer 2008.
[30] T. Tuohimaa, I. Tikanmäki, J. Rajamäki, J. Viitanen, P. Patama, J. Knuuttila and H. Ruoslahti, "Is Big Brother watching you," International Journal of Systems Applications, Engineering & Development," issue 5, vol. 5, 2011. [Online]. Available: http://www.universitypress.org.uk/journals/saed/20-726.pdf accessed on April 3, 2012.
[31] Kären M. Hess, Christine Hess Orthmann, Introduction to Law Enforcement and Criminal Justice, 2008, p. 1
[32] J. Jackson, et al., Trust in Justice: Topline Results from Round 5 of European Social Survey, February, 2012.

III

LAW ENFORCEMENT AUTHORITIES' LEGAL DIGITAL EVIDENCE GATHERING: LEGAL, INTEGRITY AND CHAIN-OF-CUSTODY REQUIREMENT

by

Jyri Rajamäki & Juha Knuuttila, 2013

Proceedings of The European Intelligence and Security Informatics Conference (EISIC), 2013, 198-203

2013 European Intelligence and Security Informatics Conference

Law Enforcement Authorities' Legal Digital Evidence Gathering

Legal, Integrity and Chain-on-custody Requirement

Jyri Rajamäki and Juha Knuuttila
Laurea SID,
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo, Finland
{jyri.rajamaki, juha.knuuttila} @laurea.fi

Abstract*—When carrying out criminal investigations, Law Enforcement Agencies (LEAs) apply new technology in very effective ways. However at worst, LEAs must perform many stages twice with the help of different technical tools. When investigating the identity of criminals LEAs may apply totally different technical tools than when gathering evidences for charge, because the data provided by investigating may not be valid in court. For that reason, a new monitoring system that goes beyond state of the art is needed. Three organizational layers need attentions: 1) LEA; the people that actually retrieve and store the information. 2) Prosecutors and their offices; how they get access to the information. 3) Courts; the final destination of the retrieved information. Until now, the information gathering tools for LEAs have been engineered focusing only on the best way to retrieve the information from the target. The attention paid to the legal, integrity and chain-of-custody requirements as well as social acceptance and legal oversight in connection with retrieving information has been inadequate and guidance on the matters has existed only in manuals written by legal departments.

***Keywords*—Law enforcement; Law Enforvcement Authority, Digital evidence, Forensic, Chain-on-custody**

I. Introduction

The evolution of the societies has been rapid since the industrial revolution and major changes are following each other in accelerating pace. Recently, telecommunication and computing technologies have converged under ICT and are jointly creating the platform for digital services. Internet economy and digital services will be everywhere from our houses to industrial plants [1]. However, the public sector is somewhat late in competence building, including legal competences, and only tasting the surfing opportunities of improving their operational procedures.

Increasing crime forces the Police to find more accurate evidence. When carrying out criminal investigations, Law Enforcement Agencies (LEAs) are able to obtain evidence in very effective ways that were impossible a few years ago. One remarkable aspect is that law enforcement investigations increasingly lead to very large amount (terabytes) of data [2]. Also, legislations on criminal procedures in most countries were enacted before these technologies appeared, thus taking no account of them. European Commission notes that as a result of this, three very important problems appear [2]:

"*(1) The admission in Court of evidence obtained this way is frequently uncertain, giving judges no clear criteria on its admission and assessment, and therefore causing uneven application of the law.*

(2) These new technologies can loose their efficiency quickly, as soon as criminal organizations become aware of their existence, obtain technical details about them and adopt countermeasures. The absence of standards and regulations protecting them from having to be publicly exposed during trials, burn them out as soon as they are used. This is particularly valid for criminal transnational organizations, usually having almost unlimited resources.

(3) Globalization of criminality requires the tight collaboration of the law enforcement and judiciary systems of different countries: evidence obtained in a State has to be shared and accepted in other States, while simultaneously observing fundamental rights and substantial or procedural safeguards. The lack of legislation and standards at the national and international level obviously makes this particularly difficult."

By reasons of above mentioned, LEAs need to have an easier access to all investigation data, independently from place and time and attention has to be paid to public awareness and concern on the use of surveillance equipment. LEAs apply widely gather for example multimedia data (audio, video) and tracking data from global navigation satellite systems (GNSS). The SATERISK research project [3] studied risks associated with satellite based tracking. It found the following five main challenges when LEAs are operating with new satellite based tracking technologies [4]:

1. GNSS sensors: Commercial sensors do not fulfil the needs of LEAs.
2. Cross-border operations: International nature of criminals where LEAs are national organisations.
3. Efficient secure mobile communications: An emergency inter-networking system is needed that ensures seamless operation regardless the access technology and take advantage of coverage and responsiveness of existing Professional Mobile Radios (PMRs) and broadband data services of 4G networks

978-0-7695-5062-6/13 $26.00 © 2013 IEEE
DOI 10.1109/EISIC.2013.44

for the support of both classical and enhanced emergency services.

4. Digital evidence: LEAs collected surveillance data should be valid in the court.

5. Legality control: LEAs' operations should be transparent.

The challenges 2 to 5 are valid also other technologies than GNSS. This paper concentrates on the fourth challenge; how investigation data could also be used as digital evidence at court. Today at worst, LEAs must perform many stages twice with the help of different technical tools. When investigating the identity of criminals LEAs may apply totally different technical tools than when gathering evidences for charge, because the data provided by investigating may not be valid in court.

This paper has five sections. The second section examines related work on digital evidence and their explicit and implicit objectives and assumptions on reality. The third section presents our idea and approach to build a new monitoring system for crime prevention that takes into account all three important organizational layers: LEAs, prosecutors and courts. Also, benchmarking of banking sector is suggested, because they have evidences on functional digital transactions with high inbuilt security. The fourth section discusses about the requirements, restrictions and possibilities of the monitoring system. The last section concludes this paper.

II. State of the Art of Digital Evidence

Today, computer based money transactions cover the majority of all money related transactions and the most amount of all money in the globe is digital. On the other hand, the forensic evidence is mostly based to physical evidence, such as DNA samples and testimonials. This section studies the state of the art of digital evidence. We have studied for example digital forensics, bank transaction technics and forensics based on bank transactions. At the moment, methods of economic crime investigation are most advanced. This section tells about the investigation methods that are used to resolve economic crime and how bank transactions could be used to help investigating these crimes.

Organizations have the need to collect evidence data on their networks to resolve computer intrusions, fraud intellectual property theft, sexual harassment and violent crimes. This data will be useful for the organizations when they consider legal remedies against criminals who have targeted them. To hold up in court the data must be proper which raises the expectations of computer security professionals who need to have the training and knowledge to handle the digital evidence properly. That means corporations and military operations need to respond to and recover from incidents rapidly to minimize losses that the incident has caused. But because of the number of crimes occurred the computer security professionals need to limit the damage and close each investigation as fast as possible. The rapid development in computer-related crime has created the demand for people who can collect, analyze and interpret digital evidence. This especially means preservation of digital evidence, extraction of usable information from digital evidence, interpretation of digital evidence to see the aspects of an offence. These acts are not always made by law enforcement but by corporations and single individuals. [5].

A. Digital Forensics

Computers are often used to provide digital evidence in a case because they contain lots of information. Computers can contain information about devices like USB memory sticks, cell phones, digital cameras and portable hard drives. The evidence is primarily found on a computer hard drive which consists of user accounts, log files, time stamps, images and e-mails [6].

Cell phones and cell phone service provider records include to cell phone forensics and are commonly examined due their widespread use. Cell phones contain information like contacts, text messages, images, videos, audio recordings and e-mail. Deleted data from a cell phone is possible to recover. The more computers like the cell phones are, more likely the deleted pieces of data are possible to recover. Data used as digital evidence consists of numbers that represent information of various kinds. These include text, images, audio and video [5].

Crimes of fraud committed in small businesses, large corporations, government bodies, or nonprofit organizations. Fraud is committed by individuals who take assets from other individuals or organizations. Because these acts are usually covert operations, it is hard for employers to prove how or why they occur. Frauds are investigated and prevented by fraud examiners who work on cases that involve acts as bribery, property or monetary theft [7].

Fraud investigation has its ways to examine a case. One way is to look for financial statements. This way financial statements and tax-records should be obtained. These records can be analyzed to see what are the trends and conditions of the investigated target. Investigation may go through if sales or assets have been increasing on previous year. Or maybe compare the deposits to the gross receipts reported on tax returns and the financial statements. Explanations can be sought out if inventory, liabilities or assets do not increase [8].

B. Forensic Economy Today

Forensic economists are retained for expert witness services in court. They give their input to the case by giving their professional opinion about issues, usually giving testimony at depositions, trials or other legal hearings [7]. Business entities are examined with procedures called audit programs. In these programs various kinds of evidence is collected by examiners relating to economic events and transactions. Financial evidence is collected to sort out business entities financial condition [8].

Crime investigation is hard because the environment has unclear roles and procedures [9]. Fraud investigation might rely on records that are not as precise as required. So investigation requires accurate records if the underlying trail of transactions crosses through several accounts and records [9]. Many fraud cases involve threats and crimes posed by organization insiders and are possible objects for in-house measures, only, in order to avoid public risking of the organization's brand.

Business is directed more and more towards online services. This brings big risk while consumers do credit card transactions over the Internet [8]. Today, criminals are cybercrime organizations that apply laptops and the Internet, not guns and masks [10]. One way to start an economic fraud investigating is to do an analysis of financial statements to determine at-risk accounts and make a detailed examination for them. This can include analysis of bank statements and supporting documentation. Financial statements are reconstructed based on evidence under covered and actual revenues and expenses could be confirmed. If needed, reports and supporting documentation are issued. This way evidence is sliced into logical pieces [11].

C. Collecting the Evidence

It is important to have generally accepted standards of practice and training in digital forensics because they reduce the risk of mishandled evidence and errors in analysis and interpretation. It can also prevent innocent individuals to prevent consequences of false handling of evidence data. An investigation targets to follow the trails that offenders leave during the commission of crime and to tie perpetrators to the victims and crime scenes. Tangible evidence of individual's involvement tends to be more compelling and reliable than witness' identification of a suspect [5].

While intruding a computer the attacker leaves multiple traces of their presence through the environment. That includes file systems, registry, system logs and network-level logs. It's also possible that the attackers have stolen passwords or other elements of crime that could be used to link an individual to an intrusion. The most volatile data should be collected first from the compromised computer. Volatile data is the data that has the highest chance to disappear or damage on a running system. To be more specific, this data is for example CPU registers. But because CPU registers are rarely collected, it's better to collect a memory dump first. This way no contents of memory will be compromised due to any process executed in the system [5].

While the hardware contains the evidence data, it is necessary to collect the computer in question. It's investigators choice between investigating every piece of equipment found and only essential to conserve time, effort and resources and the risk of being sued for disrupting a person's life or business more than necessary. It's also possible that the hardware size or quantity is too large to collect that it would be feasible [5].

D. Evidence Presentation

Digital evidence can be presented a written summary also called as expert reports, a well-rendered text that outlines the digital investigators findings. Expert report may not contain assumptions or lack of foundation in evidence but solid arguments by providing supporting evidence. Assertions should be supported with multiple independent sources of evidence. The report should clearly state the origin of the evidence to help decision makers to interpret the report and to enable another component digital investigator to verify results. Important items of digital evidence in a report include figures or attachments which are useful when testifying in court [5].

Expert report consists of Examination Summary, File System Examination, Forensic Analysis and Findings and Conclusions. Examination Summary bundles up the critical findings relating to the investigation. It is usually in a short form and is intended for decision makers to with short time to prepare for a decision. Examination Summary summarizes tools used in examination, the recovery of important data and elimination of irrelevant data. File System Examination covers file inventory, directories and recovered data which are relevant to the investigation. All the path names, date time stamps, MD5 values and physical sector locations on disk must be included in the examination. In Forensic Analysis and Findings the report specifies the location where each referred item was found. It helps others to verify the results in the future. Photographs, screenshots or printout of evidence can be included in this section. Conclusions references are the supporting evidence for the case [5].

E. Investigating Bank Records

When credit card fraud is investigated, the card holder information submitted will be reviewed. This may include the times of charging of the card. Among this the credit card receipts for the transactions will be reviewed. This may often be sufficient to prove a fraudulent charge. These type of investigations are unfortunately time-consuming [12].

Bank statements, cancelled checks and deposit tickets are bank records that are useful financial document when investigating a fraud. Bank records are valuable evidence while tracing the money. This kind of documentation comes from unaffiliated third party and is therefore considered very reliable. The bank documentation can be in hardcopy or digital format and it provides proof positive of how much was paid or received. The documentation points also to whom the payment is addressed, or from whom it was received. These kinds of documentation are instrumental to reconstructing the finances and determining where the money went, if a company's accounting records have been compromised [11].

Large banks have large number of bank transactions and analyzing their documents is a time consuming when the money flow is being definitely traced. Multiple transfers between bank accounts can make it hard for investigators to trace the flow of the money. Besides this the examination of bank records includes additional challenges because it may be hard to identify all active bank accounts if someone suspected of being involved in the fraud has concealed the existence of some accounts. The increased use of technology has made possible for banks to produce account documentation with a few clicks of computer mouse. The technology guarantees higher level of accuracy and reduces manual human labor in identifying the checks [11].

III. Proposed Approach

At present, many LEAs are still using point to point investigation tools and tracking systems, where the information is transmitted from the sensor to, for example, a laptop of the surveillance team for monitoring. These old-fashioned stand-alone systems create neither watermarks nor log file marks; the system only retrieves the information and stores it locally. For that reason neither chain-of-custody nor social acceptance by transparency comes true [13].

Legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way raise two problems: 1) how to ensure the accountability of law enforcement officers making use of such intrusive techniques, and 2) how to ensure that sufficient privacy safeguards are implemented to ensure that these measures are used exclusively when overriding interests prevail and in a proportionate way.

To address above mentioned problems, a monitoring system is required that will go beyond state of the art taking into consideration thoroughly the organizational and procedural interoperability. There are three organizational layers that need attentions:

1) LEA; the people that actually retrieve and store the information.

2) Prosecutors and their offices; how they get access to the information.

3) Courts; the final destination of the retrieved information.

Until now, the information gathering tools for LEAs have been engineered focusing only on the best way to retrieve the information from the target. The attention paid to the legal, integrity and chain-of-custody requirements as well as social acceptance and legal oversight in connection with retrieving information has been inadequate and guidance on the matters has existed only in manuals written by legal departments.

The banking sector is one of the most regulated sectors. However, in Europe it is completely digitized and compatible with Single Euro Payment Area (SEPA). The existing systems could be used for wide variety of event management issues or something else where various accounts can be applied; and the inbuilt security is certainly very valid asset in almost any service category [1]. In the banking sector, the requirements of digital services are very high. For that reason, it is a good area for benchmarking when most forensic evidences are moving from physical evidences to digital ones.

LEAs have developed new informal forum to team up quickly with best possible experts to counter-attack economic cyber-crime, an area where legislation far from comprehensive.

IV. DICUSSIONS

A. Requirements for the Monitoring System

Remote operation is the control and operation of a system or equipment from a remote location. In systems engineering, monitoring means a process within a distributed system for collecting and storing state data. LEAs' monitoring stations are workstations or a place in which sensor information accumulates for end-users how needs it. There must be a central control station, which collects and stores all the information according to the rules and provides also legality control. The real time information will be sent on demand to the end-user where ever he or she is. In many cases, the users of information are not in the office but in the field using portable devices. This is called front deployed knowledge. Monitoring systems should be able to combine multiple forms of information, temporal, spatial, audio and visual, etc. However, combining information from many sources is technically, operationally and legally difficult task and analysing is suffering from it [4].

Safety, encryption and availability of the data are very important. Information must be understandable and collected in a trusted way. Data needs to be available in spite of location but you need to be aware of the law when handling data. Integrated multimedia sensor systems collect data and they must be more miniaturized, sustainable and low power.

Data must be reliable and must include position marks and time stamps where, when and by whom the data is produced. Multimedia file must contain all the information but it is needed to be compress to as small as possible. Video and sound data always includes information when and where data is generated. All this information must put together as a one file. So you don't have to search different information from various systems.

B. Restrictions of the Monitoring System

The gathering, conservation, communication and presentation of the computer-derived evidence must fulfill legal requirements with regard to the admissibility of the evidence; they should be admissible, authentic, complete, reliable and believable. Electronic evidence not gathered in accordance with the law will be inadmissible and be ruled out of court. Today's main evidence authentication system is the hash value calculated from the retrieved information. With hash value you can prove that the data is the original and no one has tampered with it. The problem is that systems like hashing are incapable to fully expose when, where and by whom data is produced [4].

Life cycle of the data is also important thing and has to be included when designing systems. This has leaded to a situation where commercial systems are preferred in the field because they are selling better.

With regard to tracking devices, many problems occur. For better quality devices need to be big and for that reason power consumption comes too high. Bigger size also makes tracking devices more easily exposed. Smaller devices with lower power usage mean lower quality. But lower quality is out of the question. At the moment there are no devices that can support cross-over platforms for positioning and communications. It is easy to interrupt tracking devices because they don´t have built-in alarm features. Tracking device's own time is not trustworthy because it can be easily modified. When position and time comes from satellite, makes it more reliable.

C. Possibilitie of New Digital Services for Crime Prevention

In order to bringing about the LEAs' special requirements for digital evidence, technological and socio-technical research and development work is needed. Development of novel monitoring systems and new sensors improves LEAs' evidence-gathering abilities while respecting legal and ethical expectations of society. The over-all development target will be accomplished through the following specific objectives:

1) to enable new operational models for investigation for LEAs by improving existing technology and developing new integrated digital services for tracking and audio and video retrieving and monitoring.

2) to develop methods of working that are legally binding and social acceptable; information gathered is legally binding and court proof developed technology will enable audit trail, accountability and further societal acceptance

3) to support wider European goals, such as recognizing the needs for regulation and harmonization, and promoting the use of other European technologies like Galileo and create needed interfaces.

D. Benchmarking of Banking Sector

Despite all challenges, bank documents bring huge value providing the proof of who of what company paid or received money. This evidence consists of forged signatures or endorsements, fake company names or people. Investigating this kind of evidence may lead to other clues that may help unravel things. [11]

Economic crime investigation has always relied on known scenarios of economic crime. For example, when a gang of cybercriminals stole \$45m by hacking into a database of prepaid debit cards and draining cash machines around the world, law enforcement agencies in Japan, Canada, the UK, Romania and 12 other countries were involved in the investigation [10]. Economic crime still follows it roots using methods known for ages. By using the technology created to provide bank transactions it´s possible to use these get more into details of crime.

This paper shows that investigating bank transactions can be challenging but it provides very useful and reliable financial documents when investigating a fraud. With modern technology it is possible to get reliable and accurate digital evidence for economic forensics.

E. Legislative and Political View

The focus of this paper has been in the latest technological developments in crime scenes, which are framed by societies' laws and practices. On the legislative and political level several nations are taking steps to enhance Law Enforcement Authorities' possibilities and readiness to tackle "not so entirely new" ways and means of transnational crime, which is put into historical perspective [14] by Political Science Professor Peter Andreas:

"The particular smuggling activities and policing priorities will surely shift over time, as they always have, but it is safe to predict that the centuries-old illicit trading tradition will survive [15]. This is now fueled by the United States´ addictions to cheap immigrant labor and mind-altering substances. The United States will make little progress if policymakers continue to see these problems as primarily rooted in transnational crime, rather than in outmoded labor-market regulation, a dysfunctional immigration system, an overly punitive drug-control system, and failures in education and public health policy."

International warehouses of crime route their activities into the most lucrative avenues. One can say that nation states are responding with slower pace in an almost respective manner: Wassenaar [16] and Prum [17] type and bilateral agreements are made in a relatively ad hoc manner outside international bureaucracies on purpose giving more international lee-way to LEAs. This has and will be facilitated by the newest technical principal and applied research. Therefore, researchers should approach LEAs in order to address real problems while drafting their research agendas and politicians when disseminating their results, too.

V. Conclusions

Forming the basis for the technological development concentrating on the development of new sensors, monitoring stations and their communication channels for LEAs, this paper will contribute towards the operational environment and different phases of chains-of-custody applied in different countries. This will be done by adding a legal / societal layer on the technological development and by developing mechanisms and recommendations that will enable safeguarding the accountability, legality and social acceptance of the developed technologies. In this regard, two research tracks should be developed: 1) Procedural safeguards and 2) data protection safeguards from "privacy-by-design" to "accountability-by-design". Procedural safeguards will ensure the transparency (for purposes of accountability of law enforcement officers) of investigation techniques use. Specific attention should be paid to privacy safeguards. In data protection safeguards specific relevance should be given to the introduction of accountability mechanisms into the design of the system.

The new monitoring system should go beyond state of the art taking into consideration thoroughly the organizational and procedural interoperability. There are three organizational layers that need attentions: 1) LEA; the people that actually retrieve and store the information. 2) Prosecutors and their offices; how they get access to the information. 3) Courts; the final destination of the retrieved information. Until now, the information gathering tools for LEAs have been engineered focusing only on the best way to retrieve the information from the target. The attention paid to the legal, integrity and chain-of-custody requirements as well as social acceptance and legal oversight in connection with retrieving information has been inadequate and guidance on the matters has existed only in manuals written by legal departments.

The monitoring system should enable a use process where the fulfillment of legal oversight requirements is possible in all phases. In practice this means that we are no more building equipment that someone is using and the output of which is used in part in courts. Instead, we are creating a total solution that creates an auditable log for every phase of the process. Following this, the tools do not start operating when a battery is installed in them but the tools are always connected to the authority's central system that gives them the permission to operate. The authority giving the operation permission has to connect to the system always via authentication, which creates a log mark on who gave the permission into the system. As long as sensors are capable to operate without authenticated permission token, there is no means for controlling their use. The new kind of a monitoring system will be able to present publicly accepted auditable log-based proof of correct use of the equipment. This will be done with publicly proven technical control methods involved in the command chain. It does not only give tools for LEA, but also important building stones to more open society with built in oversight and legal audit systems [4].

Submitting electronic evidence before a Criminal Court as evidence means it should have all attributes of conventional evidence, i.e. that it must be admissible, i.e. it must conform to legal rules to be put before a court; authentic, i.e. it should be possible to positively tied evidentiary material to the incident; complete (as much as possible); reliable, i.e. there must be nothing about how the evidence was collected and subsequently handled that casts doubts about its authenticity and veracity; and believable, i.e. understandable by a Court [18].

The information created for LEAs by the sensor is always multi sensor information, i.e. the video or sound always include the data on its production time and place, which can be checked based on the geometry of the positioning satellites. The mere time stamp based on the tool's own clock is not reliable as they can be changed. Furthermore, the system always calculates the hash value from stored data that safeguards the unchanged character of the original data. All log information can be sent in an encrypted form to LEAs or even to courts of justice to whom the LEA can provide the encryption key for oversight purposes. All information created by the system will be encrypted as inserting unencrypted information into public networks endangers the subject's privacy in a way not allowed by law for LEAs.

REFERENCES

[1] R. Paajanen, P. Kuosmanen, J. Talvitie and J. Juopperi, "Digital services – The next boom – White paper,Tieto- ja viestintäteollisuuden tutkimus TIVIT Oy. Available: http://www.tivit.fi/digitalservices

[2] European Commission C (2012)4536 of 09 July 2012, "Work programme 2013, Cooperation, Theme10, Security." Available: ftp://ftp.cordis.europa.eu/pub/fp7/docs/wp/cooperation/security/k-wp-201301_en.pdf

[3] J. Rajamäki, R.Pirinen and J. Knuuttila (eds.) *SATERISK: Risks of satellite based tracking,* Sample of evidence series volume (2), Edita Prima: Helsinki 2012.

[4] J. Rajamäki, J. Tervahartiala, S. Tervola, S. Johansson L. Ovaska and P. Rathod, "How Transparency Improves the Control of Law Enforcement Authorities' activities?" in *Proc. of European Intelligence and Security Informatics Conference*, August 22-24, 2012, Odense, Danmark.

[5] E. Casey, *Digital Evidence and computer crime: Forensic science, computers and the internet*, Academic Press, 2011.

[6] L. Daniel and L. Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*, Elsevier, 2012.

[7] S.Echaore-McDavid, R.McDavid, *Career Opportunities in Forensic Science,* Infobase Publishing, 2008.

[8] G. Manning, *Financial Investigation and Forensic Accounting*, CRC Press, 2010.

[9] K. Pickett, J.Pickett, *Financial Crime Investigation and Control*, John Wiley & Sons, 2002.

[10] BBC News US & Canada, "Cybercriminals 'drained ATMs' in $45m world bank heist", 9 May 2013 [online]. Available: http://www.bbc.co.uk/news/world-us-canada-22470299

[11] T.Coenen, *Expert Fraud Investigation: A Step-by-Step Guide*, John Wiley & Sons, 2009.

[12] V. Fox. (2013). "How Do Banks Handle Credit Card Fraud?" [Online]. Available: http://smallbusiness.chron.com/banks-handle-credit-card-fraud-12537.html

[13] P. Viitanen, P. Patama, J. Rajamäki, J. Knuutila, H. Ruoslahti, T. Tuohimaa, and I. Tikanmäki, "How to Create Oversight in Intelligence Surveillance". [Online]. Available: http://www.wseas.us/e-library/conferences/2011/Meloneras/ACELAE/ACELAE-07.pdf accessed April 5, 2012.

[14] P.Andrea: *Smuggler Nation: How Illicit Trade Made America*, Oxford University Press, 2013.

[15] P.Andreas "Gangster´s Paradise, The Untold History of the United States and International Crime" in *Foreign Affairs,* Vol. 92, Nr. 2,2013.

[16] Wassenaar Arrangements [online] available: http://www.wassenaar.org/

[17] B. Prainsack and V. Toom, "The Prüm Regime: Situated Dis/Empowerment in Transnational DNA Profile Exchange", in *The British Journal of Criminology*, Volume 50, Issue 6, 2010.

[18] O.Leroux, "Legal admissibility of electronic evidence," International Review of Law Computers & Technology, vol.18, pp. 193–220, July 2004.

IV

SATELLITE BASED TRACKING SYSTEMS FOR BETTER LAW ENFORCEMENT: A SYSTEMS ENGINEERING EXPLORATORY RESEARCH VIA A MULTIPLE CASE STUDY ANALYSIS

by

Jyri Rajamäki, 2014

WSEAS Transactions on Systems and Control [In review]

V

DECENTRALIZED FULLY REDUNDANT CYBER SECURE GOVERNMENTAL COMMUNICATIONS CONCEPT

by

Jyri Rajamäki, Paresh Rathod & John Holmström, 2013

Proceedings of The European Intelligence and Security Informatics Conference (EISIC), 2013, 176-181

2013 European Intelligence and Security Informatics Conference

Decentralized Fully Redundant Cyber Secure Governmental Communications Concept

Jyri Rajamäki and Paresh Rathod
Laurea SID, Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo, Finland
{jyri.rajamaki, paresh.rathod} @laurea.fi

John Holmström
Ajeco Oy (Inc.)
Arinatie 10, FI-00370 Helsinki, Finland
john.holmstrom@ajeco.fi

***Abstract*—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.**

***Keywords—* critical communications; public safety communications; distributed dystems intercommunication protocol**

I. INTRODUCTION

European Defence Agency (EDA) was established to enhance European defence capability, especially in the fields of crisis management to help European Union (EU) nations and council. The broad goals of EDA are to sustain the European Security and Defence Policy in the present state and develop it to keep it up-to-date. EDA must ensure coordination and synergy with member states and European investment to enhance and update capabilities in civilian security [1]. It is common practice in EU nations to use military and civilian defence actors during crisis management and operations. The partnership ensures safety and security of EU residents and citizens. Researchers have often observed an overlap of military and civilian functions. Especially, in the areas of communication, information gathering, command and control operation. Increasingly the research, development and innovation in technology based on 'dual-use' requirements provided by both civilian and military actors [1].

Critical infrastructure protection (CIP) is the analogous shared concern and responsibility. Water, power, finance, Internet, transport and all communication systems are part of the critical infrastructure (CI) and are essential to daily activities. Hromada's study [2] suggests that private industry owns and operates the majority of CI assets. Government serves as a regulator and consumer but often has a limited role [2]. The various CI components are to varying extents dependent upon one another within a country's borders and internationally. As such, problems in one CI component can quickly spread to others [3]. An operation of most CIs rests simultaneously and partly on their own dedicated communication systems as well as commercial networks.

In recent years, the capabilities of Public Protection and Disaster Relief (PPDR) organizations across Europe have significantly improved with the deployment of new technologies including dedicated Terrestrial Trunked Radio (TETRA) networks. Nevertheless, a number of events like the London bombing in 2005, the Schiphol airport disaster in 2009 and the flooding disasters in 2010-11 have highlighted a number of challenges that PPDR organizations face in their day-to-day work. Secure and reliable wireless communication between first responders and their Emergency Control Centre is vital for the successful handling of every emergency situation. This also applies to each connected respondent including Police, Fire, Medical or Civil Protection [4].

PPDR, CIP and MIL organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe but also enable collective responses to threats and crisis in an increasingly interconnected network. In addition, the organizations stand to gain from interoperability functionality in their routine work. On one hand, Europe is a patchwork of languages, laws, diverse cultures and habits that can change abruptly across borders. On the other hand, even in the same country, each security and CIP organization develops its own operational procedures. For efficient operations, many serious challenges need to be addressed, including critical governmental communication systems (not compatible even when they use the same technology), differing procedures as well as inadequate language skills in cross-border cooperation. This paper addresses not only the technical challenges of security and interoperability, but also the strategy to build a redundant critical governmental communication system for a multi organizational environment; enabling external users to collaborate towards keeping the intrinsic and vital cyber security mechanisms of such networks. Our paper presents a

978-0-7695-5062-6/13 $26.00 © 2013 IEEE
DOI 10.1109/EISIC.2013.39

solution based on the Distributed Systems intercommunication Protocol (DSiP).

II. Gaps in State of the Art

A. Communication Concept of the Finnish Government

Finland is globally known for its high-tech information society. To meet the requirements of any society characterized as an information society needs secure ICT systems; that fulfills the prerequisites of businesses, government and citizens. Obvious scenario leads to synchronize services with the available diverse network and information system services. They are optimized for the objective in question and must complement each other. The communication concept of the Finnish Government consists of many different networks that can be roughly divided into four different levels of preparedness. First, the Defence Forces' strategic communications have the highest level of preparedness and, also, highest budget [5]. 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, defence forces, police, rescue units, and border guards. TUVE is a Finnish project aiming to implement 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 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 [5], [6]. However, dedicated secure data network used by the state officials cannot be ubiquitous and suitable for all the needs that are vital to society. Therefore, the third level government's common secure communications requirements are mostly realized by 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 concerning Finland's security. The forth level consists of commercial networks and it has 60 000 governmental user [7].

Finnish TETRA-based PPDR network VIRVE is fully operative since 2002 with full domestic interoperability. It has 1350 sites all of which are electromagnetic pulse (EMP) protected with back-up power supplies. Statistic shows the pool of users including oversized consumers like rescue services with 33 percentage, police and military with 21 and 15 percentage respectively, social and health services with 13 percentage. There are also small consumers like border guard, customs, air traffic-SAR, other authorities with 5, 2 and 1 percentage respectively. Rest is used by other individual and organizations [8]. Every week, VIRVE transmits 800,000 group calls and 32 million short data service (SDS) messages [8]. The Finnish experience shows that GSM networks were overloaded during emergency situations. It is noticed in high school massacres in 2007 and 2008 and summer storms in 2010, whereas, the VIRVE network was operating normally.

Mobile data is essential within PPDR field operations. As a result of increasing cooperation between PPDR organizations, more data will be transmitted. In the near future, Finland is developing several new data systems for PPDR in the year 2013-2015 [8]. These systems are: 1) joint command and control system, 2) joint data system for investigating authorities and 3) joint field-command application. These systems will increase transmission of situational pictures that will result in data transfer demand. The master plan in Finland is to close fixed police stations and create a mobile office concept for police, which also means more data transmissions. According to Finnish authorities, the demand for data transmission has increased several folds in recent times and their experience demands the dedicated PPDR mobile data network [8]. Such future network should be independent of every single public mobile network technology to serve highly demanding needs.

B. IP Protocol and Multichannel Commmunication

Multichannel communication is a method for simultaneously using several communication paths provided by various telecom operators. Multichannel communication means parallel use of data channels regardless of technology. For end-user applications, all the multiple parallel communication paths should appear as a single uninterruptable path. People can use parallel communications paths simultaneously if they want; they can collect and integrate information coming from different sources. However, computers are technically not able to do this even if they 'would want to do' because the IP protocol used for data transfer cannot bind a socket over two or more physical connections simultaneously. That is first gap in multichannel communication: IP is not 'good' at multi-channeling. On the one hand, creating a multichannel communication solution utilizing Virtual Private Network (VPN) technique solves some problems; on the other hand, it ties the solution to the VPN system. The real challenge is VPN solution covers only a fraction of the total need.

The IP protocol has poor control of priority, and services should adjust to the physical transfer capacity. For that reason, low capacity lines can transfer only high priority data.

All centralized solutions are vulnerable to many threats, such as e.g. denial-of-service (DoS) attacks, system failures, repudiation, spoofing, tampering. Wherefore, decentralized modular communication and information management systems should be used; if one part goes down, other part works. Also, turning to the services of a single operator is a risk. Utilizing parallel connections of multiple operators ensures connectivity, minimizes risks and maximizes reliability.

C. Cyber Security and Qaulity of Service (QoS)

It is undeniable that the communication of military and security authorities must be secured. Modern CI includes not only physical components and hardware, but also software, services and intellectual properties. These integrated systems are examples of cyber–physical systems [9]. The term 'assurance' has many similarities in the context of CI than of traditional communications assurance [3]. Information assurance consists of five services: confidentiality, integrity, authenticity, availability and non-repudiation. Consider the water supply, availability is the first requirement, but integrity is an additional concern. Integrity ensures that it has not been tampered or contaminated with, remains in original state. The health care industry must consider availability, integrity, authenticity and non-repudiation. The security needs of CI follows assurance model of traditional information security [3]. By now, some of these challenges are known and receiving attention from the research community and governmental agencies; e.g. the European Network and Information Security Agency (ENISA) is such an organization

As critical governmental communications becomes more digitalized, there are significant risks and threats. Traditionally, there are 'conventional' concrete challenges, such as natural phenomena, strikes, disruptions, war, information security problems, which have fairly stabilized range of means. These conventional challenges are already affecting Quality of Services (QoS). In addition, there are 'new' challenges concerning intertwined risks and threats caused by cyber security problems, changes in ownership of telecommunications infrastructure, globalization of systems and business operations, extensive outsourcing chains and other changes in working structures [6]. The recent report published by US government citing 782% increase in reported breaches of federal agencies security in last 6 years [10]. Recent study also shows that growing threats of disruptions to operations for government organization rely on information sharing amongst their employee, partners, agencies and civilians [11]. The mightiest challenge in the current situation remains to protect CI, especially against the consequences of rapid changes and turning points. Meeting these challenges also assures superior Quality of Services [6].

D. *Interoperability and Multi Organizational Environment*

In major disasters, not a single PPDR organization can work alone. Hence, co-operation is extremely critical between actors. The working parties should not simply trust and rely on their own resources. Even though, few organizations possess all the required areas of expertise in a large-scale incident and disaster. Information sharing and education at the organizational level is required in order to achieve a working relationship between the actors. This means the actual and operational interoperability between the first responding organizations; also in reality and in the field – not only in the form of an official agreement [12] but much larger.

PPDR, CIP and MIL actors, have multiple similar needs. . Lapierre's research [1] suggests that similarities in disaster relief operation scenarios include a) severe disruptions in expected functionalities of critical infrastructures, e.g. transport, supplies, infrastructures, b) operations in remote areas without transmission infrastructures, c) cross border operations and multinational teams, d) high demand for interoperability, e) no remaining infrastructures after a serious disaster, f) congestion or no use of commercial networks, and g) utilizing both AdHoc networks and stable infrastructures. Similarities in command and control communications involve 1) want to obtain information on the operational environment, 2) need for the decision maker to monitor operation (live feed), 3) need to examine and issue orders, and 4) want to assess the progress of the operational environment after order [1].

With respect to European mission-critical public safety communications, TETRA or TETRAPOL is widely used and recommended, and there are no other improved standards available at the moment. Data transmission over TETRA is rather slow and does not fulfill future needs. However, it is extremely reliable even though its low capacity communication. Wideband data (TEDS) is an effort for improved data services but falls short to current and future needs. However, a dedicated PPDR mobile data network independent of public mobile networks may not be available in Europe until 2020. The current situation needs complementary technologies in addition to TETRA. Research suggests the multichannel communications would solve the problem. There is a global demand for safe and secure multichannel communications and it expanding day by day.

III. Multipurpose Secure Communication Network

A. *Distributed Systems intercommunication Protocol – DSiP*

DSiP forms multiple simultaneous communication channels between the remote end and the control room; if one communication channel is down, other channels will continue. DSiP makes communication reliable and unbreakable using various physical communication methods in parallel. Applications, equipment and devices can communicate over a single unbreakable data channel. Satellite, TETRA, 2G/3G/4G, VHF-radios and the other way can be used simultaneously.

DSiP manages selection of communication channel and overcomes link establishment issues. DSiP solves incompatibility issues and is an invisible layer to all applications, hardware and software. It provides modularity, data integrity, security and versatility to data communications systems of any size. The DSiP software uses both IP and non-IP based communication links when required. DSiP is capable of converting classical polled systems into event driven function. This feature improves response time and speed. DSiP also contains compression of data which is useful with low capacity communication channels [8].

Virtual Private Networks (VPN) can be tunneled through the DSiP communication system. This feature makes it possible to maintain constant communication without re-authentication even though one communication channel would

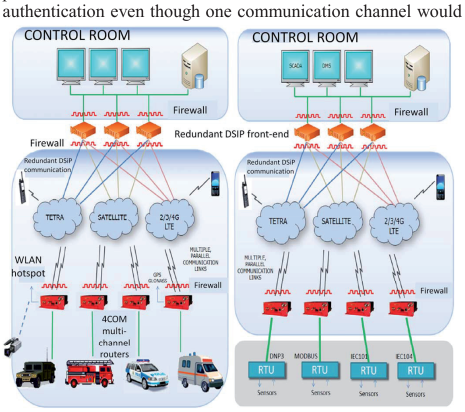


Fig. 1. Fully redundant PSC (left) and SCADA (right) networks

be at fault. The DSiP telemetry system brings many significant benefits and useful functions. DSiP system 1) increases reliability and security, 2) is resistant to network Denial of Service (DoS) attacks, 3) decreases the risk for viruses and malware, 4) results in less system downtime and lower maintenance requirement, 5) contains authenticated and encrypted communication, 6) allows connections to TETRA- and mobile handsets, 7) has the capability of interfacing to many different kinds of hardware and software like radar, AIS, Radio Direction Finders, CCTV equipment, 8) is a transparent communication of DNP3, IEC101/104, MODBUS, NMEA and other protocols, and 9) includes network monitoring and management tools improving overall system performance.

Mobile multichannel communication improves communication reliability and quality, for example, in PPDR applications. Police cars, ambulances and fire engines benefit from uninterruptable secure communication. DSiP provides a uniform, reliable and maintainable communications services platform capable of withstanding time. The system is not dependent on any particular telecom operator's services or communications protocols. Figure 1 (left) demonstrates redundant public safety communications (PSC) using DSiP. Figure 1 (right) illustrates fully redundant data networks for SCADA communications utilized by DSiP. There are layer of components including Remote Terminal Units (RTU), secure network routers and switches, communication frameworks like TETRA, satellite, LTS and others that connect with command and control center using DSiP front-end hub. The secure routers and switches carried advances hardware and software firewalls to ensure high degree of security. The sensors allow communication channel to connect with RTUs. Secure routers and switches establish multiple parallel communication links to communication framework equipment where layered firewalls implemented on redundant DSiP front-end. It ensures secure

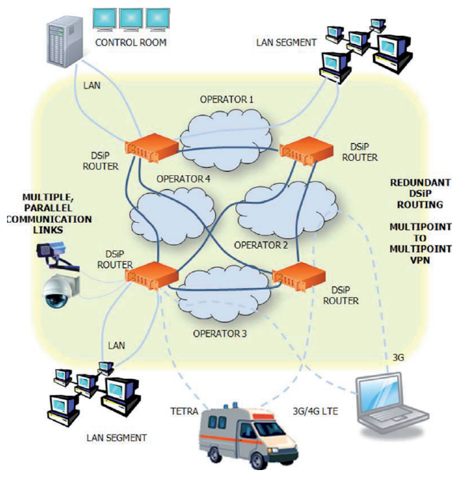


Fig. 2. Decentralized multipurpose cyber secure communications network

communication connections with command and control room.

DSiP is currently in pivotal use by the Finnish Frontier and Coast guard in a coastal surveillance application, by Fingrid Oyj for controlling Finlands main power grid, and by Elenia Verkko Oy (former Vattenfall Verkko) for controlling and operating the mid-voltage power grid.

B. Qaulity of Service and Cyber Secure Communications

IP traffic and its packets have methods for controlling priority and quality. The IP QoS is either not supported at all, or supported in non-conforming ways, in operator traffic. Customers using DSiP have enhanced controlling possibilities for the data flow and traffic including 1) control priorities – important information is routed first, less important later, 2) control over network timeouts – no undetermined delays or waits, 3) control the usage of communication and bandwidth – DSiP always ”knows” the condition of all routes, 4) have better control over maintenance and configuration, 5) the DSiP telemetry system has built-in congestion control, and 6) routing services based on cost-factors enabling certain, less important traffic to be filtered, e.g. the used low capacity communication.

The decentralized architecture based on DSiP is highly fault-tolerant in normal conditions as well as in crises as demonstrated in Figure 2. 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 to build a practical and timeless cyber secure data network for multi organizational environment, which being fully decentralized and 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. Proposed solutions using DSiP achieves cyber security objectives mainly, prevents cyber-attacks against critical communications channel, reduces vulnerabilities against current network infrastructure, and minimizes damage and recovery time if cyber-attack realizes [13].

In September 2012, Louhi Security Oy security audited the DSiP solution with 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, DSiP system provides a high level of reliability and security for applications demanding uninterruptable communication and extended usability.

C. The DSiP Solutions – Key Elements and Functionalities

As earlier mentioned, the DSiP is entirely a software protocol solution. There are fundamentally two types of software elements in the solution: DSiP-routers and DSiP-nodes. Figure 3 depicts the blueprint of DSiP solutions. The nodes constitute interface points (peers) to the DSiP routing solution, and the DSiP-routers drive traffic engineering and transport in the network. DSiP routers establish multiple authenticated and encrypted, sometimes parallel connections according to configuration parameters, between each other. Nodes establish multiple simultaneous connections to one or more routers in the system. All connections may be strongly encrypted and trustworthy based upon usage of certificates effectively meaning that all elements in the DSiP routing solution are known. As routers may use multiple parallel connections between each other and as nodes may make multiple parallel connections between themselves and one or more routers, the solution results in a true mesh-like structure between the network peers (nodes).

DSiP-routers in the routing network are typically distributed to different physical locations. The nodes are typically located at, e.g., but not limited to, emergency service vehicles and control rooms. The connection establishment is always constructed from the node towards the router element and one router to another router in a preconfigured manner. The system features a third element named configuration server software from where nodes may read new configuration data should the underlying physical transport layer request changes or configurations needed to be done.

The nodes and routers maintain multiple parallel physical connections between each element in the DSiP routing solution. That removes this complex burden from external equipment and software that use the system as routing. Consider e.g. a vehicle computer in an emergency service vehicle. This computer either contains a DSiP-node which uses multiple wireless modems, or it connects to a vehicle router-hardware containing the DSiP-node and multiple modems. The DSiP-node is performing tunneling of the users applications IP-traffic from the vehicle to the control room and vice versa, thus mitigating complex issues routing in between network peers. The DSiP solution is capable of transparently maintaining the connections and communications between users' systems or applications or hardware without having to program this functionality into the applications – DSiP is fully transparent to its users. For example, a user may run VPN client software in his laptop. The nature of the VPN demands that it must establish its connections over a single physical communication line. If this line has a problem or breaks up, the user must re-authenticate his or her VPN session over another physical media. When DSiP is used, the user may use his or her VPN client or server to establish a VPN session over multiple physical connections – should one or more have problems, the VPN session remain intact as the DSiP is tunnels the session through itself. This feature is of utmost importance in critical applications.

Another extremely essential aspect of critical networks is their sustainability and handling of Denial-of-Service (DoS) network attacks. As the communication in the DSiP routing solution is based on multiple connections over multiple physical media, it is not sensitive towards DoS-attacks as there will always be "some route" between the network peers. It is highly unlikely that an attacker would, and could, attack all elements in a heterogeneous network simultaneously.

The transport layer in the DSiP routing solution may be IP networks. However, DSiP is not limited to use IP – it may use proprietary, non-IP networks, as well. This feature adds to the security and robustness of a DSiP routing solution. The DSiP may interconnect peers in an IP network by using non-IP connections. In addition to the aforementioned, DSiP is a tunneling protocol. It may interconnect so-called 10-based IP networks over regular teleoperator service provider's IP networks although 10-networks are not routable regularly.

The DSiP-network and solution contain de-centralized authentication server software (no credentials are stored at the routers) mitigating the complex task of providing access to peers. In addition to this, the DSiP-network management server software provides reports and material over DSiP-node accesses, transported number of bytes and detected link latencies which all are useful information to the system maintenance team. A DSiP-node can be constructed in native programming languages (e.g. C, C++) and Java. The latter provides typically an easy path for creating DSiP-based applications in, for example, mobile handsets.

All addressing in DSiP is based upon individual node-organization, and routing-cloud-numbers. Ending points in DSiP routing solutions do not need to "know" the IP-addresses or locations of its counterpart. The addressing scheme in addition, to a concept called DSiP-translation barrier makes it possible to interconnect users from different organizations having different IT-policy statuses because the DSiP may constitute a service providing network and not just a "pipe" or "tunnel" from one network to another. The translation barrier functionality residing in the DSiP-nodes may be used for

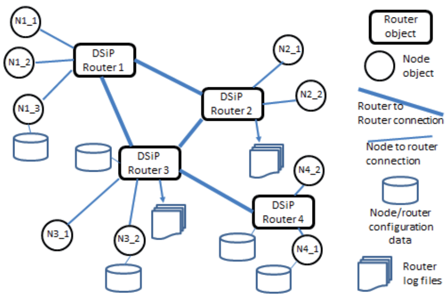


Fig. 3. Blueprint of DSiP network solution

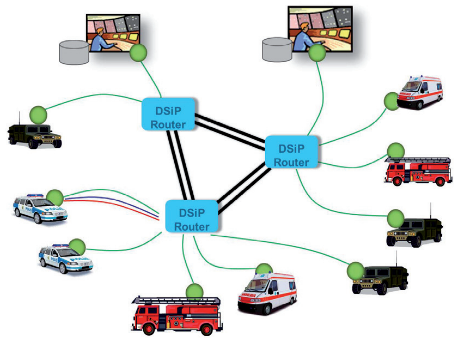


Fig. 4. Multi-user DSiP network solution

fetching data from core networks and filtering access to the core in much the same way as HTML and PHP are used in browsing applications. A typical multi-user, multi-policy, DSiP routing solution may look as in Figure 4.

Maintaining an IP network is a tedious and many times difficult task involving thorough understanding of IP-firewalls, switches and routers. It is many times highly risky to parameterize a firewall as a faulty firewall rule may endanger a complete network. The DSiP solution mitigates this task. The IP network maintainer or creator may set-up his or her network, tune firewalls and routers locking the tested/hardened IP-routing. Then the DSiP can be used as a logical traffic-engineering layer on top of the robust IP-network.

IV. Discussions and Conclusions

The nature of secure and reliable critical communication depends on serving actors; e.g. Figure 5 shows the difference of demands between tactical military communications and civilian PSC. Let us see a scenario where an electricity transmission system operator detects a problem in the main power grid, the load and power plant must be disconnected in milliseconds. This hellish requirement demands the proprietary communication channels. Most other PPDR, CIP and MIL users can rely on a regular telecom operators' latency but, not on the performance of a single operator. The communication should use parallel distributed communication channels because it must be failsafe and unbreakable.

From the investment point of view, the technical solution must withstand time, avoiding 'painting self into the corner'. The exceptional circumstances that should be taken into account include that the telecom operator may not always be there. That surveillance, command and control data should move even though the IP-network would not be available. Cooperation amongst various actors is becoming more valuable due to aforementioned reasons. Organizations may have different operational statuses, but the communication solution should support each other, and not suppressing any cooperation. The customer should have the freedom of choices, being the 'master' of his application. This cannot be assigned to any telecom operator or vendor because situations change constantly and the selected communications architecture should bend to the needs, not vice versa.

The nature of a crisis event affects the usable media. During a panic event, public cellular technology is useless. The public cellular data is highly loaded during minor event with a large crowd, but dispersed communication may get through. In a

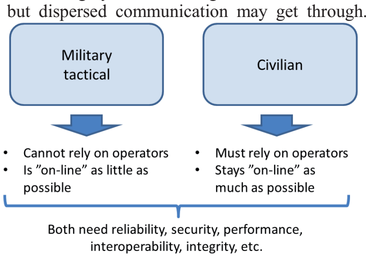


Fig. 5. Difference of demands between military and civilian communications

case of the oil disaster within large geographic area, cellular technology is operative and interoperability required. TETRA works in all circumstances, but the data capacity is limited. TEDS will bring some improvement, however, may fall short to future needs. Satellite communication can be considered pretty advantageous. The 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, while on the other hand, it supports redundant and secure way of communication. 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 they would be a single connection channel; thus eliminate the modification of any application or device.

References

[1] G. Lapierre, "Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU?", PSC Europe Conference, 7-8, Brussels, June 2011.

[2] M. Hromada, "Resposibility of the operator of European Critical Infrastructure", Security Magazin, vol. XVII, No. 95, pp. 52-55, May 2010.

[3] R. George, "Critical infrastructure protection", International Journal of Critical Infrastructure Protection, vol. 1, pp. 4–5, December 2008.

[4] M. L. Goldstein, "Various Challenges Likely to Slow Implementation of a Public Safety Broadband Network." GAO-12-343. Washington, D.C.: February 2012.

[5] Y. Benson. (2011, March 2). *Authority IT serving national security*, VIRVE Day -seminar, Helsinki, Finland. Available: http://www.erillisverkot.fi/public/files/Authority IT serving national security_Benson.pdf

[6] K. Manni. (2011, March 2). *Security communications – possibilities and challenges*, VIRVE Day -seminar, Helsinki, Finland. Available: http://www.erillisverkot.fi/public/files/Security communications – possibilities and challenges_Manni.pdf

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

[8] H. Riippa, "The future of PPDR networks in Finland – Requirements and options", presentation in the EU workshop on The future of PPDR services in Europe, Brussels, Belgium, March 2011.

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

[10] L. Hawes (2013, March 27). *Cybersecurity and the Threats to Networked Business, Forbes Magazine*. Available: http://www.forbes.com/sites/larryhawes/2013/03/27/cybersecurity-and-the-threat-to-networked-business/

[11] J. Snyder, P. Mattingly (2013, March 18). *U.S Lawmakers Warns for Security Threats from Cyberattacks.* Available: http://www.bloomberg.com/news/2013-03-17/cyberattacks-increasing-risk-to-u-s-national-security-economy.html

[12] R. Akella, H. Tang, B. M. McMillin, Analysis of information flow security in cyber–physical systems, International Journal of Critical Infrastructure Protection, vol. 3, Issues 3-4, 2010, pp. 157-173.

[13] Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", European Commission, Brussels, February 2013.

VI

MOBILE DIGITAL SERVICES FOR BORDER PROTECTION: STANDARDIZATION OF EMERGENCY RESPONSE VEHICLES

by

Jyri Rajamäki, 2013

Proceedings of The European Intelligence and Security Informatics Conference (EISIC), 2013, 256-261

2013 European Intelligence and Security Informatics Conference

Mobile Digital Services for Border Protection

Standardization of Emergency Response Vehicles

Jyri Rajamäki
Laurea SID,
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo, Finland
jyri.rajamaki@laurea.fi

***Abstract*—Law enforcement authorities (LEA), such as border guards, suffer from intensive human involvement. Due to the economic situation, the main need of LEAs is to maintain their core services with significantly reduced budgets. According to our multi methodical development research, the only realizable solution is the better piggybacking of information and communications technology (ICT) and digital services. This also means in field operations and thus in emergency response vehicles (ERV), ICT applications and digital services play a more and more important role. This paper presents a new layered approach for standardizing the electrical, electronic and ICT devices of ERVs. Thus on the basis of this infrastructure, the mobile digital services needed for public safety responders could be supplied.**

***Keywords*—Law enforcement, Digital services, Public safety, Border protection, Standardization, Emergency response vehicle**

I. INTRODUCTION

Traditionally border protection consists of border troops and security checkpoints. Border troops include many border patrol agents in vehicles (cars, snowmobiles, helicopters, etc.) or on foot to patrol areas searching for intruders. Once intruders are detected, the patrol agents must switch tasks and attempt to arrest the intruders [1]. The Border Guard uses both permanent and temporary security checkpoints, where all vehicle traffic is stopped in order to detect and apprehend illegal aliens, drugs, and other illegal activities. Permanent checkpoints are generally located on international roads, while temporary checkpoints are located on smaller arterial and rural streets [1]. Each border troop watches and controls a specific section of the border [2].

Traditional border protection systems suffer from intensive human involvement. Recently, new high-tech devices (unmanned aerial vehicles, unattended ground sensors, surveillance towers equipped with camera sensors, etc.) have been put into operation. However, any single technique encounters inextricable problems (high false alarm rate, line-of-sight-constraints, etc.) [2]. Also, most new digital security services are supplied via stand-alone systems without in-built interoperability. There is a real lack of a coherent system that coordinates the various technologies, and improves the system's accuracy and usability. According to Frost and Sullivan [3], the need for interoperability between services is the key market driver with regard to first responders' communications, command and control, and the intelligence (C3I) market. The main market restraint is fragmented decision-making and budgetary allocations [3], as shown in Fig. 1.

In the EU, many new information exchange systems and networks are under preparation under the domain of "smart borders". The Commission has suggested the establishment of a registered traveler programme (RTP) for frequent, prescreened and pre-vetted third country travelers, and an entry/exit system (EES) allowing the electronic recording of the time and place of entry and exit of third country nationals. 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 [4]; the future European integrated border surveillance system. A concept is being developed in EUROSUR which 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; whereas the second objective is exclusively related to border surveillance.

The recent developments regarding smart borders pays significant attention to the development of the smooth passage of third country passengers and their requirements. First, border checks should be developed so that as large a portion as

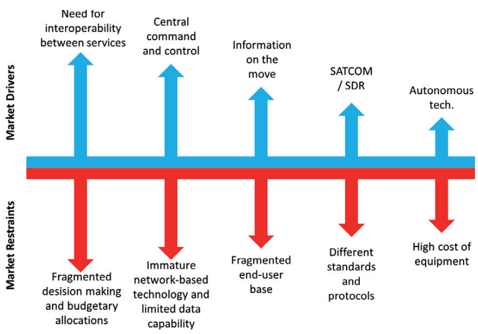


Fig. 1. Key market drivers and restraints of first responders' communications, command and control, and intelligence market.

978-0-7695-5062-6/13 $26.00 © 2013 IEEE
DOI 10.1109/EISIC.2013.66

possible of third country passengers themselves will register with RTP. Special attention must be given to the differentiation of information flows generated from border checks to EES purposes on the other hand and to the RTP purposes on the other. These information flows are complimentary and should be adjusted to those in the EUROSUR system with routine international messaging through official channels between border authorities and Frontex. This requires elementary development towards an automated border check (ABC) process for RTP applicants. A similar procedure has been tested by the USA´s Customs and Border Protection in Nogales, facilitated by an interviewing avatar kiosk developed by the BORDERS-network funded by the US Department of Homeland Security (DHS).

However, the inflows/outflows of travelers at some border crossing points (BCP) are extremely seasonal. Hence an integrated border management approach cannot be tackled without taking into consideration 'ABC-lite' products, such as handheld/portable devices. This becomes more apparent when considering the integration of all information from a BCP to work with remote systems, such as EES, and crucially the RTP. With regard to mobility, the vehicle is the most important tool for all first responders (FR) [5] due to the long patrolling distances; this is especially true with border troops. In their field operations, FRs should have access to most of their digital services from their vehicles. The basic requirement for all mobile digital services is an infrastructure including data communications and the service platform. This paper presents a layered framework for standardizing the electrical, electronic and information and communications technology (ICT) devices of emergency response vehicles (ERV). The presented generic framework for all ERVs is a baseline on which the harmonization and standardization of the proposals will be based upon. On the top of the framework, the mobile digital services of e.g. border troops could be supplied.

II. Related Standards, Projects and Solutions

The European Standard series EN 1846-x for "Firefighting and rescue service vehicles" has currently three parts that include: Part 1: Nomenclature and designation; Part 2: Common requirements – Safety and performance; and Part 3: Permanently installed equipment – Safety and performance. The National Fire Protection Association (NFPA) is an international non-profit organization that has a mission to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. NFPA is responsible for 300 codes and standards designed to minimize the risk and effects of fire by establishing criteria for building, processing, design, service, and installation in the US and other countries. NFPA has two ERV-related standards: NFPA 414 "Standard for aircraft rescue and fire-fighting vehicles"; and NFPA 1071-11 "Standard for emergency vehicle technician professional qualifications. The Ministry of Health and Long-Term Care of Ontario, Canada [6], has standardized the minimum acceptable requirements for land ambulances for use by an operator of a land ambulance service.

The One Box Single Vehicle Architecture (OBSVA) criteria [7] are an approach aimed to facilitate the development and installation of effective, safe, emergency service equipment in vehicles. The OBSVA criteria are owned and maintained by the Home Office Centre for Applied Science and Technology (CAST). The OBSVA criteria suggest the standardization and the of harmonized technologies as a way to ensure emergency services in the future with significantly reduced budgets. It outlines the standards of the future fitment of law enforcement authority (LEA) vehicles. Its aim is to provide a safe and efficient working environment for officers. This equipment fit should deliver better usability, cost efficiencies and provide a link to the standardization of all types of LEA vehicles currently in use. The OBSVA criteria introduce, for instance, requirements and specifications for controls, switches and interfaces. For example the criteria suggest that a LEA vehicle should have a graphical user interface with touchscreen capability. It also gives guidelines for how voice activation or hands-free operations should be utilized in a police vehicle. In addition to that the OBSVA criteria introduce specific instructions on how different equipment should be fitted in a LEA vehicle in order to maximize work safety and to avoid as much as possible driver distraction.

Project54 is a modular system that integrates in-car based electronic systems, software and user interfaces [8]. It also allows officers to access the in-car system using handheld devices. There is a main executable application and individual applications that control in-car electronic devices or provide other services. The devices are controlled by integrated software components running on an embedded computer. The integrated software components also implement an integrated user interface. The system allows the officer to have control over all the electronic devices, either through a touchscreen or through a voice interface. The Project54 system aims to improve the ability of LEA to collect and interpret data, and exchange data between mobile units. It also aims to increase the functionality of ERVs, increase the information available to officers in the field, and to facilitate communication between mobile units. Also, increased effectiveness and improved safety of the officers are important aspects. In 2009, the system was in use in over 1,000 LEA vehicles in New Hampshire [9].

Feniex Olympus 16X software is compatible with any PC system. A 2-user customizable interface features memory button functionality. This software and hardware combination allows a user to control all ERV electronics with a click of a mouse, keyboard stroke, or finger touch of a digital button. The user interface set up allows each officer to customize, configure, label and position their own digital buttons, as well as their three main programmable memory buttons. The system also includes a three switch face plate, which serves as a fail-safe option in the event of a computer crash. Each button controls one of the programmable memory buttons. There is an optional touchscreen add-on. The touchscreen mounts inside a vehicle console and allows the user to control all vehicle electronics [10].

The Rockwell Collins iForce™ is an integrated ERV solution that can be tailored to meet specific requirements. At the heart of the system is a Linux-based, high assurance computer that allows users to control all vehicle electronics through a single integrated system. iForce™ offers three ways to control all electronics: a color touchscreen display, a hand controller and voice activation capability. As a result, much of the electronic hardware is removed from the front of the vehicle, creating a much safer and more efficient work environment for the officers. iForce™ integrates standalone vehicle electronics into a command and control system that improves functionality, communications, ergonomics and safety. iForce™ allows officers to cross band with other FRs at an accident, emergency or crime scene. iForce™ integrates radio, video and computer functions into one system that enhances an officer's on-site communications, control and security needs while ensuring public safety [11].

The National Information Exchange Model (NIEM) is a community-driven, government-wide, standards-based approach to exchanging information, which aligns with user-driven requirements engineered for interoperability [12]. NIEMS is widely used in the USA and internationally. It is a consistent starting point including a data model, governance, training, tools and technical support services. Its active community assists users in adopting a standards-based approach to exchanging data.

III. Research Problem and Methodology

Our research and experiment case is focusing on the development of a new ERV concept. The existing solutions and services are lacking some substantial feature to provide interoperability and usability of systems. They are also struggling to address issues related to security, power efficiency, authority regulations and standardization.

New digital technical solutions are facing the challenges of current businesses. If we put innovative artifacts into the action and analyze how they are used and how they perform we will see things that cannot be seen in the laboratory [13]. Management information systems (MIS) involve three primary resources: people, technology, and information. This paper follows the basic development research in the MIS wheel diagram, first published in 1991 [14]. According to the "going the last mile" approach [13], the starting point of research should be a real problem for real people. In this paper, the real problem came from FRs in Finland who are experiencing challenges. This paper integrated science in both the laboratory and the field, including the theory, prototyping and validation by experiments. This paper gathers results from several Finnish research and development (R&D) projects. These ERV related R&D projects include:

- An enterprise project, led by Insta DefSec Ltd., developing secured software services. The project utilized the results of the related research project and aimed to develop product concepts which have potential in both domestic and export markets. Additionally, Insta DefSec Ltd. will further develop its business model in order to be able to utilize the growth potential of the product concepts. The project started in June 2010 and ended December 2012 [15].
- An enterprise project, led by Cassidian Finland Ltd., to implement a vehicle-installed professional mobile radio concept for law enforcement, and fire and rescue operations. The project started in January 2010 and will end May 2013 [16].
- The Mobile Object Bus Interaction (MOBI) research project generates research data for enterprise and governmental projects by researching and documenting the needs and requirements of the users, power generation and supply and specifying existing solutions. The project started in September 2010 and will end August 2013 [17].
- PARVI project. From an end-user and customer side, the Police Technical Center has made a proposal for a Pre-commercial Procurement project aimed at a new patrol car [18].
- KEJO project. Ministry of the Interior's ICT Agency HALTIK and the National Police Board are developing a common Field Command System for all public safety actors. The project started in January 2013 and will end December 2016 [19].

A. End-User Requirements Gathering

The inclusion of user requirements in the design of the technology has been of paramount importance in the deployment of ERVs. Therefore the identification of user requirements comprises the initial step performed by any standardization organization and project prior to the technical definition of a system. This has also been planned as MOBI's initial step. In the context of this activity, the input has been gathered from end-users, while previous experience has also been obtained from international organizations, standardization bodies and related projects. One of the main tasks of the MOBI project is to create and maintain an end-user requirements specification for ERVs. Fig. 2 shows the end-user requirements gathering process, which includes both qualitative and quantitative data analysis, and grounded theory-based research that determines the theory from data. The first draft of the life document was ready in the autumn of 2011. The current, sixth version [20] was completed in May 2013.

The purpose of the end-user requirements specification is to provide information on features and components, when assembled, and produce capable and efficient emergency response vehicles for both on- and off-pavement performance. The border guards, customs, police and rescue officers work in

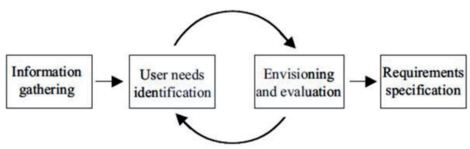


Fig. 2. End-user requirements gathering process

challenging situations and conditions, hence considering their own requirements is very important in the provision of efficient services.

The end-user requirements specification is also helping guide engineers and technology firms to adequately design and implement technical products or tools in ERV, mainly the requirements described by users during the requirement gathering phase of the MOBI project. In addition, it will also greatly assist authorities in the design of non-technical services and solutions for ERVs. Research work is an effort to standardize the processes of building a user-centric ERV.

IV. Standardization Aspects

The review of current ERVs emphasizes that the design, services and solutions are working under normal conditions. There are effective implementation of services and solutions in existing ERVs across various spectrums. However, the research study shows shortcomings on various aspects. The study of the MOBI project emphasizes end-user's requirements and their needs in various conditions, especially for challenging conditions. There are possibilities of improvements in various aspects of ERVs. These will enhance the performance, effectiveness and optimum usage of resources. Research studies show that areas of improvement include emergency response preparedness, critical communication and real time updates, optimization of power supply, availability of resources and equipment, safety and sustainability, ease of use and optimization of computer systems (hardware and software). The EVRs are used in different conditions and environments. Hence, considering end-users needs leads to better and more sustainable services and solutions [20].

The end-user requirements specification has functional and non-functional requirements [20]. The requirement gathering, analysis and specification resulted in working closely with end-users. Popular requirements-gathering techniques, such as the interviewing of law enforcement officers and users of Finnish ERVs, joint application development (among R&D teams), literature reviews and observation, have been used to generate the requirements specification. In certain requirements, an activity diagram and use cases are provided

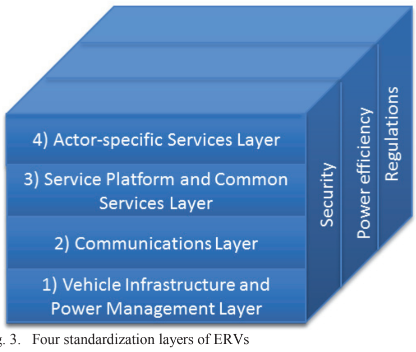


Fig. 3. Four standardization layers of ERVs

to visualize the logical modeling of the business processes and workflows, as well as the basic function of the systems in ERV. The end-user requirements specification reflects the actual users' views and how they see things in ERV. Hence the focus of requirement specification is user-centric, along with the conducted research.

The grounded theory based research of end-user requirements results in a layered approach. According to this approach, ERVs' electrical, electronic and ICT systems are divided into four layers that have standardized interfaces, as shown in Fig. 3. These layers 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 layers.

A. *Vehicle infrastructure and power management*

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

B. *Communications*

In the current digital world FRs are aware of the benefits that interconnection between different professional mobile radios (PMR) and the integration of new advanced data services could bring to their professional sectors. LTE is considered an appropriate technology for building next-generation broadband public safety networks. However, it does not yet support some voice communication characteristics that PMR technologies already offer. Also, PMR systems are widespread all over the world, making their replacement quite difficult within a short period. Therefore some public safety organizations are working on dual solutions to provide TETRA voice capabilities, together with broadband data transfers. Our other study [21] is focused on this topic.

C. *Service Platform and Common Services*

All ERVs have many similar applications, such as a navigation system, patrol tracking, target maps, activity logs, alarms and remote access to central databases as well as the control of blue lights and sirens, power supply systems, and communications equipment. Roughly the common needs of the service platform and common services layer could be divided into two main areas: 1) decrease in the number of physical Human-Machine Interfaces (HMIs); and 2) a common field command system for all PPDR actors that also improves interoperability between different FR actors.

However several physical HMIs are needed for different modes of operation. For example, the HMIs when driving at full speed should be totally different to those in mobile office mode, where ergonomics have an important role. Applying the design principles of service-oriented architecture, from an end-users point of view, different existing systems will seem to form one part of the field command system.

One example of standardization aspects is in the application of different security level IT service environments using the same data terminal equipment. Penttinen's [22] implementation was defined to cover the Finnish national security audit criteria (KATAKRI)-based information security sections. The solution is intended for Windows operating systems. A technical solution was accomplished using the DevCon command-line device manager utility software created by Microsoft. DevCon script was defined in the non-encrypted master boot record which automatically separates different hard disks during the startup process of the operating system when the end-user chooses the environment to be used. The technical solution offers the possibility to use different security level Windows-based ICT environments in the same device, which could enable designers to reduce the number of ERV devices. The reduced number of devices will also help solve problems reported regarding power consumption and cabling, as well as reducing the cost of ICT on the Finnish government.

D. Actor-specific Services

By 'actor-specific services' we mean these digital services that differ substantially from other FR needs. For example, LEAs ought to have forensics technology for investigations and field work. These kinds of technologies include advanced tracking systems that apply the Global Positioning System (GPS) to track criminals and vehicles that have been tagged. This allows LEAs to keep track of suspicious activity that can help solve cases. We have widely studied these kinds of services in our SATERISK research project [23]. However, they will run on top of common services via a standardized interface.

When looking at new actor-specific services for border protection, unmanned border patrol systems, such as unmanned aerial vehicles (UAV), employ high-tech devices. For example, the border between Russia and southern Finland has many twists and turns. Small UAVs and micro air vehicles (MAV) could be posted at intervals and launched either automatically to check abnormalities detected by static surveillance sensors or by duty officers at the command posts [24]. The United States uses a full-scale military UAV MQ9 Predator B to monitor its borders; however there are limits to their intended use [25]. According to Bolkcom [26], UAVs are likely to be fielded as part of a larger system of border surveillance, not as a solution in themselves. MAVs launched from command posts along hard-to-access borders could provide low-cost, rapid-response imagery and other data in response to suspected border incidents [24]. A new ERV should be able to act as a mobile field command and control station. Future field command system standards should to take account of the control of UAVs/MAVs.

V. Discussion

A. Solution Benefits

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

In particular, open standards ease the ability of SMEs coming into the business, which improves the supply of new public safety ICT products and degreases their prizes. In addition to cost savings, the interoperability and availability of new public safety ICT services is improved.

B. Competition

The problems within the public safety branch are similar within all countries; for example the constant increments in ICT devices of ERVs. Different public safety actors need different kinds of ERV; since an ambulance differs from a border patrol vehicle. The current ERV-related standards specify the majority of construction and design details, including voice radio installation requirements. However these standards offer no information about field command systems and interoperability requirements between different first responders. According to our approach, although ERVs are different their communications layer as well as their service platform and common services layer could be identical. This enables interoperability between first responders, at least at a technical level.

The MOBI project advantage over other development projects is the traditionally well-operating and organized co-operation between Finnish authorities at different levels, e.g. national police, customs and border guards [27]. The project will enhance cooperation between the authorities through networking and the development of common processes. The project involves authorities from the National Police Board, Police Technology Centre, Police College, Emergency Services College and the Border Guard. Also individual experts from local police departments, regional rescue departments, customs, emergency response centers, emergency medical services and private security companies have taken part in the MOBI development process.

VI. Conclusions

LEAs main need is to maintain their core services with a significantly reduced budgets. Traditionally LEAs suffer from intensive human involvement. The only realizable solution is the better piggybacking of ICT and digital services. In field operations, the LEAs' most important tool is their vehicle. This paper presents a layered approach for standardizing the electrical, electronic and ICT devices of ERVs. On the basis of this infrastructure, the mobile digital services needed for first responders could be supplied.

References

[1] A. Patrascu, "Optimizing distributed sensor placement for border patrol interdiction using microsoft excel," Thesis, Department of the Air Force, Air Force Institute of Technology, April 2007.

[2] Z. Suna, P. Wanga, M. Vuranc, M. Al-Rodhaanb, A. Al-Dhelaanb and I. Akyildiz; "BorderSense: border patrol through advanced wireless sensor networks," *Ad Hoc Networks*, vol. 9, pp. 468–477, 2011.

[3] B. Srimoolanathan, "World security market outlook", presented at *Tekes Safety and Security Programme's Annu. Seminar*, Nov. 2012. [Online] Available: https://tapahtumat.tekes.fi/uploads/3ef8185/balaji_frost_sullivan_safety_seminar-4590.pdf

[4] G. Ameyugo, M. Art, A. Esteves and J. Piskorski, "Creation of an EU-level information exchange network in the domain of border security," in *Proc. of European Intelligence and Security Informatics Conference*, Odense, Denmark, Aug. 22–24, 2012.

[5] J. Rajamäki, "The MOBI project: designing the future emergency service vehicle," *IEEE Veh. Technol. Mag.,* June 2013 [In Press].

[6] Ministry of Health and Long-Term Care, *Ontario Provincial Land Ambulance & Emergency Response Vehicle Standard*, Version 5.0, September 28, 2012. [Online] Available: http://www.ambulance-transition.com/pdf_documents/standards_land_amb_emergency_response_vehicle_standard.pdf

[7] Home Office Centre for Applied Science and Technology, *One Box Single Vehicle Architecture Criteria*, Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/115688/cast3911.pdf

[8] A. Pelhe, N. Kozomora, A. L. Kun and W. Miller, "Distributed components in the Project54 system," in *Proc. Winter Int. Symp. Information and Communication Technologies* (WISICT '04), Cancun, Mexico, January 5–8, 2004, pp. 1–6.

[9] A. L. Kun, *Project54 Introduction, UNH Consolidated Advanced Technologies Laboratory (CATlab)*. [Online] Available: http://www.catlab.sr.unh.edu/overview/introduction

[10] Feniex, *Feniex Product Catalog 2012*. [Online] Available: http://corepublicsafety.com/catalogs/Feniex2012catalog.pdf

[11] Rockwell Collins. [Online] Available: http://www.rockwellcollins.com.

[12] NIEM, *National Information Exchange Model*. [Online] Available: https://www.niem.gov/Pages/default.aspx

[13] R. Winter, "Interview with Jay F. Nunamaker, Jr. on 'Toward a Broader Vision of IS Research'", *Bus. Info. Syst. Eng.*, vol. 2, iss. 5, pp. 321–329, 2010.

[14] J. F. Nunamaker Jr., M. Chen and T. D. M. Purdin, "Systems development in information systems research", *J. Manage. Inf. Syst*. vol. 7, no. 3, pp. 89–106, 1990.

[15] Secure software services. [Online] Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10210602

[16] *Vehicle installed professional mobile radio concept for law enforcement and fire & rescue operations*. [Online] Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10201742

[17] *Mobile Object Bus Interaction*. [Online] Available: http://www.tekes.fi/programmes/Turvallisuus/Projects?id=10199203

[18] H. Riippa, "Procurement at the Finnish Police," presented in *Tekes Safety and Security Programme's Annu. Seminar*, Nov. 2012.

[19] *Projektipäällikkö – Kejo-hanke (Project Manager – Kejo Project)*. [Online] Available: http://www.poliisi.fi/poliisi/bulletin.nsf/PFC/6FA46AF5EF825F98C2257AF3002E83A8

[20] P. Rathod and P. Kämppi, "User requirements specification: MOBI work package 2", version 1.0, May 2013 (unpublished).

[21] J. Rajamäki, P. Rathod and J. Holmström, "Decentralized fully redundant cyber secure governmental communications concept," in *Proc. European Intelligence and Security Informatics Conf.*, Uppsala, Sweden, Aug. 12–14, 2013.

[22] J. Penttinen, "How to use different security level IT service environments using the same data terminal equipment" (Eri tietoturvaluokan palveluympäristöjen käyttö samalla päätelaitteella), Master thesis, Laurea University of Applied Sciences, Espoo.

[23] J. Rajamäki, R. Pirinen and J. Knuuttila, Eds. *SATERISK - Risks of Satellite Based Tracking*, Sample of Evidence Series, Vol. 2. Helsinki: Edita Prima, 2012.

[24] H. Ruoslahti, R. Guinness and J. Viitanen, *Airborne Security Information Acquisition Using Micro Air Vehicles: Helping Public Safety Professionals Build Real-Time Situational Awareness*, HICSS 2010.

[25] S. Waterman, *UAV tested For US border security*, Washington, UPI, Feb. 12, 2007. [Online] Available: http://www.spacewar.com/reports/UAV_Tested_For_US_Border_Security_999.html

[26] C. Bolkcom, "Homeland security: unmanned aerial vehicles and border surveillance", *CRS Report for Congress*, 2005. [Online] Available: http://epic.org/privacy/surveillance/spotlight/0805/rscb

[27] A. Niemenkari, "Integrated border management – case Finland," *Euromed Migration II Project*, Rome, Italy, Feb. 23, 2010. [Online] Available: http://www.euromed-migration.eu/e1152/e1483/e2556/e2585/e2641/ presen92NiemenkarM2s21feb2325rome2010.pdf

VII

THE MOBI PROJECT: DESIGNING THE FUTURE EMERGENCY SERVICE VEHICLE

by

Jyri Rajamäki, 2013

IEEE Vehicular Technology Magazine, vol.8, no.2, June 2013, 92-99

THE MOBI PROJECT

Designing Future Emergency Service Vehicles

Jyri Rajamäki

Digital Object Identifier 10.1109/MVT.2013.2252294
Date of publication: 1 May 2013

The proliferation of information and communications technology (ICT), facilities in public protection and disaster relief (PPDR) vehicles has highlighted several questions, including: "Why can't vehicles' ICT applications be simplified and rationalized to help PPDR responders work more efficiently and effectively?" and "Can two items of equipment be combined to make it easier to use and decrease power consumption?" Our project aims to create a common ICT infrastructure for all PPDR vehicles based on better integration of ICT systems, applications, and services. Our approach is to divide PPDR vehicles' ICT systems into four layers (a vehicle infrastructure and power management layer, a communications layer, a service platform and common services layer, and an actor-specific services layer) with standardized interfaces between them. Open standards make it easier for small- and medium-sized enterprises (SMEs), in particular, to enter the market. In addition to

 1556-6072/13/$31.00©2013IEEE

providing cost savings, our system significantly improves interoperability and the availability of new PPDR ICT services.

The most essential tasks undertaken by PPDR responders, such as law enforcement authorities (LEAs), firefighters, emergency medical services (EMS), and disaster recovery services, are to deal with different kinds of emergency situations on land, on water, and in the air. The vehicles they use and the devices installed in these vehicles must be suitable for very demanding and variable conditions. Today's PPDR vehicles are packed with a large body of equipment. This has generated new problems with air bags, power supplies, cables, etc. The documentation of applied solutions has been variable, and there has been no standardization, which is needed in this field, particularly because of the diversity of the equipment suppliers.

The Mobile Object Bus Interaction (MOBI) research and development project aims to create a common ICT infrastructure for all PPDR vehicles based on better integration of ICT systems, applications, and services [1]. Another goal of the project is to extend it to other PPDR vehicles in European countries, permitting standardization of tools and technology in European Union (EU) countries. MOBI is a three-year (1 September 2010—31 August 2013) project involving collaborative work between Finnish research organizations, PPDR actors, and diverse industrial partners. MOBI's research methodology follows Nunamaker's integrated, multidisciplinary, and multimethodological going-the-last-mile approach [2].

PPDR responders operate a large number of vehicles and many different types of vehicles, which are normally production vehicles retrofitted with a wide range of aftermarket equipment, depending on their roles. MOBI concentrates on van-sized vehicles, as shown in Figure 1. Depending on the organization, a PPDR vehicle can be divided into two or three sections, and EMS vehicles might also have two or three sections. In general, vehicles used by the LEAs and rescue services have three sections. The cap comprises the front of the vehicle, from which the vehicle is steered and controlled. The cap can also be applied for the field command. The mobile office is a space where troops can be chauffeured and/or a longer-lasting field-command environment can be set up. The transport unit is used for transporting goods, equipment, police/sniffer dogs, and/or clients. The patient service unit of an EMS vehicle comprises the space where the patient is cared for and transported.

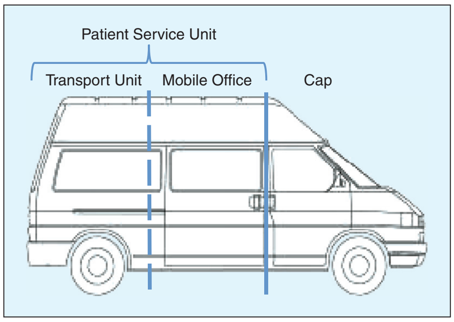


Figure 1 Sections of a van-sized PPDR vehicle body.

Modern PPDR vehicles hold more information technology and other technical devices than ever before. For example, police vehicles are mobile offices in which many customer queries can be dealt with, such as ticketing and filling out passport or driver's license applications. Police vehicles also contain many tools, cameras, and technical devices for speed control and other traffic surveillance.

Overview of Some Ongoing PPDR Vehicle Development and Standardizing Projects

The National Safety Agency (NSA) of Australia has integrated technology into police patrol vehicles and command vehicles. A new police patrol vehicle concept provides benefits to jurisdictions seeking to use technology to improve their law enforcement capability. NSA's police patrol vehicle has been designed to allow greater functionality while reducing clutter inside the cabin. The technology integrated into the vehicle enables more work to be undertaken in the field. Overall, the technology and purpose-built interior increase the officers' safety as well as operational effectiveness. A key feature is an LCD touch screen embedded into the dashboard of the vehicle; all of the equipment included in the car is operated through this touch screen.

The level of technology integration in the vehicle provides superior surveillance capability. This includes automatic number plate recognition cameras, night vision cameras, speed-detection equipment, and biometric devices. A key risk of installing this technology would be vehicle battery drain. This problem has been overcome with the development of a power management system that enables a range of equipment to function without affecting the vehicle's battery. NSA's command vehicle project will create a mobile command center that is able to operate in remote locations for extended periods. The high level of connectivity in the vehicle enables communication between a central base and the personnel in the field. Active repeaters fitted in the vehicle boost signal strength, supporting communications in the most remote areas. The vehicle is fitted with solar panels to ensure continuous generation of power so that the equipment will operate without being constrained by the vehicle's battery capacity. Power-management systems also aid in extending the length of time the equipment is operational in the vehicle without affecting battery charge. The vehicle is designed to be ready for immediate deployment so as to reduce response time when there is an incident [3].

The Association of Chief Police Officers (ACPO) intelligent transport systems (ITSs) working group identifies and works to incorporate emerging technologies to benefit the police services of the United Kingdom ACPO ITS leads a public-private partnership to develop the One Box: Single Vehicle Architecture [4] and One Box: Driver and Vehicle Data Management [5] concept and functional requirements for police, with work currently underway to develop products showing how the data can be utilized to better manage the police vehicles and drivers proactively. This work is one aspect of police vehicle standardization that is intended to increase functionality and reduce cost, providing an efficient and cost-effective approach to police transport equipment and procurement in the future. This concept ensures that the equipment fitted adheres to the standard and is fit for purpose and functionality, creating a technology platform for the future.

The Ministry of Health and Long-Term Care of Ontario, Canada, has standardized the minimum acceptable requirements for land ambulances for use by an operator of a land ambulance service [6]. This 126-page standard specifies all construction and design details, including voice radio installation requirements. However, the standard includes no information about data communications, field-command systems, or interoperability between different PPRD responders.

End-User and Market Needs

With an ever-increasing amount of technology being installed in vehicles, the number of electronic devices, cables, and user manuals that need to be carried also increases greatly. These are becoming increasingly difficult to manage as they eat into the available space in the vehicle. The trend to transmit more data is also increasing, driven by the need to quickly transfer photos, videos, and heavy documentation between different units, combined with the need for strong network security. Mobile data connection must be available for PPDR responders in all situations. The essential features are the network capacity, secure connections, transfer rate, load capacity, and flexibility [7]. In the future, it will be necessary to ensure transmission of more data. Particularly in Finland, the amount of transferred mobile data is growing very rapidly because of increased cooperation between PPDR organizations, new data systems with better situational awareness, and the moving-office concept for the police.

Since current mobile terminals are not able to meet users' needs for short-term mobile data operations, new multichannel devices are needed. The level of mobile data services for every professional mobile radio (PMR) network should be clarified. In the near future in Europe, terrestrial trunked radio (TETRA) or Tetrapol-based PMR networks and commercial mobile networks will act in parallel as service platforms for PPDR. User needs, possibilities, and restrictions should be considered when developing an application as a part of a PPDR mobile data system.

Due to the economic situation in Europe, PPDR organizations' resources are meager. This has led to increased pressure on PPDR organizations to pick up their slack. To do that, better cooperation between PPDR organizations and utilization of ICT systems is needed. PPDR responders have an increasing amount of ICT facilities and applications in their vehicles. However, each country and even each PPDR organization is developing its own solutions according to their legislation and requirements because uniform standards are missing. Tailored systems are expensive, are difficult to support, and have no in-built interoperability. This problem has been recognized. For example, the European Commission, the European Law Enforcement Agency (EUROPOL), and the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX) have come to the conclusion that the lack of interoperability limits the effectiveness of PPDR practitioners in actual operations [8].

However, many potential aspects to interoperability exist, and it would be unaffordable and probably undesirable to provide for arbitrary seamless interchange of information. While most potential user requirements for interoperability were catered to in the technology standards, they were not always implemented or activated in actual systems. So, while user needs had been expressed in the formulation of standards, these interoperability needs were not specified when procuring and operating communications systems [8].

Technical standards are currently developed by separate bodies focused on critical communications or ITSs. The TETRA + Critical Communications Association is focusing on mobile broadband for professional users. The International Organization for Standardization (ISO) technical committee (TC) 204 develops ITS standards at a global level, and the European Committee for Standardisation (CEN) TC 278 and European Telecommunications Standards Institute (ETSI) TC ITS do so at the European level. These technical standards define the capabilities of the systems. There is a need for an overarching body that can harmonize the profiles across systems and come to an agreement on the optimal means for achieving interoperability between critical communications and ITSs. Such a body might have a growing role in defining data standards as the need for consistent data semantics grows, and applying to PPDR the much more quickly advancing standards emerging from commercial

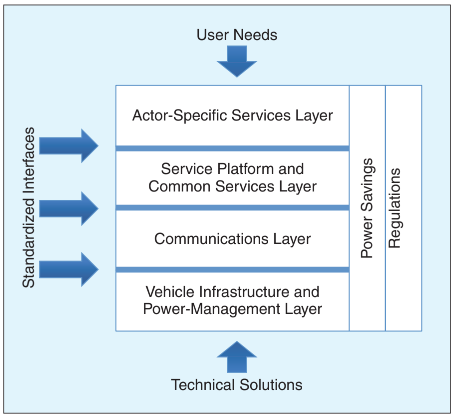


FIGURE 2 Layered approach to ICT integration of PPDR vehicles.

mobile services. This role would be similar to that of the Internet Engineering Task Force (IETF) and might be carried out by the Law Enforcement Working Party (LEWP) in conjunction with ETSI and CEN.

Solution Approach

The main challenges of the MOBI project are to know how the PPDR vehicle's ICT architecture should be arranged and how the vehicle should be built. In parallel with vehicle control systems, components of PPDR equipment have historically been standalone equipment that was individually hard-wired using bespoke cable runs and connectors. Our solution for simplifying the ICT services provided for PPDR vehicles is to divide vehicles' ICT architecture into certain layers that have standardized interfaces. Figure 2 shows the layers of our solution: 1) the vehicle infrastructure and power management layer, 2) the communications layer, 3) the service platform and common services layer, and 4) the actor-specific services layer. The starting point of our solution is the needs of PPDR end users; we apply the basic lines of the human-centered design processes for interactive systems outlined in the ISO 9241-210 standard. Our solution is based on the technology available. The future development work is to standardize the three interfaces between these four layers.

Vehicle's Infrastructure and Power Management

Usually, a van-sized PPDR vehicle is a generic van with added features, as shown in Figure 1. In this section, we discuss the example of the demo vehicle that we have equipped, shown in Figure 3. Our van-sized police car is a standard Volkswagen Transporter whose roof has been cut off from the cap and mobile office sections. Then, a new fiberglass roof element containing emergency lights, alarms, and GPS, 2G/3G/4G, TETRA, and Wi-Fi antennas was retrofitted. The antennas were wired on the top of the original metal roof above the transport unit. In addition, e.g., the bars of the transport unit (also used as a jail) in the rear were installed, in addition to the mobile office room table and seats. A view of a mobile office room of a modern Finnish police car is shown in Figure 4.

Our demo vehicle includes an intelligent electric power distribution and control system called Standby. It contains a control unit that turns off low-priority systems during low-battery voltages. The inverter converts 12 V dc battery voltages to 230 V ac required, e.g., for a laser printer. A 230 V ac/12 V dc rectifier is used in garages and other places where the mains current is available. Standby includes headlights, an alarm, and work lights and their control systems as well as electric central locking systems and fans for cooling. When the engine is running, the start battery charger of the van also recharges Standby's batteries. Certain information from the vehicle's

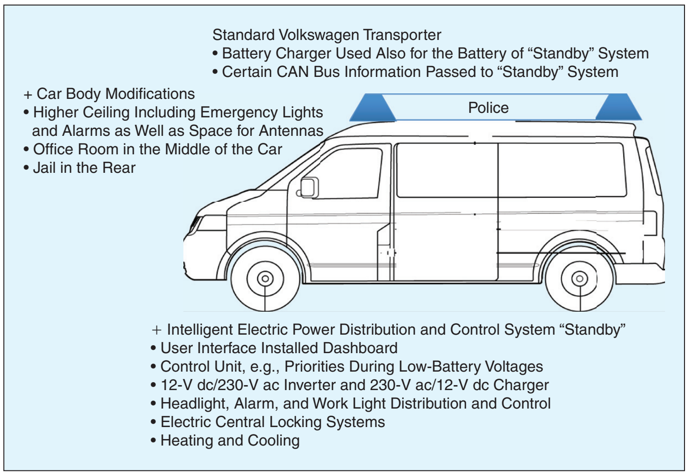


FIGURE 3 MOBI demo vehicle: a van-sized police car.

control area network (CAN) bus is passed to the Standby system, such as engine performance, available fuel amount, and the level of battery voltages.

Since power consumption is one of the biggest challenges in PPDR vehicles, we are currently determining the number of necessary physical and virtual computers and examining the power consumption of other devices during various operational modes. Currently, our demo vehicle includes a lead-acid start battery (72 Ah) and nickel-metal hydride batteries (3×30 Ah) for PPDR ICT systems. In the near future, other options for power generation, such as fuel cells, will be examined.

FIGURE 4 A view of a mobile office room of a modern Finnish police car [9]. (Photo courtesy of Sami Hätönen.)

Communications Layer

PPDR vehicles' communications needs can be divided into long-distance communications, local area networks (LANs), and accessory communications. Furthermore, each category is scaled from light to heavy. ICT solutions have to be robust and easy to install. Special attention has to be paid to information security. Various encryption methods between different kinds of systems bring their own challenges to this project and its information security solutions. In addition, each PPDR actor has its own requirements regarding how to implement the information security into its vehicles' systems.

Our demo vehicle is equipped with a TETRA radio, which is mainly used for voice communications, and a separate multichannel router, which is connected to the control and command room applications via parallel TETRA, 2G/3G, LTE/4G, wireless LAN (WLAN), and satellite data access technologies. A multichannel router offers a redundant solution when more than one functional data communication channel exists for data transmission. Our demo, shown in Figure 5, uses the distributed systems intercommunication protocol (DSiP), which allows the use of several parallel communication paths simultaneously [10]. DSiP handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution [10]. Multichannel router's quality-of-service option sets the desired order of the network access by desired cost-of-service (CoS) value. Therefore, when operating in areas where the network availability and signal strength vary widely, the network exchange should proceed without being noticed by the user and without breaking the connection. The user organization will choose in advance whether to use either the strongest signal or the cheapest network or some combination of these rules. This selection is done by setting the value of the CoS.

There is a need for secure, uninterruptable communication in many applications. Different approaches have been addressed to mitigate the problems; examples include multipath transmission control protocol stack and an open-source project with a multichannel virtual private network solution. However, DSiP appears to be the only commercially available solution that addresses a large number of known problems. Other options include, e.g., communications access for land mobiles (CALM) for intelligent transportation systems initiative by the ISO, but this is still a work in progress. Therefore, large-scale implementations of the standard do not yet exist. In contrast, DSiP-based systems have been in operative use in critical installations for several years, e.g., the Finnish Coast Guard's coastal surveillance solution and supervisory control and data acquisition (SCADA) control of Finland's main power grid.

Another reason for selecting the DSiP solution for our demo vehicle is that the CALM architecture is based on an IPv6 convergence layer that decouples applications from the communication infrastructure. However, DSiP is insensitive toward the transport layer and may freely use IPv4 and IPv6 networks as transport with tunneling capabilities. Also, compared with CALM, applications may use and transparently communicate through the DSiP mesh without having to implement the interfaces with application programming interfaces. This effectively means that there is no need to modify applications or equipment when applying DSiP.

Service Platform and Common Services

The standardized communication layer for all PPDR organizations enables cooperation between authorities, e.g., by setting up a common talk group for incident communications. The next pitch of harmonizing is the service platform and common services layer, in which the design principles of service-oriented architecture could be applied. All PPDR vehicles have many similar applications, such as a navigation system, patrol tracking, target maps, activity logs, alarms, and remote access to central databases, as well as controlling of blue lights and sirens, power supply systems, and communications equipment. Generally, the common needs of this layer could be divided into two areas: decrease

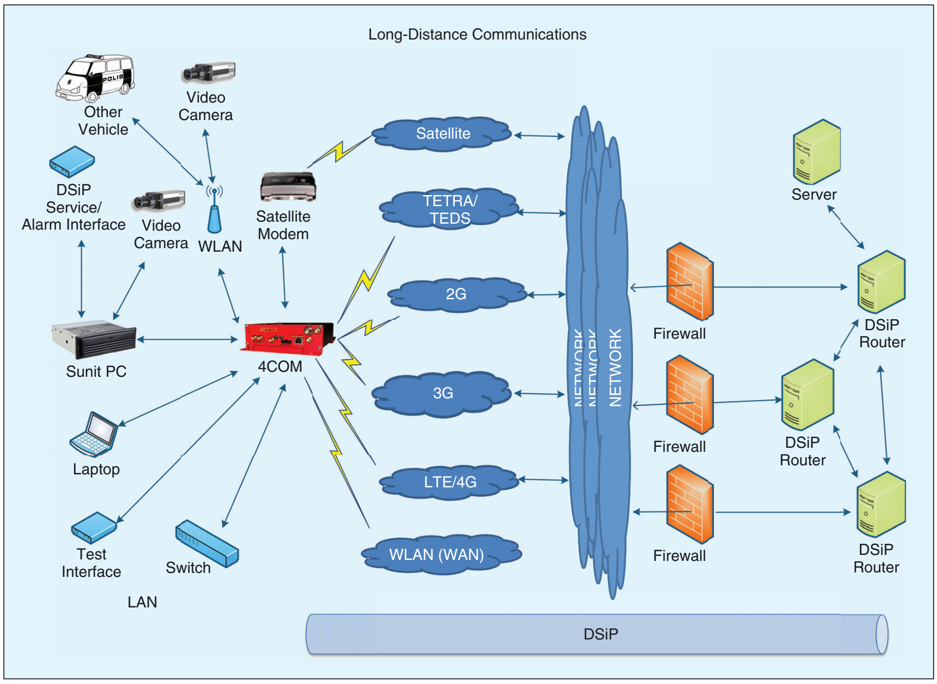


FIGURE 5 MOBI demo vehicle's communication system.

in the number of physical human–machine interfaces (HMIs) and a common field-command system for all PPDR actors.

Human–Machine Interfaces

With a plenitude of new ICT systems in PPDR vehicles, the number of user interfaces has increased by dozens. Of course, ICT systems require HMIs. However, the number of different HMIs should be reduced. So, whenever possible, HMIs should interact with multiple systems and/or functions. HMI functions and logic should be standardized to simplify the use of multiple systems. Standardized HMIs (a standard keyboard, touch screen, and mouse) increase the ease of user experience and improve efficient usage of the systems. The HMIs in PPDR vehicles should be robust and easy to operate in all conditions. PPDR vehicles must be able to operate in varying natural conditions, such as when the environment is dark, cold, hot, or humid. HMIs must be easy to access and use even when the vehicle is moving at a high speed. All HMIs should be operable with thin gloves, at least to some extent. The systems should be able to generate any information, notice, or warning in the same language as the HMI. The system navigation should be clear and easy to adopt. The user should be able to get 24/7 operational support related to the system.

In our demo vehicle, a key feature is the graphical HMI running on a Windows XP operating system that has replaced many hard keys on the dashboard with soft keys on a touch screen. It enables an easy-to-reach functionality in the main applications, such as the field-command system, power management, emergency lights, alarms, and voice radio as well as management of the PC itself and any other third-party application running on a Windows XP platform.

Field-Command System

A field-command system is a complete solution and platform that integrates different applications into one easy-to-use interface. The same technology and application could be used by all PPDR responders. This improves inter-operability between PPDR organizations and enables field operations to be more effective.

Today, the most important data system of Finnish police vehicles is the poliisin kenttäjohtojärjestelmä (POKE) field-command system. It consists of different kinds of maps, including aerial photos, patrol tracking, messaging, activity logs, and information sharing, as shown in Figure 6. The system has access and enquiry facilities to several databases and includes resource management and dispatching as well as reporting applications. POKE has many other features and several devices, such as fingerprint scanners, can also be connected to it [9]. It is also used by other Finnish authorities, and some information is shared. However, POKE has been created for the police and does not fulfill all the needs of every PPDR responder. Therefore, further development work is needed, but POKE is a good starting point.

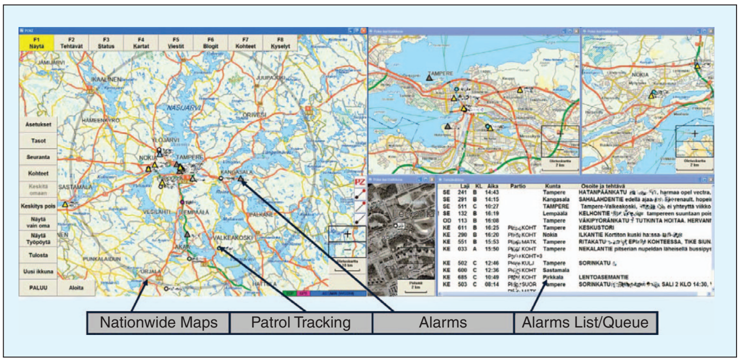


Figure 6 A basic view on two screens of POKE [9]. (Photo courtesy of Sami Hätönen.)

Other field-command systems to be studied include the MERLOT product family, developed by Lociga Ltd. and used in some Finnish regional rescue departments, SAFE command, developed by EADS Astrium Company and used in rescue services in the United Kingdom, and an army-specific Blue Force Tracking technology, Force XXI Battle Command Brigade, and Below (FBCB2) used by the U.S. Army, the U.S. Marines Corps, and the British Army.

Actor-Specific Services Layer

With regard to actor-specific services, we have researched different needs of specific PPDR actors. We are in the process of choosing the most essential applications for each actor group for further study (e.g., video and speed radars for the police). The common HMI to these services will be the field-command system.

Discussions and Conclusions

The MOBI project divides the ICT systems in PPDR vehicles into four layers with standardized interfaces. We have equipped a demo vehicle that is used for tests and further research by the PPDR actors and business partners. Our end-user requirement analysis shows that while ambulances, police cars, and fire trucks are quite different, their communications layer as well as service platform and common services layer could be identical. Similarities within the two middle layers will also help in standardizing all three interfaces.

The adoption of open standards and the capability to change between vehicle and equipment suppliers will become increasingly important for PPDR organizations, which are facing significant pressure to maintain core services with significantly reduced budgets. Open standards ensure that PPDR equipment is generic and has a high level of interoperability. The equipment fitted to a vehicle may well be replaced during its operational life as organizations introduce new technologies. Similarly, equipment may be added, removed, or modified, such as when there is a change of equipment supplier. Standardized interfaces will minimize or ideally eliminate the requirement for a partial or full refit of the cabling and additional control systems within the vehicle, resulting in significant reductions in the costs involved in stripping out and refitting proprietary control systems.

PPDR organizations will also promote innovation and competition between equipment providers in terms of the provision of user functionality, interoperability, and services to actively support delivery of front-line services. In the future, standards should be also suitable for actors other than PPDR. For example, critical infrastructure companies, private-security sector, and fleet-management services may have needs for mobile-office-like vehicles.

It is a proven fact that standardization strongly affects businesses that develop and sell technologies and technology-based products and services [11]. Development of a new ICT concept is significantly expensive, thus making access to the international market desirable. By improving the supply of new PPDR ICT products and decreasing their prices, standardization makes it easier for SMEs to compete against bigger firms. Applying standardized interfaces and common platforms enables new innovations to place more emphasis on the development of digital, rather than physical, services. SMEs are often quicker at making digital service innovations.

Today, in many countries, de facto standardization of emergency service vehicles is ongoing with the participation of the car industry, public safety organizations, critical-communications equipment suppliers, and software integrators. Also, many de jure standardization projects are underway, e.g., in the field of public safety communications by ETSI, the International Telecommunications Union, the Third Generation Partnership Project, the IETF, and the IEEE, and in the field of ITSs by the ISO, the CEN, and ETSI. Our goal is to work toward an international open standard that enhances and eases the cooperation between PPDR actors. To improve interoperability and availability of new PPDR ICT services, standardization development with like-minded countries should be started in Europe. The potential engine of such development could be the LEWP in conjunction with ETSI and CEN.

In the future, the results of our research will enable us to build new business models that answer the question: How can a developed overall solution or a part of it be marketed as a compatible set? The industry's market and volumes, the relations between international, national, and public–private partnerships' regulations in different countries, will be examined. One task is to monitor the development of the markets in the EU on the branch. The objective is to create scenarios out of the business models to clarify who should be responsible for the integration work, further equipment acquisitions, and administration.

Within this article, the Finnish model is being developed and documented as a basis for creating request for qualification documents. Development in the EU is contingent on the European surveillance system EUROSUR forming in the future a part of the EU's wider common information sharing environment, under which information may be shared with a whole range of third actors, including police agencies and defense forces. This development will have effects on the future mobile and vehicular systems that LEAs are using in their everyday activites.

Acknowledgments

The author would like to acknowledge all the participants of the MOBI project [1], jointly cofunded by Tekes—the Finnish Funding Agency for Technology, Finnish industrial partners (Cassidian Finland Ltd., Insta DefSec Ltd., Ajeco Ltd., and Sunit Ltd.), Finnish Police (The National Police Board and the Police Technical Centre), and Laurea University of Applied Sciences.

Author Information

Jyri Rajamäki (jyri.rajamaki@laurea.fi) received his M.Sc., Lic.Sc., and D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology, Finland, in 1991, 2000, and 2002, respectively. From 1986 to 1996, he was with Telecom Finland. From 1996 to 2006, he worked with the Safety Technology Authority of Finland, where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006, he has been with Laurea University of Applied Sciences, Espoo, Finland, where he is the head of Laurea's Data Networks Laboratory. He has 17 years of experience in electrotechnical standardization, with seven years as the secretary of the Finnish National Committee on EMC and ten years as the chairman of the Finnish Advisory Committee on EMC. He has been a member of several EC working groups, and the scientist in charge for several research projects funded by EUREKA and the Finnish Funding Agency for Technology and Innovation. His research interests are in electromagnetic compatibility as well as ICT systems for private and public safety and security services. He has published 80 papers in international journals and conference proceedings.

References

[1] (2013, Apr. 4). Laurea MOBI wiki [Online]. Available: http://mobi.laurea.fi/
[2] R. Winter, "Interview with Jay F. Nunamaker, Jr. on 'Toward a Broader Vision of IS Research'," *Bus. Inform. Syst. Eng.*, vol. 2, no. 5, pp. 321–329, 2010.
[3] (2013, Feb. 3). National Safety Agency [Online]. Available: http://www.nsaaust.com/
[4] Home Office Centre for Applied Science and Technology. (2011). One box: Single vehicle architecture criteria [Online]. Available: http://www.homeoffice.gov.uk/publications/science/cast/cast3911?view=Binary
[5] Home Office Centre for Applied Science and Technology. (2012). One box: Driver and vehicle data management system criteria [Online]. Available: http://www.homeoffice.gov.uk/publications/science/cast/crime-prev-community-safety/cast2812?view=Binary
[6] Ministry of Health and Long-Term Care. (2012, Sept. 28). Ontario Provincial Land Ambulance & Emergency Response Vehicle Standard, Version 5.0 [Online]. Available: http://www.ambulance-transition.com/pdf_documents/standards_land_amb_emergency_response_vehicle_standard.pdf
[7] H. Riippa, "The future of PPDR networks in Finland: Requirements and options," presented at the EU Workshop on the Future of PPDR Services in Europe, Brussels, Belgium, Mar. 30, 2011.
[8] G. Baldini, "Report of the workshop on 'Interoperable Communications for Safety and Security'," Publications Office European Union, Rep., 2010.
[9] S. Hätönen. (2012, May 30–31). "Police field commanding: The role and supportive ICT and communication system. presented at the PSC Europe Conf. [Online]. Available: http://www.psceurope.eu/index.php?id=libraryworking&dir=8.PSCE_Conferences/PSCE_Conference_Helsinki_2012/3. Keynote_presentations/Day_2&mountpoint=5
[10] J. Holmstrom, J. Rajamäki, and T. Hult, "The future solutions and technologies of public safety communications: DSiP traffic engineering solution for secure multichannel communication," *Int. J. Commun.*, vol. 5, no. 3, pp. 115–122, 2011.
[11] A. Kivimäki, *Wireless Telecommunication Standardization Processes—Actors' Viewpoint* (Acta Universitatis Ouluensis A Scientiae Rerum Naturalium No. 483). Oulo, Finland: Oulu Univ. Press, 2007.

VT

VIII

MULTI-SUPPLIER INTEGRATION MANAGEMENT FOR PUBLIC PROTECTION AND DISASTER RELIEF (PPDR) ORGANIZATIONS

by

Jyri Rajamäki & Markus Vuorinen, 2013

Proceedings of The International Conference on International Conference on Information Networking (ICOIN), 2013, 499-504

Multi-Supplier Integration Management for Public Protection and Disaster Relief (PPDR) Organizations

Jyri Rajamäki
Laurea SID Leppävaara
Laurea University of Applied Sciences
Espoo, Finland
jyri.rajamaki@laurea.fi

Markus Vuorinen
HP Enterprise Services
Hewlett-Packard
Espoo, Finland
markus.vuorinen@hp.com

***Abstract*—Cloud sourcing and multi sourcing are growing rapidly and are success criteria's for today's IT departments. IT services are often operated by multiple suppliers but only very few of the client organizations are getting planned savings and service quality within multi-supplier environment. The Information Technology Infrastructure Library (ITIL); Service Level Agreements (SLA) Management; Enterprise Service Management (ESM); Responsible, Accountable, Consulted, and Informed (RACI) matrix and selective sourcing practices have been created to respond to this problem but never aligned to be jointly used during service lifecycle. This paper presents a model how multi-supplier environments should be managed. New method presents how existing frameworks should be aligned from service management point of view. An attention is taken how Public Protection and Disaster Relief (PPDR) organizations should choose their service delivery model. Especially, if delivery is a mixture of in-house, outsourcing and cloud sourcing services, how to clarify the responsibilities, operating model and scorecards between suppliers? This new aligned model is described also graphically and the achieved benefits are described in detail.**

Keywords*— IT governance; IT outsourcing; multi supplier management; public protection and disaster relief; public safety; service management

I. Introduction

IT departments are struggling with same problems about sourcing methods around the world. Organization's IT services requires several suppliers to run – usually different suppliers to operate e.g. software, hardware and network – and as the suppliers are usually competitors to each other there is hardly any collaboration between them unless strongly supervised by client. Industry is lacking of framework to manage multi-supplier IT service sourcing. Several companies are specialized to only certain areas; some companies are very effective at proving utility services, some at traditional outsourcing and some IT services are most effective when insourced. Ways to use and manage IT services are extremely diverted. IT governance methodologies have not been developed to respond for such a challenge. IT governance has been lacking of a single framework to use for choosing sourcing strategy and is causing that suppliers are not collaborating enough and clients are facing problems with managing multiple service providers – both internal and external. At the same time organizations are not aware if their current practices are mature enough for multi-supplier management, why they should use multi sourcing and how to measure if it is successful.

There are wide differences in the operation frameworks applied to outsourcing; the vast majority of outsourcing disciplines assumes a one-to-one relationship between the client and the service supplier [3]. However the IT service management is usually complex and only very seldom the whole IT-service base is managed by a single supplier. The everyday principles have been designed for operating with a single supplier whereas in real-life the IT services are managed by multiple parties.

"By 2006, 80 percent of Type A enterprises (leading-edge technology adopters) will externally source at least 60 percent of their IT-related services (0.7 probability)" [7]. Based on this information all organization needs to be able to effectively manage their IT-suppliers and services in order to stay competitive. Supplier management has become a success criterion for all organizations. Many of the organizations are using multiple service providers but only very few of those are achieving the targeted expectations with multi-supplier sourcing model. [12]

Public Protection and Disaster Relief (PPDR) means critical public services that have been created to provide primary law enforcement, firefighting, emergency medical, and disaster recovery services for the citizens of the political sub-division of each country. PPDR services bring value to society by creating a stable and secure environment. PPDR organizations have specific requirements for their IT services, e.g. in the field of robustness and cyber security. They are public organizations having national procurement legislations that e.g. in the EU derive from the European Community directives on public procurement. Under these rules public procurement must follow transparent open procedures ensuring fair and non-discriminatory conditions of competition for suppliers. These regulations aim at (1) a more efficient use of public funds in order to ensure value for money on public procurement financed out of general taxation; and (2) to enhance the competitiveness of national and European enterprises. When procuring e.g. IT services, the contracting PPDR must take advantage of existing market conditions and improve the functioning of markets.

Multi-supplier management is an important but complex area for all organizations. The purpose of this paper is to study how PPDR organizations should operate within multi-supplier service base and create framework responding to this problem. This paper describes essential frameworks and practices to improve organizations success in their sourcing strategies. Earlier researches show that utility based computing, smart sourcing and Responsible, Accountable, Consulted, and Informed (RACI) matrixes are effective tools in supplier governance [1]. This paper proves that these can be combined to support The Information Technology Infrastructure Library (ITIL) based service design that helps organizations to use effective methodologies for smart sourcing, responsibility definitions, clear service levels agreements, assuring that services are responding to IT service strategy requirements and aligned to corporate IT services structure. It is suggested that all these guidelines should occur in different phases of service lifecycle management. Together with Enterprise Service Management (ESM) framework this provides organizations with toolkit for successful sourcing strategy. This paper will discuss the problem about the frameworks and practices originally created for one-to-one client-supplier services when working in complex multi-supplier environment.

II. FRAMEWORKS AND MODELS FOR IT GOVERNANCE

A. *ITIL - Continuous Service Improvement*

First, The Information Technology Infrastructure Library (ITIL) offers framework to delivery of IT services. It is not only the best practice framework but also a philosophy shared with people who work with IT service management [6].

The fundamental service principle of ITIL is based on five phases of IT service lifecycle; Service strategy, Service design, Service transition, Service operation and Continuous service improvement [6]. Fig. 1 describes these five phases and their relationships.

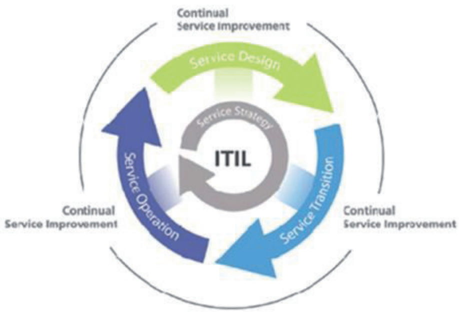


Figure 1. ITIL – Service Design [5]

Service strategy is the core axle in center of design, transition and operation phases and continuous service improvements including the projects, learning and programs which improve the inner circles performance and quality. [6]

B. *RACI Model*

The RACI matrix is used to define role and responsibilities between the organizations. This RACI matrix captures cross supplier dependencies, roles and responsibilities for all suppliers in multi-supplier organization. Following are the definitions of each of the roles: “Responsible” the party authorized to execute the activity, “Accountable” the party that owns the “bottom-line” for the activity, “Consulted” the party involved in providing inputs to the activity and “Informed” the party informed on the outcome of the activity. [3]

Using RACI Matrix to define the clear responsibilities between suppliers is key factor to succeed in supplier management. In multi-supplier environment the roles of suppliers might be similar but responsibility might differ [3]. Therefore, it is crucial to understand clearly and document the roles between suppliers and customers. Table I is an example which describes the different activities in rows and the parties with corresponding roles in columns.

Suppliers in multi-sourcing engagements which are individually accountable for their Service Level Agreements (SLA) are not usually accountable to each other. Here rules provide a framework for collaboration and co-ordination among suppliers. Development roadmap involves creation of supplier dependencies between the suppliers and determination of gaps in their management. An Operational Level Agreement (OLA) should be created to manage interdependent relationships between different suppliers to describe responsibility of supplier towards other suppliers. [15]

The process of creating these rules needs to be done by a core group which includes authorized supplier representatives and the client organization. The client company’s role is important providing oversight responsibilities for implementation.

Unlike in traditional sourcing where a single supplier is given well defined work units and accountability, in multi-sourcing none of the suppliers is accountable for the entire scope of work. Also, the rules of public procurement bring its own challenges in the field of PPDR. Scattered accountability makes supplier coordination and collaboration difficult for the client. Supplier governance through effective implementation of RACI matrix can help the client organization extract the most value from its supplier network.

C. *Enterprise Service Management (ESM)*

Hewlett-Packard has published a framework shown in Fig.

TABLE I. RACI EXAMPLE [1]

Function **R=Responsible, A=Accountable, C=Consulted, I=Informed**	**Helpdesk (Vendor A)**	**Infrastructure (Vendor B)**
Incident Management Tool/Application Maintenance	I	I
System Monitoring & Alerts		A/R
Application Monitoring and Alerts		C
Incident Logging: Assign Severity, Priority, Application	A/R	I
Incident Escalation	A/R	I
Incident Response	I	A/R (if System)
Incident Closure	A/R	
Permanent Fix/Follow-up Activity	I	I
Applications Incident Reporting: SLA, Root Cause, Permanent Fix		I
Infrastructure Incident Reporting: SLA, Root Cause, Permanent Fix		A/R

2 [12] for organizations to manage with multiple suppliers. This framework describes the key points about the benefits and challenges for multi-sourcing. How can be defined if such is required and basic measurements to say if it's effective or not.

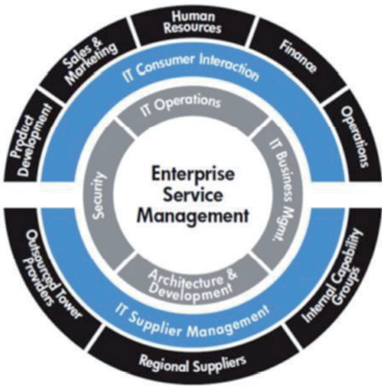


Figure 2. ESM Graph [12]

Most of the organizations applying multi-sourcing are facing regular challenges and only very few has been able to achieve their expected targets [12]. Multiple governances, processes, different reporting's and support tools are killing the benefits of multiple suppliers and actually making it less effective than operations with single supplier in most of the cases.

In order to make multi-sourcing possible and right way, it must meet four criteria's: (1) Transforming organization processes, governance and policies to support multi-supplier operations must create an aggressive transformation plan which usually requires at least two years' time and approximately 5% increase in IT operations spending. The transformation plan must be supported by the executives of the organization. (2) Organizations must define why they are looking for multi-supplier possibilities. Are the reasons cost savings, service quality, flexibility or something else? These reasons must be tangible and measurable. (3) Organizations must evaluate their current IT practices and evaluate which of those are mature enough with multi-supplier practices or those need further development. (4) When organizations have defined the areas and objectives, they should prefer a phased approach towards the multi-supplier model rather than a 'Big Bang' approach. [12]

In ESM model, the IT supply and IT demand organizations are separated. The ESM framework makes the IT services as single interface towards the users of IT services. Users could request any service from the corporate service catalogue or be working in any division or in any country and they all would have single interface for requesting the IT services. The service providers are invisible behind the corporate IT ESM framework interface. Ultimately if the users are satisfied with the service quality provided through multiple suppliers the model is working fine.

The challenge with ESM model is for the IT organizations to have all suppliers aligned with corporate IT Operation, Security and architecture policies and practices while still constantly developing those through business demand management. The requirements for the suppliers must be aligned for the policies and services provided to the end users. If any of the suppliers is not compliant with organization's requirements for IT suppliers they should not be used. Noncompliant service providers would make corporate services weak if some of the providers can't commit to tools, SLA's or processes required.

D. Utility Based Computing

The traditional outsourcing business is emerging with new business models. The applications are merging more and more Web-based which enables new type of "Software as a Service" (SaaS) model. Other trend is server virtualization which is driving capacity based datacenter usage a bit further, known also as Infrastructure as a service (IaaS). Tomorrow's IT is more and more based on services provided over the network as a utility services similar to water or electricity today. [2]

Organizations are moving from Outsourcing to Cloud sourcing. For the client the management of utility based IT infrastructure where mailboxes are charged per mailbox monthly rather than buying servers, licenses and performing the installations have a big difference. The cloud services are doing the same revolution for IT that industrial revolution brought to manufacturing. The provisioning of services is consolidating to fewer suppliers and with automation and large volumes the unit prices are going down. [10] Client does not any more need to know the technical details of how much memory server holds but his requirements for service. These requirements are more discussed in Chapter F.

There are risks to capitalize on the potential benefits of utility computing, client firms will rely more heavily on the technical — and perhaps business process — capabilities of suppliers. This reliance will reshape the risks associated with outsourcing. [2]

One of the challenging questions behind the utility computing is if strategic processes require certain IT- services to be available - what happens if supplier for any reason is not able or willing to provide that service? [2] In the worst case, this can lead to the lack of a particular PPDR service to citizens.

Partly due to the risks and the ongoing revolution of utility based services, the environment is in situation where the services are delivered in hybrid mode. The environment consists of both utility based services and traditional self-maintained and developed IT services. To manage IT consisting of various utility, outsourced and insourced services requires advanced frameworks for IT-governance to be effective. Governance model should be flexible enough to support the service strategy for both utility services and traditional IT services provided from both internal and external organizations. The study [14] figures out which cloud computing deployment model and cloud service model would be suitable for PPDR. The study shows that new Enterprise Architecture (EA) will reduce some of the problems that come when installing the programs locally when they are not intend to work that way. This EA also covers how to use cloud computing in the PPDR field [14].

E. Selective Sourcing

The consequences when organizations outsource only certain parts of their IT environment compared to alternatives outsourcing everything or nothing if known as selective sourcing or also as smart sourcing. A model where is defined key areas to be kept in-house. [13] These key-areas provide additional value when hold in internal organization, and less key areas that can be outsourced. This matrix is shown in Fig. 3.

		Commodity	*Differentiator*
Contribution of IT activity to business operations	*Critical*	Best source	Insource
	Useful	Outsource	Eliminate or migrate
		Contribution of IT activity to business operations	

Figure 3. Selective sourcing [13]

Areas that should be kept in-house are critical strategic differentiators, services that are critical to core operations. Nearly always these are critical differentiators are tailored applications which other organizations do not have.

Critical commodities are group which are required to run the operations but they do not provide additional value to them. A type of critical commodity is a system that is used only to fulfill legal requirements. As these could be standard commodity systems that customers are using usually the best sourcing option for these systems is suitable if there are high-quality suppliers available. [13]

Useful commodities are standard services such as email or accounting that supports the operations. This group is likely to have lower costs through external suppliers outsourcing through standardization and volume. Standard and often high-volume services could be often provided as utility services most effectively.

The last group is useful differentiators. Their problem is that they are always costly to maintain. They are usually tailor-made and require more management than standard systems. Outsourcing of useful differentiators does not help to run the costs down. These systems should be migrated or eliminated as they provide more costs than benefits.

PPDR organizations should use this matrix to categorize their services regularly in which group they are. For some organizations there could be plenty of useful differentiators which are costly to maintain and provides only a little operational value. Correct usage of the matrix helps organizations to focus on value adding IT services and eliminating or outsourcing non-value adding IT services.

In some cases the outsourcing versus insourcing is not financially as justified as one might expect. If client is large enough they could critical mass to provide same service as the supplier would. The difference is that external suppliers are also looking for a profitable margin for themselves. In such case that client has critical mass and client has managerial practices developed it can be cheaper to insource than outsource due to the fact that internal IT organization don’t need to be profitable. The aspects of volume and management skills are described in Fig. 4.

		Subcritical mass	*Critical mass*
Managerial practices	*Leading*	Best source	Insource
	Lagging	Outsource	Eliminate or migrate
		In-house economics of scate	

Figure 4. Supplier offerings vs. in-house capability [13]

F. SLA based management

A Service Level Agreement (SLA) is defined as a formal written agreement developed jointly between a client and a supplier that specifies a product or service to be provided at a certain level in order to meet objectives. SLA helps to clarify responsibilities, improve communication, reduce conflicts, and build trust between the companies [8], [9].

The service level management requires that there must be defined metrics to measure the service. The controlling of service is built on controlling the effectiveness of certain SLA’s. As there can’t be hundreds of different SLA’s the SLA’s in use must be well defined. There could be numerous performance indicators usually known as Key Performance Indicators (KPI). Sample performance indicators for any process could be process speed, process volume, errors in process or cost of process.

“Contractual elements under governance characteristics include communication plan (documenting communication processes to facilitate consistent knowledge exchange), measurement charter (specifying tactical measures of service performance), conflict arbitration plan (stating the parameters and conduct rules for involving a third party for resolving problems), enforcement plan (states appropriate incentives and penalties based on performance).” [8]

The changing of service levels should be possible during the contract period. The continuous change processes causes that requirements for service levels and quality are changing also regularly. Client should maintain the possibility to adjust Service Levels during the contract period. For example change the measurement of process time to process quality.

A weak IT service (with little redundancy or over-utilized resources) has the advantages of having low running cost but may generate high quality losses in PPDR field operations. A service with much better availability and lower response times will possibly generate better quality of PPDR field operations but have usually much higher running costs. Thus, in both cases, total financial outlay may be high. It appears that a middle ground can be found that will minimize this sum. [9] This is illustrated in Fig. 5. On Y axis there is the total cost and on X axis there service quality.

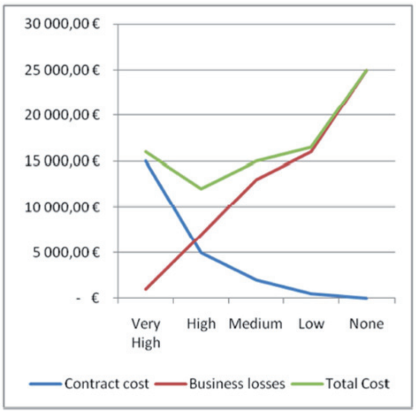


Figure 5. Total cost of SLA levels

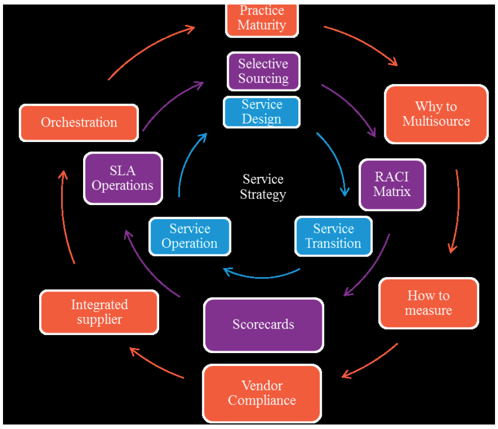


Figure 6. Selective sourcing, RACI matrixes, SLA's and ESM at the different phases of service strategy.

The SLA based management requires the key deliverables of supplier are well defined as well as the metrics for the service. Enforcing very high SLA requirements which are going above business requirement could cause very high running costs towards the IT service.

III. IT Service Governance Model for PPDR Organizations

The foundation for IT Service governance should be based on ITIL service management. The service strategy is the driving the service portfolio based on the operational requirements of PPDR organizations.

Fig. 6 shows our new framework for IT service governance. Around the service strategy is the cycle for planning, implementing and operating services. The input for service requirements is coming from inside from the service strategy.

Within the service design phase, it is planned how the service should be delivered. For service design there are alternatives from standard utility servers to the tailored in-house systems. The aspects of utility based computing and selective sourcing should be planned as shown in Fig. 4 and Fig 5. Is the service something is effective to operate in-house? Is the service something that can be provided cost effectively as cloud/utility service? Main sourcing strategy for the service is chosen at this stage.

Next phase is the service transition, where the service is implemented and defined in detailed level within the service operating model. In order to assure effective governance model in the service transition phase, a RACI matrix should be created. The matrix informs the deliverables and responsibilities between client and the suppliers. Creating a RACI matrix assures that during service operation phase all roles and scope are defined in advance and the service can be operated. Based on the RACI matrix and the service deliverables can be started design of Service Level Agreements (SLA's) and other Key performance indicators (KPI). These service levels will be in the agreement between suppliers and client.

The final service operation phase is when the service is in production phase and used. Based on the responsibilities defined in service transition can be designed initial SLA measures for the agreement. This way can be assured that SLA's are in line with supplier accountability and are in line with deliverables, the SLA's must be flexible in order to maintain possibility to adjust those based on changing business requirements.

The ESM framework is guiding to check the readiness for sourcing at different phases of service design. Is the organization ready for multi sourcing, what are the targeted benefits, how those can be measured, are the suppliers compliant with PPDR requirements, how to migrate it to an integrated supplier and in the operation phase is some further orchestrations required? The ESM practice is described in outermost cycle.

IV. Discussions

If the multi-supplier governance on service strategy is done based on described practices there can be gained several benefits. The ITIL service strategy is divided into three phases, design, transition and operation. In this chapter the benefits are described for each phase.

The decision about what and how to outsource is done in design phase. There are areas which are more effective to be outsourced and some areas where insourcing is more effective. Further there can be some areas where utility based services are more effective than traditional services. Using this framework gives organizations the right sourcing solution from the start. The ESM practice also guides to answer why that is being done.

Within the service transition phase, the RACI matrix usage will clarify in clear documented form the responsibilities between the client and suppliers. If this RACI matrix is done prior service operation phase a lot of problems during the operation can be avoided when all gaps and responsibilities are defined in advance. Based on the responsibilities defined in service transition can be designed initial SLA measures for contract. This way can be assured that SLA's are in line with supplier accountability and are in line with deliverables. What is measured and how.

Prior going to service operation phase the service compliance must be verified that they are compliant with PPDR service and policy requirements and assign correlating scorecards.

The service operations phase is the phase where service is operation and supplier has integrated to part of PPDR services. During this phase the service is reviewed and performance evaluated if there are requirements to change the SLA levels. The benefit of adjusting SLA measures and levels at this stage is to have service levels responding to the business requirements.

In brief the model will allow multi-supplier governance deliverables to be well defined, measurable, aligned, sourced best way and service levels to be adjustable based on requirements. This model also provides PPDR organizations with answers why they are multi sourcing certain activities, are they compliant with their service requirements and are the targets achieved.

VI. CONCLUSION

The multi-supplier governance has been well studied during the past years. Despite the research no standard best practices for managing multi-supplier governance are yet in place. ITIL and other Information Technology Service Management (ITSM) methodologies support and give certain advices for this matter but a framework is required in order to assure that the service quality in multi-supplier governance is high quality and meeting expectations by all parties.

This paper proposes a new framework for operating model in multi-supplier sourcing. This new model is combination of smart sourcing, usage of RACI matrixes and ongoing SLA management. These are toolkit for ESM making the companies and public organizations compliant with service requirement. When correctly applied, model will improve the service quality, supplier collaboration and cost efficiency of IT services. The proposed framework provides organizations with sourcing method aligned with corporate ITSM practices.

This paper has been written from IT Service strategy perspective looking at the overall picture of IT Services. The methodologies in multi-supplier management in ITIL core processes have not been studied. Multi-supplier operating framework for some of the ITIL main processes such as change management, incident management and problem management would be important to be studied to provide organizations with more practical approach in operational duties.

Each organization has their own requirements for IT services. When external suppliers are providing IT services there might inflexibility in standard services in multitenant service base. Supplier standard services might not respond to client requirements. The ways how organizations could manage the gaps between the supplier's standard services and clients requirements is vital to understand and study.

This method is not looking the dependencies between the different IT Services for multi-supplier service base but from single IT service perspective only. Synergies and/or conflicts between the IT services need to be studied multi-supplier service base.

Additionally, it should be investigated how governance practices for traditional outsourcing methodology differ from cloud sourcing governance methodology where the services are more fixed for multitenant especially in public cloud services.

REFERENCES

[1] M. Ramakrishnan and V. M. Pro,. "IT Program Governance in Multi-supplier Outsourcing", *SETLabs Briefings*, vol. 6, no. 3, pp 19-22, 2008.

[2] J. W. Ross and G. Westerman, "Preparing for utility computing: The role of IT architecture and relationship management," *IBM Systems Journal*, vol. 43, no. 1, 2004.

[3] M. Gallivan and W. Oh., "Analyzing IT Outsourcing Relationships as Alliances among Multiple Clients and Suppliers," *Proc. 32nd Hawaii Int. Conf. on System Sciences*, IEEE, Georgia State University, 1999.

[4] M. Debusmann and A. Keller, "SLA-Driven management of distributed systems using the common information model", *Int. Symp. on integrated network management*, 2003.

[5] *ITIL V3 Foundation Bridging Certificate Course*. ALC Group. Available: http://www.alc-group.com/itilv3_info.php

[6] *IT Service Management based on ITIL V3*, itSMF International, Van Haren Publishing, 2007, pp. 19-126.

[7] "10.0 Best Practices in Data Center Outsourcing," in *Next-generation Data Centers.* Gartner, 2005, pp. 140-151.

[8] J. Goo, "Structure of service level agreements (SLA) in IT outsourcing: The construct and its measurement," *Information Systems Frontiers,* vol. 12, Iss. 2, April 2010, pp. 185-205.

[9] J. Sauvé *et al.*, "SLA Design from business perspective," *Proc. 16th IFIP/IEEE Ambient Networks Int. Conf. on Distributed Systems: Operations and Management*, 2005, pp. 72–83.

[10] S. Wardley, "Cloud Computing - Why IT Matters". presented at the OSCON (Open Source Convention), July 20-24, 2009, San Jose, California.

[11] J. Erbes, HP Labs Director, US Texas, private communication, Feb. 2. 2011.

[12] P. Yates. (2012, Oct.) *Successfully manage multiple suppliers* (Rev. 3). Available: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA2-9014EEW.pdf

[13] M. Lacity *et al.*, "The Value of Selective IT Sourcing," *MIT Sloan Management Review*, April 15, 1996, pp. 13-25.

[14] J. Lehto *et al.*, "Cloud computing with SOA approach as part of the disaster recovery and response in Finland," *International Journal of Computers and Communications*, vol. 6, iss. 1, 2012, pp. 175-182.

[15] T. Herz *et al.*, "Mechanisms to Implement a Global Multisourcing Strategy." *New Studies in Global IT and Business Service Outsourcing*, vol. 91, 2011, pp. 1-20.