The SATERISK project studied risks associated with satellite based tracking, specifically whether the use of tracking generates additional risks. The project analyzed risks using different approaches: legal, technical and how the tracking is used. It also tried to find solutions that could help us avoid the risks in the future.

The base of the SATERISK project came from a five-credit development assignment of two Laurea's graduate students in spring 2008. Soon, the burning issue expanded not only to an academic multi-disciplinary collaboration with the University of Lapland, ITMO in St. Petersburg, Russia, and the BORDERS network coordinated by the University of Arizona, USA, but also to a collaboration with four companies using satellite based tracking on daily basis, as well as government officials such as customs and police. The main sponsor of the SATERISK project was the Finnish Funding Agency for Technology and Innovation, Tekes.

"So, you should be careful when choosing your research subject, you never know where it may take you!" stated Jouni Viitanen, Laurea's graduate student in 2008-2009.

Project information

Project name	SATERISK
Project type	Research project
Tekes' funding share	260400 €
Tekes' program	Safety and Security
Start date	9/1/08
End date	12/31/11

Contact information

Company/Organization	Laurea-ammattikorkeakoulu Oy
Research Director	Dr. Jyri Rajamäki

LAUREA JULKAISUT | LAUREA PUBLICATIONS

ISSN 2242-5241 | ISBN 978-951-799-268-8 (NID.)

LAUREA UNIVERSITY OF APPLIED SCIENCES *Prime Mover*

SATERISK Risks of Satellite Based Tracking Sample of Evidence Series: Volume (2)

Jyri Rajamäki, Rauno Pirinen and Juha Knuuttila (eds.)

SATERISK

Risks of Satellite Based Tracking
Sample of Evidence Series: Volume (2)

LAUREA LEPPÄVAARA *Service Innovation and Design*

LAUREA JULKAISUT | LAUREA PUBLICATIONS

Jyri Rajamäki, Rauno Pirinen and Juha Knuuttila (eds.)

SATERISK

Risks of Satellite-Based Tracking

Sample of Evidence Series: Volume (2)

Laurea-University of Applied Sciences, Leppävaara Unit
2012 Vantaa

Technical editor: Mari Aro (body text) & Oskari Kolehmainen (cover)

Cover picture: iStockphoto

ISSN 2242-5241
ISBN 978-951-799-268-8

Edita Prima Oy, Helsinki 2012

Table of Contents

Foreword

I graduated from the Laurea University of Applied Sciences Security Management Program in spring 2003. I continued my studies in the beginning of 2008 by taking part in The International Security Management Specialisation studies in Laurea Leppävaara. By then, I was aware that the first ever Master Program in Security Management in Finland would start later in the autumn of 2008 at Laurea, and I thought that these specialisation studies might be a good start.

In February 2008, I was looking for a subject for my thesis in studies of International Security Management, which could also be useful in my office in the Law Enforcement Authorities (LEA). In my office, I have been involved in projects where Global Navigation Satellite Systems (GNSS) based tracking has been the key technology. Therefore, I was worried about how it was used. It seemed that people were mainly only considering the advanced effects of tracking, and that they were not aware of the risks involved. That is how I came up with the idea to study the risks involved in GNSS tracking. Originally, the research was meant to be only for five credits, and I thought that I could only scratch the surface of the subject. Fortunately, my old friend and colleague Jussi Ojala, who was using tracking technology in his daily work, was also participating in the same specialisation course. To get a wider perspective on the subject, I asked him to join this research.

With Ojala, the research subject was formulated: Research problem: Is GNSS tracking generating risks? Points of view: 1) concentrating more on risks than on legislation; 2) of those who decide about the use of tracking; and 3) trying to find something that could help us avoid the risks in the future.

Our first draft paper was formulated on 12.2.2008, and it was sent to Laurea's Principal Lecturer Juha Knuuttila. His feedback was something that we had never expected. Knuuttila told us that the research should be much wider and thorough than planned, and that Ojala and I should start writing the research funding application to TEKES. That meant much more work than those original five credits! Calling together the consortium that was needed took a long time. Anyway, the task was so interesting that neither I nor Ojala counted the working hours anymore. With the help of Knuuttila and Dr. Jyri Rajamäki, we managed to get the consortium together, and

TEKES accepted our application for the project. That is how the project SATERISK was born.

Besides that, the project SATERISK also affected our personal lives. The following year, I took a leave of absence from my LEA office job and became a Senior Lecturer in LaureaSID Leppävaara. Ojala also worked as a full-time worker in the SATERISK project for a few months. After that year at Laurea, I returned to my LEA office, but I am still working as a part-time lecturer at LaureaSID.

So, you should be careful when choosing your research subject, you never know where it may take you!

Tuusula 7.2.2012
Jouni Viitanen
Laurea University of Applied Sciences

Preface – Technology Develops Taking International Cooperation to New Level

Customs joined the SATERISK research project steering group in February 2009. The use of positioning systems in a national and international operating environment has been widely studied within the framework of the 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 ambitious objective of the project is to create new and better operational models by recognising the risks, and to support the research and development of positioning branch and hardware and system suppliers.

The project also maps out what the future systems and new technologies should make possible by taking into account authorities and private-sector organisations that use positioning systems.

The positioning systems are widely used by private-sector companies in cross-border traffic for localisation of consignments, equipment and vehicles. In the public sector, the positioning systems are used to establish a picture of the situation and to support law enforcement. In the future, the picture of the situation will also be needed by security and other companies involved in positioning. On the other hand, the public sector may, in the future, utilise the positioning of vehicles for taxation of use. The project also highlights the necessity of cooperation between the public and private sectors for development and use of this technology.

As a result of the research carried out during the project, Finnish security companies have received new international know-how. In the future, the results of SATERISK can be utilised as a part of the above-mentioned development, and it might produce new research objects. The parties involved in the project have also built the basis for the cooperation between public and private sectors required in the future.

From time to time, the department stores of international organised crime have used satellite positioning more effectively than the authorities, for example, for the concealment of drug trafficking. Often, effective international activities of the authorities 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 and the EU and ESA as a result of which the law enforcement authorities could seamlessly and reliably exchange positioning information of cargoes of special interest.

The use of advanced technologies in Customs work has become increasingly more 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. Accordingly, this project will support operative cooperation between Customs and other authorities while creating business opportunities for security companies. Hopefully, these opportunities can now be utilised effectively.

Helsinki 24.4.2012
Tapani Erling
Director General
Finnish Customs

Preface – GNSS; from Security Applications to Secure Everyday Use

On October 4, 1957, the USSR launched the Sputnik 1-satellite. Scientists at the Johns Hopkins University used Sputnik's radio signal's Doppler effect to work out the satellite's orbit. They soon realised that for a known orbit, the solution can be reversed: one can use satellites to work out the position of a receiver on earth. The US Navy built the Transit satellite navigation system in the early 1960's for its submarines carrying Polaris-missiles in the Arctic Ocean. In the 1970's, the US Air Force designed a satellite navigation system for all US military arms. NAVSTAR GPS was a much more complicated system based on codes, atomic clocks and signal transfer time. GPS became formally operational in 1993. It became increasingly more open to civilians in 1983 (KAL 007), in 1991 (Gulf War) and in 2000 (end of "Selective Availability"). The civilian applications for satellite navigation started from sailing in the 1970's; then, merchant marine and aeronautical uses started to emerge. Prices of navigation equipment were in the tens of thousands of dollars.

In the year 2000, European Galileo's design work had started, Russia was planning to recreate its GLONASS, and China planned the Beidou/Compass systems. At this time, mass market for GPS-equipment was born in the form of car navigation, Dutch TomTom being still the most notable name. The situation rapidly changed from then on: cellular phones started to carry GPS-chips. At the moment, 99% of GPS use is in cell phones and car navigation.

GNSS, i.e. using of more than one navigation satellite constellation, started in 2010: a great deal of equipment now use GPS and GLONASS satellites together for positioning. Compass and Galileo will be ready in less than 10 years – in 2020 the number of navigation satellites will be well over 100. This will improve navigation accuracy and availability.

In 2012, the use of atomic time coming from navigation satellites is seen e.g. by the UK as a critical issue since it uses GPS-time to synchronise its cell phone networks, ATM machines etc. Independent time is one of the reasons why large countries have wanted to build their own systems. India is currently deciding whether it will also develop its regional INRSS system into a global GNSS system.

Finnish use and research in satellite navigation started in the 1980's. Many of the companies that work in this field were founded in the 1990's. Fastrax is the only Finnish component designer and maker: its products are widely seen as the most powerful and least power consuming. It has also developed software navigation solutions that will enable using all types of navigation satellites, and in the future also other radio signals for navigation. Nokia has a natural role in GNSS, and this role lead it to purchase Navteq-company - now the digital maps are seen as its major asset. The tens of other Finnish navigation companies are SME's that work in applications such as fleet management (trucks, taxis), logistics, leisure (sports, hunting), wellness (elderly, children) and security. In research, e.g. Tampere University of technology, Finnish Geodetic Institute and Laurea University of Applied Sciences are performing research in this field funded by national sources and by the European Commission.

During the last dozen years, companies have also been able to develop products and services for small and local markets. The sales growth of navigation equipment has been more than 10 per cent per year. Thus, the business has room for new companies to enter and old ones to grow. Being a start-up in GNSS is easier than in many other fields of B2B electronics. Now new services, such as car parking in cities, are searching for business models. Changes are expected when giant companies in electronics (e.g. Apple), software (e.g. Microsoft) and the internet (e.g. Google) are entering the radio navigation arena.

Indoor (and in city) navigation are expected to be the next "new thing" once the issue of compatibility of systems, i.e. standardisation, and division of costs of the local infrastructure are solved. Technologies for local navigation augmentation systems, pseudolites, have been developed e.g. at Space Systems Finland. The use of local augmentation to GNSS is needed e.g. in ports and open mines. Non-satellite-based navigation systems for in-door navigation have been introduced in hospitals in Finland and in the United States by e.g. Ekahau. Similar technologies are likely to emerge first in large shopping centres and amusement parks, then everywhere. 3D mapping and 3D models of cities are part of the urban navigation development. Laser scanning is seen as one way to efficiently create 3D models of cities.

Seamless use of GNSS and other navigation systems (e.g. inertial navigation) is a hot topic in research (e.g. FGI). In the military world, the USA has been developing the concept of navigation warfare using “whatever known signal” for its troops’ navigation. This concept is likely to enter civilian navigation later on.

Legal aspects, such as privacy, have finally started to emerge. Some of the legal issues fall into the field of international law because people and things cross borders. These issues have been researched during the last three years by the University of Lapland in the SATERISK project.

Legal demands by governments for e.g. traffic can be useful to force a change. To foster the use of its GLONASS system, Russia is using the treat of import taxes to “GPS-only”-devices. It is also starting to implement ERA-GLONASS, a system for road safety, in all new cars. The system is quite similar to the European Union’s eCALL, which is a system that helps people in traffic accidents. Thus, Russia and the EU believe that security applications in road traffic could be beneficial for the further development of satellite navigation use in Europe. They are likely to be right. The legislation for the transport of animals in the EU and the transport of dangerous goods on roads are already now in place. Both rely on the use of GSP navigation. In Finland, the Ministry of Transport and Communications and VTT are developing intelligent transport systems involving GNSS. Satellite navigation has relied on the infrastructure in space (GPS satellites), but for further applications, ground infrastructure investment is needed, existing cell phone networks being a major part of it.

The security aspect of “everything sending its position” (through GSM) has risks – especially in the transport of valuable property. The civil security arm (emergency vehicles, fire trucks, ambulances, police cars) are, in a way, a living laboratory for the security issues of GNSS navigation. The decision making of these organisations is based on goals of cost reductions - this makes them cautious customers in the purchasing of new systems. In large countries, e.g. France, the civilian security sector can be the early user that drives change is the use of GNSS.

Military requirements defined the first 30 years of satellite navigation, and then transportation took over. The last years have diversified the GNSS applications and brought the navigation technologies to portable computers and cameras, etc. In business - e.g. Walmart’s use of RFID as a tool for its logistics - and institutional environment, legal, safety and security aspects are becoming more important every day. Laurea's SATERISK project has done extensive research in the security aspects of satellite navigation.

Helsinki 4.2.2012
Pauli Stigell
Tekes, Environmental Data and Space Applications.

I Introduction

Jyri Rajamäki, Robert Guinness and Seija Tiainen

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. The European Commission launched its first two operational satellites for the Galileo positioning system in October 2011. Amongst all of these developments, Laurea University of Applied Sciences led a research project to investigate the risks associated with satellite-based tracking.

The SATERISK (SATEllite positioning RISKs) 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, end-users, and authorities to clearly understand these risks and take steps to mitigate them.

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—both in the public and private sectors—where the risks could be high if they were not properly addressed.

The SATERISK project had partners and other participants from the whole value-chain of satellite-based tracking; starting from the network operators like Cassidian Finland (EADS DS when SATERISK started) to companies that offer information-gathering devices and tracking software, and finally to the users of these tracking systems, such as Finnish Customs. The legal aspects of satellite-based tracking were studied at the University of Lapland in its own SATERISK co-project.

Students participated in many interesting projects related to SATERISK and have over 1600 credits from that work. One interesting area of student work was the evaluation of risks from satellite-based tracking in different corporate sectors and for different use cases. Studies of current risks were followed by producing risk scenarios for the future. Another interesting area was developing service innovations that use satellite-based tracking. Finally, students organised and participated in seminars about SATERISK, including "Situation Scope" seminars 1-3 and the "Building Trust on Borders" seminar, giving students an opportunity to interact directly with experts and practitioners working in this field.

Thus far, the results of the SATERISK project have mainly been featured in various publications, conferences, seminars, workshops and theses. About twenty peer reviewed articles have already been produced, addressing various aspects of the project. Some of the most extensive results can be found in the theses of students who have participated in SATERISK. For example, Pasi Kämppi's (2011) master thesis "Grounded View to Technical Risks of Satellite-Based Tracking Systems: A Multimethodology Research" contains the results of extensive field tests and analysis of many different uses of satellite-based tracking. It won the best thesis of the year 2011 award in Finland. In 2011, about 20.000 students graduated from universities of applied sciences and 20 awards were honoured.

1.1 Research Methodology

Jyri Rajamäki

Neither computer science alone with its technical solutions nor psychology or other behavioural disciplines are able to address the challenges of today's security problems in a 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 lab. (Nunamaker 2010.) 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 by Nunamaker, Chan and Purdin (1991). 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 (March & Smith, 1995; Van Aken, 2004; Hevner, March, Park, & Ram, 2004). DR and DSR are research approaches that can be combined with other social science methods, such as the grounded theory or action research as well as case study research.

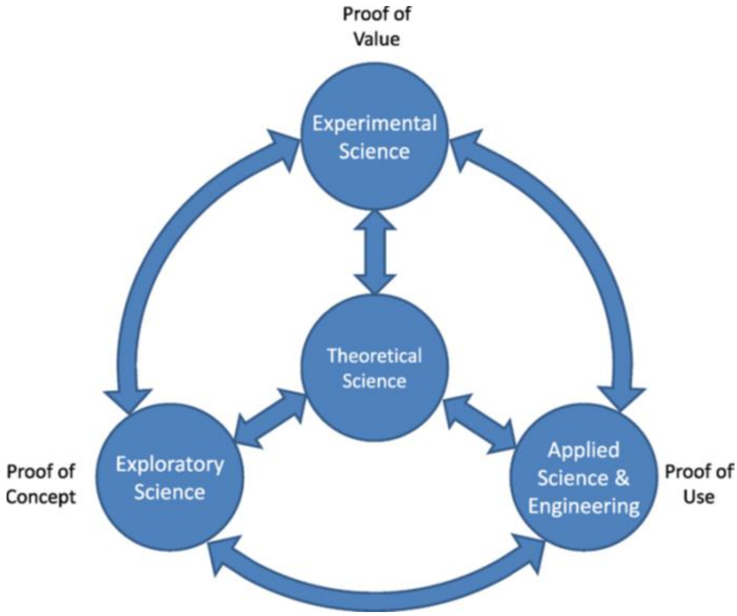

Figure 1: Integrated, multidisciplinary, multi methodological development research

According to Nunamaker's (2010) "going the last mile" approach, 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 had fretted about how it had been used. Nunamaker continues that the creation of innovative artefacts includes three phases: proof of concept (POC), proof of value (POV) and proof of use (POU). This means that a designed artefact is not really understood and cannot really be evaluated before it is actually implemented. In addition to POC and POV, they should also strive for POU. The SATERISK project integrates science both in the lab and in the field (see Figure 1), including the theory, prototype and validation by experiments or field study.

This report collects and summarises the main research result of the SATERISK project. The report consists of abstracts and summaries of earlier published, mostly peer-reviewed articles and conference papers. It also includes abstracts of selected theses and international workshop presentation abstracts. The results are divided into five topics; chapters 2 – 6 of this report. Each of these chapters contains an introduction to the topic, selected abstracts, discussion about findings and references. Chapter 2 introduces the SATERISK project and Laurea's integrative student-centred research and development model; how the student-centric research and development work is integrated into learning as an actualisation instance of the Learning by Developing (LbD). The learning activities have shifted the focus of traditional teaching methods to learning by taking part in authentic research, development and innovation work. In this way, the students are participating in authentic R&D&I, and they occupy the main active role in Laurea's collaborative R&D&I processes.

Satellite-based tracking and navigation systems are very complex. Chapter 3 is focused on the technical risks of these systems, chapter 4 concentrates on operational risks, and chapter 5 tackles risks occurring from legislation. Chapter 6 studies new services and risks in the future. Chapter 7 is précised differently, including no abstracts of earlier studies. On the other hand, it concludes the main results of the SATERISK project and shows how Laurea's other safety and security-related research projects are linked together. It also presents future research topics. The last part of this report contains the list of the publications produced during the SATERISK project.

References

Hevner, A., March, S., Park, J. & Ram, S. (2004). Design science in information systems research, MIS Quarterly 28, No 1.

March, S. & Smith, G. (1995). Design and natural science research on information technology, Decision Support Systems 15.

Nunamaker (2010). Interview with Jay F. Nunamaker, Jr. on "Toward a Broader Vision of IS Research", Business & Information Systems Engineering Issue 5.

Nunamaker, J., Chan, M. & Purdin, T. (1991). Systems Development in Information Systems Research, Journal of Management Information Systems. Vol. 7, No. 3.

Van Aken, J. (2004). 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.

2 SATERISK, Integrative Student-Centred Research and Development Project

Jyri Rajamäki and Rauno Pirinen

2.1 Background and Planning of the SATERISK project

Jyri Rajamäki

The idea to study the risks of satellite-based tracking came from two graduated students of Laurea Service Innovation and Design (SID) Leppävaara in 2008, Jouni Viitananen and Jussi Ojala. With the help of principal lecturers Juha Knuuttila and Jyri Rajamäki, they found partners for the project and received funding from Tekes, the Finnish Funding Agency for Technology and Innovation. The project started in September 2008, and Viitanen (2009) compiled the planning and requirements analysis of the SATERISK project in his master thesis.

Viitanen, J. (2009). SATERISK-projektin suunnittelu ja vaatimus-määrittely. (Planning and Requirement Analysis of the SATERISK Project). Master thesis. Theseus. Espoo: Laurea, (in Finnish).

*Abstract: **The** SATERISK project's goal is to find all the risks involved in using satellite navigation. Tracking is used to decrease risks in logistics and optimize workflow. We need to know what the risks and needs in legislation, as well as in tracking equipment and systems are in order to keep people safe.*

GPS satellite navigation system, commonly used in Western countries, will get a rival from EU: s own Galileo. Galileo will be operative in 2013[1]. It is timely to evaluate what the risks and needs are if we want to have guidance for future systems, legislations and regulations in general.

This requirement analysis is the first phase of the SATERISK project. What are those risks that must be tackled with in tracking systems, and the new technology used in them? Do we need new adaptive systems that can take care of security, legality and privacy issues, reacting actively to faced conditions and state of approved limits?

Is the lack of international legislation or user knowledge in tracking a risk? Is it possible that if you are tracking an asset in a foreign country, you might violate the local laws? Can the local authorities use other interpretations of law and think that tracking can, in fact, be seen as espionage? Is the tracker violating the privacy of the truck driver or other third party?

The goal of this project is that all the procedures used by security-oriented companies or authorities counter measurements by the criminals, legislation, and the business risks created by the all above are not preventing the use of tracking in international traffic. Most of this communication in tracking systems is machine-to-machine communication (m2m).

The SATERISK project was officially concluded in the end of 2011, but some of the project results are still under publishing procedure. In March 2011, the research director of the SATERISK project, D.Sc. (Tech.) Jyri Rajamäki, was invited to give a Plenary Lecture from vulnerabilities in satellite-based tracking systems.

[1] After the abstract has been written, the Full Operational Capability (FOC) of Galileo is postponed by this decade’s end (ESA 2012).

Rajamäki, J. (2011). Vulnerabilities in Satellite-Based Tracking Systems, Plenary Lecture, Proceedings of the 9th WSEAS International Conference on APPLIED ELECTROMAGNETICS, WIRELESS and OPTICAL COMMUNICATIONS, 24-26 March, Meloneras, Gran Canaria.

Abstract: Satellite-based navigation and tracking has become a routine feature of modern society and everyday life. Their use is still growing, as the EU's new satellite system Galileo is expected to be operational in the late 2010's. Especially in logistics, positioning, navigation and tracking are used to decrease risks and to optimize workflow. But it is questionable whether this is always the case. For example, when tracking is applied abroad, international legislation, or the lack of it, causes problems. From a technical standpoint, is a tracking system likely to increase the security of a valuable consignment? Or would these merely provide an additional resource to potential thieves? This lecture answers these questions.

2.2 SATERISK in Perspective of Learning and Regional Collaboration

Rauno Pirinen

It is noteworthy, that SATERISK is a Student-Centred and Student-Driven research and development (R&D) proposition (Viitanen, 2009; Ojala, 2011). It is a novel R&D scope which collaborates learning, mutual discursion and research in an interoperative way within a regional innovation system (Pirinen, 2009; Tarkkanen, 2009). Regarding my teacher's work, the SATERISK-related research investigations were addressed to two questions: First, how can learning within R&D be understood, designed, defined and actualised in a university of applied sciences (UAS)? Second, how can regional R&D be understood, designed, defined and actualised in higher education?

Because of the used cyclic research method, and the fact that the research data was continuously being enriched, the research data was collectively analysed while new data was being collected. While the research data became more enriched, preliminary interpretations of the data were conducted in the next phase of the study. The preliminary interpretations of the research data guided the continuous data collection process. Here, the first view takes an approach to the SATERISK learning environment within externally funded R&D and clarifies the modes of collaboration (Rajamäki & Fred, 2001).

Rajamäki, J. & Fred, M. (2011). Externally Funded Research, Development and Innovation Projects as Learning Environment. Proceedings of International Technology, Education and Development Conference, 7-9 March, Valencia, 4130–4139.

Abstract: Multi-disciplinary Research, Development and Innovation (RDI) projects can be regarded as learning environments that create new skills and competencies for all stakeholders: students, teachers, researchers, companies and public organizations. This paper presents an RDI project model that develops academic knowledge and competencies for all partners by solving real problems in real-life situations. We describe the model through a case-study of the research project SATERISK (SATEllite positioning RISKs) that was initiated by two security management students of Laurea University of Applied Sciences (UAS), that evolved into a substantial 3-year project (2008-2011) funded by the Finnish Funding Agency for Technology and Innovations (TEKES).

Finnish UAS students in adult degree programmes normally study alongside their work. A mandatory 3-year period of work experience after the Bachelor degree is required before a Master's level programme can be commenced, so that students can be regarded as experts, as they have experience in the specific area they are studying. The start of the SATERISK project was user-driven: the two students were working as police officers during their studies when they realized that there was very little discussion about the risk of satellite-based positioning and tracking. "Satellite-based tracking services are used to improve the security of property and personnel, but does the tracking involve new risks?" At first, the idea was developed in dialogue with lecturers and students; later on the dialogue was expanded to include a *more extensive network with other students, teachers, researchers, companies (both device and service developers and end-users), public end-users and publicly-funded expert organizations for financing research, development and innovations. SATERISK has expanded not only to an academic multi-disciplinary collaboration with the University of Lapland, ITMO in St. Petersburg, Russia, and the BORDERS network coordinated by the University of Arizona, USA, but also to a collaboration with four companies in the field of satellite based tracking, and government officials such as customs and police.*

Our RDI project model has its theoretical background in the Learning by Developing (LbD) approach model, which is used as a pedagogical model in Laurea UAS, combined with the "Last mile in research" approach developed by Prof. Jay F. Nunamaker, Jr. The two approaches support each other and make the RDI project a unique learning environment. According to Nunamaker, the IS research needs to be multi-disciplinary. Laurea UAS has 8000 students in e.g. the fields of business management, IT, security and service management. Our paper describes how the SATERISK project is integrated into the study units and studies in general, as well as providing a description of the roles of different stakeholders when creating a learning environment.

In these collective R&D projects, my research addressed the Student-Centred integration of education, R&D and regional development in the actualisations of study units within R&D projects, such as the phenomenon and scopes of the SATERISK project. I performed several inductive and evidence-based analyses, which included the research data regarding the SATERISK project, as data of integrated R&D and collaboration in higher education, with universities, participating in the world of work, and external funders, such as TEKES, as national innovation systems and R&D programmes of the European Union. The approach of my research is qualitative; it is based on a continuum of action research and case studies, where the common unit of analysis is a sample of evidence. My reasoning is inductive; it takes observed practice and evidence, rather than deductively formed prior theorising that prejudges reality. Next, in this chapter, the view takes the perspective of learning in the SATERISK (Pirinen, 2011).

Pirinen, R. (2011). Externally Funded Research and Development Projects in Perspective of Learning. International Journal of Engineering Pedagogy (iJEP), 1(3), 27-36.

Abstract: The focus of this study was on Stunted-Centred learning activity which collaborates learning and research in an interoperative way and shares the regional-national research and development (R&D) capabilities, interests and agenda. The study was addressed to the cooperation model and factors of learning within R&D projects that develop academic knowledge, competences and regional—national capabilities for all participants by contributing authentic R&D scopes or problems in real-life situations. The study included analysis of the research data regarding the R&D project, namely SATERISK, which was initiated by two security management students (Viitanen, 2009; Ojala, 2011) at Laurea UAS and that has evolved into a substantial three-year R&D project between 2008 and 2011 and was funded by the Finnish Funding Agency for Technology and Innovations (TEKES).

The study by Pirinen (2011) was journalized from the presentation at the International Conference of Interactive Computer Aided Learning ICL2011 and the evaluation of by the Finnish Higher Education Evaluation Council (FINHEEC) and its application in 2010 (Auvinen et al., 2010; Tarkkanen, 2009). In the study, the focus of our Learning by Developing (LbD) model has shifted from pedagogical orientation to learning within R&D orientation, and the LbD-model has gradually developed into a cooperational model, where Student-Centred learning integrates R&D. The study Pirinen (2011) presents triggers, drivers and enablers to the Student-Centred R&D and R&D-based learning. In addition, the study revises the sustainable driver model (Rajamäki & Fred, 2011) for integration of R&D to learning in the emerging thematic network in our Integrative Action Process.

In the perspective of the school of the future, this stream and change of the way of learning has also changed the leadership and management model of higher education institutions. The transformation lays in the view of the mode migration (Gibbons et al., 1994): from a coordination- and control-oriented leadership mode-1 into an expert-oriented model-2, where the attendees share a common vision, results, and influence of higher education in the region and society (Tarkkanen, 2009; Pirinen, Tarkkanen, & Teräs, 2009; Gibbons et al., 1994).

The studies of SATERISK represent the furthered steps in investigating the prerequisites to and factors of the learning for conducting R&D to integration in cooperation and R&D (Fränti & Pirinen, 2005). Here, the cooperating environment dialogue refers to future orientation, the national innovation policy, and the public-academia-industry relations as a cooperating culture that jointly develops knowledge and competences (Pirinen, Tarkkanen, & Teräs, 2009; Pirinen, 2009; Etzkowitz & Leydesdorff, 1998).

In SATERISK, R&D activities were based on student creation, upward-oriented ideation, and refining of R&D ideas, with a shift to customer-, user- and student-driven motivation (Viitanen, 2009; Ojala, 2011; Rajamäki & Fred, 2011; Pirinen, 2011). The strengths of the study lie in its findings regarding the significant change in learning, which denotes "allowing and throwing oneself into learning something new and novel within R&D" (Tarkkanen, 2009; Pirinen, 2009) and in students' competence-based changes and advantages, which were facilitated as sustainable drivers for lifelong learning (Pirinen, 2011). In this R&D union, students, working life and the region are learning in a collaborative and interoperative way (Auvinen et al. 2010; Saarela et al., 2009; Salminen & Kajaste, 2005).

In SATERISK, a project-specific, competence-based learning group was created for a student's created idea, which included the authentic view of working life. This new form of an integrative driver acts as a project preparation team, which is searching for R&D funding, and a collaborative R&D program is in a central role of learning. From this standpoint, the base of the learning scope is drawn from the student's motivation, expertise, and working life's body of knowledge, which was bridged to the competences by learning activities and integrative processes (Rajamäki & Fred, 2011; Pirinen, 2011; Rauhala, 2008). Here, our "collective mind" is co-considered for future, as understanding of the term "co-creation," which can be related to an activity of mutual creation, such as Student-Centred and user-centred approaches in design (Luojus, 2010). In this viewpoint, case-study research can be used for the beginning and improving of understanding of non-manipulated phenomenon, then a continuum of user-centred design (Luojus, 2010), and then building, improving and testing of service and artefacts; then furthered to the research of change in actualisation (Pirinen, 2011). In the end, the dissemination driver for R&D results would be much practiced; it would produce value and commercialisation advances, probable using of such methods as the last-mile research can make advances to this continuum and concept of R&D (Nunamaker, 2010).

One advance in the actualisation of SATERISK is that it takes evidence for binding and testing of different learning and R&D theories and development of new theories as sound kernel theories at the core of the LbD-model (Gregor & Jones, 2007). The variety of components, which operate as a connecting interface between R&D and learning, such as an artefact, a boundary object, a concept, a plan, an idea and issues, are influential in the context of integrative R&D. The role of these integrating components takes place in learning processes, where co-creative learning is collaborated in R&D, together with an innovation system, in which a regional and societal research agenda are described in the use of a variety of relatively new terms, such as research programs, research area and core strategies of science and lead innovations. In this, Rajamäki (2009) makes resonance with Pirinen (2008), the idea of elastic nature of R&D objects (an elastic R&D scope in learning) is expanded to the case of SATERISK.

Rajamäki, J. (2009). Elasticity of Research Objects as of Great Concern to Innovative LbD Projects. Case: SATERISK, The Learning by Developing - New Ways to Learn, Conference Proceedings, Laurea publications, D•7, Vantaa, 195-206.

Abstract: Innovations are vital for the Finnish economy and society. Over the past few years it has been discussed and written about how the foundation of Finland's future welfare and economic growth is based on an organization’s renewal and innovation capabilities. Laurea University of Applied Sciences operates in the Helsinki metropolitan area, one of the most competitive regions in the world. Laurea’s strategic choice is to implement, develop and use Learning by Developing (LbD) as an operational model in order to contribute to the growth of the surrounding region. Laurea’s aim is to be a fully authorized and international University of Applied Sciences participating in service innovation activities.

But how can a higher education institute, such as Laurea, best support innovation capabilities, and are there any theories behind an organization’s innovation capabilities? The SATERISK research project, born in Laurea, aims at a situation, where laws about positioning and tracking, and the *financial risks posed by their usage, will not prevent the use of machine-to-machine (m2m) tracking across state and union borders. The project is projected to bring new, international level know-how to the Finnish security field. The project will also create new methods and development paths for the Finnish positioning and tracking system development field. Positioning and tracking are used for increasing productivity and security. The widely used United States based Global Positioning System (GPS) satellite positioning system will soon get a European Union counterpart and rival from the Galileo satellites. While the satellites are still on the ground, it is important that any problems and possibilities that are related to the new system are being charted. The project also aims to offer technological solutions to issues that arise while the project is still on-going. The project also includes a separate law-related work package, which looks at the complicated legal issues that arise with the use of the Galileo system for tracking and positioning. These are studied on many levels: international, European and national.*

This article shows how the whole SATERISK research project shapes up within an LbD process: The research idea was born within a student group; it developed within dialogs with students and teachers; and during dialogs among value networks (e.g. students, teachers, researchers, companies, government officials) it evolved into one of the major research projects funded by the Finnish Funding Agency for Technology and Innovations (Tekes). The case study also researches how SATERISK's shaping process fulfills the models of innovation capabilities.

According to Auvinen et al. (2010, p. 146-148): "the actualizations of Student-Centred R&D were integrated into learning as a part of its LbD-dimensions, and it forms part of an organization's profile", furthered that, "the revised R&D-based model has shifted the focus of teaching to R&D; and the students' participation in R&D has been raised to a new level; so that they are now the main activating forces in the process; and the Student-Centred R&D was strongly supported by management; and it was purposefully developed throughout the organization" (Auvinen et al, 2010, p. 146–148). Rajamäki & Fred's (2011) focus is that in this view of a learning environment as a sustainable R&D-trigger and -driver, the role of personnel is centred on facilitation and as a guide to continuum and creation of R&D themes and applications.

In SATERISK, the role of the quality assurance system is placed as an enabler of activities: it involves gathering feedback of all results, organising, conducting and utilising feedback data for varying decisions (Lampelo et al., 2010; Pirinen, 2011). The student feedback system produces systematic and comparable data for the use in quality assurance, operational development, and strategic, operational and pedagogical planning. The feedback system includes themes for students to evaluate their progress into developers and to provide feedback on learning (INKA) as part of the R&D activities.

However, the Student-Centred R&D-learning model is challenging in many views, such as in SATERISK: the first challenge is in the student's commitment to the demanding study model (Auvinen et al., 2010; Vyakarnam et al., 2008); the second challenge is in the transformations of the management model and culture in higher education (Auvinen et al., 2010; Tarkkanen, 2009; Rauhala, 2008); the third challenge takes place in controlling the mass and cognitive load of projects precipitated in by the R&D-based learning model (Elen & Clark, 2006; Fränti & Pirinen, 2005); and the fourth identified challenge is related to the systematisation of stakeholder partnerships (Auvinen et al., 2010).

Auvinen et al. (2010) summarise that the pedagogical development and continuous change have created great challenges for teachers, but the samples of evidence in evaluation can already provide proof of the successful support provided by team coaching, job orientation and development resourcing; and despite the strong emphasis on R&D, theory and practice were well balanced in the education. Furthered, the Student-Centred R&D was particularly well suited to the UAS context; information on the students' development as developers and on their learning through R&D was also gathered through the student feedback system. The feedback has so far led to demonstrable development actions being taken (Auvinen et al., 2010; Tarkkanen, 2009).

The strengths of the Student-Centred model are as follows: the role of students as central actors and responsible participants; the sustainable integrative driver facilitates learning; an open interaction with an R&D operating environment and an agility in responding to the needs of the environment; teachers involved in the continuous interaction with the environment, which allows for quick reactions to actualisation of needs; and the focus itself, which was on the development of permanent collaboration structures and employment in the local region (Auvinen et al., 2010; Saarela et al., 2009; Salminen & Kajaste, 2005). Besides these viewpoints, the bottom-up approach of management is imperative so that the ecosystem of different stakeholders can come up with new ideas (Fränti & Pirinen, 2005; Rajamäki & Fred, 2011; Pirinen, 2011).

References

Auvinen, P., Kauppi, A., Kotila, H., Loikkanen, A., Markus, A., Peltokangas, N., Holm, K., & Kajaste, M. (2010). Ammattikorkeakoulujen koulutuksen laatuyksiköt 2010–2012. KKA 1:2010. Tampere: Publications of the Finnish Higher Education Evaluation Council (FINHEEC), (in Finnish).

Elen, J. & Clark, R. E. (2006). (Eds.). Handling Complexity in Learning Environments. Amsterdam: Elsevier.

ESA (2012). European Space Agency – Navigation – The Future – Galileo. http://www.esa.int/esaNA/galileo.html.

Etzkowitz, H. & Leydesdorff, L. (1998). The Endless Transition: A “Triple Helix” of University-Industry-Government Relations. Minerva, 36, 203–208.
Etzkowitz, H. & Leydesdorff, L. (1999). The Future Location of Research and Technology Transfer. Journal of Technology Transfer, 24, 111–123.

Fränti, M. & Pirinen, R. (2005). Tutkiva oppiminen integratiivisissa oppimisympäristössä. B10. Helsinki: Laurea Publications, (in Finnish).

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (2008). The new production of knowledge (12th print). Los Angeles: Sage Publications.

Gregor, S. & Jones, D. (2007). The Anatomy of a Design Theory. Journal of the Association for Information Systems (JAIS), 8(5), 312–335.

Lampelo, S., Kainulainen, S., Turunen, J., Viljanen, J., Yanar, A. Mattila, J., & Saarilammi, M-L. (2010). Laurea-ammattikorkeakoulun laadun-varmistusjärjestelmän auditointi. KKA 18:2010. Tampere: Publications of the Finnish Higher Education Evaluation Council, (in Finnish).

Luojus, S. (2010). From a Momentary Experience to a Lasting One: the Concept of and Research on Expanded User Experience of Mobile Devices. Doctoral dissertation. A559. Department of Information Processing Science, University of Oulu.

Nunamaker, J. F. (2010). Interview with Jay F. Nunamaker, Jr. On Toward a Broader Vision of IS Research. Business and Information Systems Engineering, 5, 321–323.

Ojala, J. (2011). Tekninen seuranta poliisin salaisena pakkokeinona. Master Thesis. Theseus. Espoo: Laurea, (in Finnish).

Pirinen, R. (2011). Externally Funded Research and Development Projects in Perspective of Learning. International Journal of Engineering Pedagogy (iJEP), 1(3), 27-36.

Pirinen, R. (2009). Actualization of Learning by Developing (LbD): an Analysis. International Journal of Emerging Technologies in Learning (iJET), 4(3), 46–58.

Pirinen, R. (2008). Integrative Learning Environments in perspective of Regional Development. Proceedings of Pascal International Conference, University of Limerick, 28–30 May.

Pirinen, R., Tarkkanen, J., & Teräs, J. (2009). Integrative Action Models in Regional Development, Applied Triple Helix. Proceedings of Triple Helix XII Conference, 17–19 June, Glasgow.

Rajamäki, J. (2009). Elasticity of Research Objects as of Great Concern to Innovative LbD Projects. Case: SATERISK, The Learning by Developing – New Ways to Learn, Conference Proceedings, Laurea publications, D•7, Vantaa, 195-206.

Rajamäki, J. (2011). Vulnerabilities in Satellite-Based Tracking Systems, Plenary Lecture, Proceedings of the 9th WSEAS International Conference on APPLIED ELECTROMAGNETICS, WIRELESS and OPTICAL COMMUNICATIONS, 24-26 March, Meloneras, Gran Canaria.

Rajamäki, J. & Fred, M. (2011). Externally Funded Research, Development and Innovation Projects as Learning Environment. Proceedings of International Technology, Education and Development Conference, 7–9 March, Valencia, 4130–4139.

Rauhala, P. (2008). R&D Activities in Finnish Universities of Applied Sciences Promoting Regional Development. In K. Laine, P. van der Sijde, M. Lähdeniemi, & J. Tarkkanen (Eds.). Higher Education Institutions and Innovation in the Knowledge Society. (pp. 95–101). Helsinki: Nord Print.

Saarela, M., Jaatinen, P., Juntunen, K., Kauppi, A., Otala, L., Taskila. V-M., Holm, K., & Kajaste, M. (2009). Ammattikorkeakoulujen laatuyksiköt 2008–2009. KKA 2: 2009. Publications of the Finnish Higher Education Evaluation Council (FINHEEC), (in Finnish).

Salminen, H. & Kajaste, M. (Eds.). (2005). Laatua, innovatiivisuutta ja proaktiivisuutta, Ammattikorkeakoulujen koulutuksen laatuyksiköt 2005–2006. KKA 3: 2005. Tampere: Publications of the Finnish Higher Education Evaluation Council (FINHEEC), (in Finnish).

Tarkkanen, J. (2009). Application for the Centre of Excellence in Education evaluation starting 2010. In R. Hemmilä (Ed.) Student-Centred R&D Work Integrated in Learning: Centre of Excellence in Education for 2010–2012. (pp. 5–24). Vantaa: Laurea University of Applied Sciences.

Viitanen, J. (2009). SATERISK-projektin suunnittelu ja vaatimus-määrittely. (Planning and Requirement Analysis of the SATERISK Project). Master thesis. Theseus. Espoo: Laurea, (in Finnish).

Vyakarnam, S., Illes, K., Kolmos, A., & Madritsch, T. (2008). Making a Difference: A Report on LbD, Innovation in Higher Education at Laurea University of Applied Sciences. B26. Vantaa: Laurea Publications.

3 Technical Risks

Robert Guinness, Heikki Pitsinki and Jyri Penttinen

3.1 Introduction

Robert Guinness

The systems required to provide satellite-based tracking services are highly complex, requiring firstly a highly sophisticated Global Navigation Satellite System (GNSS), such as the Global Positioning System (GPS). Secondly, a GNSS-enabled device is required. A diverse range of such devices are available on the commercial market, each offering its own capabilities and innovations, as well as limitations and failure modes. Thirdly, for applications where remote access to the positioning information is required, a communication system is needed, such as those provided by a mobile network operator, which are in themselves highly complex. Lastly, if data logging or unique data analysis and application-layer services are needed, then a server and IT infrastructure is required in order to receive, process, and store the information sent from the GNSS-enabled device via the communication system. If secure services are required—which can be considered the norm in this domain—then such IT systems themselves may be highly complex.

The result of these requirements is that the systems required that enable satellite-based tracking—which can be thought of as a system of systems (SoS)—presents the user or service operator with many technical risks, which can be difficult to predict and analyse. During the course of the SATERISK project, we came to realise that attempts to generically analyse all the risks involved in any and all satellite-based tracking applications are fraught with difficulty because each use-case scenario represents its own unique set of requirements and risks. What may be a critical risk for one application, may represent only a small risk or no risk at all for another application. For example, in money delivery applications, secure real-time data delivery is critically important, whereas for hobby applications, such as position-logging for recreational sports, real-time data delivery is not required, and data security may represent only a moderate or small risk. This reality led our research into the technical risks of satellite-based tracking to be highly use-case specific.

In addition, due to the highly complex nature of analysing risks of satellite-based tracking, it was necessary to break the technical risks into different categories, such as information security or intentional signal jamming, in order to conduct the analysis with a more constrained and methodical approach. This also allowed experts in specific technical domains—such as information security—to conduct their research in a relatively independent fashion. The results of this approach can be seen in the chapters to follow.

Lastly, in order to validate the results of our analysis, we found it necessary to conduct field testing of satellite-based tracking applications, again using a use-case specific approach. The results of this research can be seen in the study Kämppi, Guinness and Urpila (2010). It is perhaps not surprising that during the course of our field tests and data analysis, new technical risks and limitations were discovered. In addition, we found it beneficial to develop some new software tools to assist with our data collection and analysis. The approach and tools we developed should be beneficial for other researchers and perhaps service providers conducting related studies concerning the reliability, precision, and security of satellite-based tracking applications. Above all, the general public, which is becoming more and more reliant on satellite-based tracking, should take notice of the technical risks described in the sections below.

3.2 Information Security Risks

Heikki Pitsinki

Ekholm and Karhula (2012) express their concern of the increasing trend of collecting personal data in one of Finland’s major newspapers on January 26, 2012. They feel that we are threatened by a transition towards a ubiquitous society, which means that individuals can be located and identified, and accurate information of their actions, communication and location can be collected without them even knowing. This kind of development may influence the roots of society. The writers suspect that accepting commercial and technical solutions without criticism on their influence on fundamental rights and information security may be fatal.

Ubiquitous computing is not a new idea. The term was first used in 1991 by Mark Weiser (Park Communications 2008). The warnings have been around much earlier. In the conference publication of NordData 1975, a notion was made that we, if being uncritical, may drift into a situation of no choice and freedom. We may accept these perhaps Orwellian views - yes, there is an article by Sprague (2008) titled “Orwell was an optimist” - of societal level development, or decline them as overly paranoid. It is, however, a fact that satellites and wireless information collection form a fast-growing part in our everyday life. It is no surprise that many articles can be found pointing out that satellites are to be identified as a part of critical infrastructure.

Weidlich and Beenken (2012) point out that intensive cross-sectional cooperation is needed between the state and the corporate sector, while a good part of critical infrastructure is in private hands. Mutual effort is needed to ensure information security.

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 the main topic of this section.

The study Kämppi, Rajamäki, Guinness (2009a) opens this playground in the SATERISK project. It 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. The study Kämppi, Rajamäki, Guinness (2009b) describes 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.

Kämppi, P., Rajamäki & J. Guinness, R. (2009a). Information Security in Satellite Tracking Systems. In Proc. 3rd International Conference on Communications and Information Techonolgy. Athens, 153-157.

Abstract: Satellite-based tracking is one of the most rapidly growing service business areas in the world, and there are many commercial applications available already. Benefits of the service for the customer are advertised, but very seldom is there any mention of information security of the system. Modern satellite-based tracking systems contain communication and data processing on many levels, so they are vulnerable to many risks of information security. This paper covers the main satellite-based tracking system information security vulnerabilities and gives guidelines on how to make systems and services more secure.

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

Extended abstract: Many commercial satellite-based tracking systems are built on the top of commercial telecommunications networks. Telecommunications networks, like GSM and UMTS, have very limited features for end-to-end packet data protection. The data transfer path is secured in the air interface but only partially in the core network. On the Internet, the data path is fully unprotected. Additionally, a user does not know how a network operator has protected the network against security threats. The position data is processed and stored in a data center. The data center can be compared to a small corporate data center from the security point of view. If it is connected to the Internet, it is vulnerable to many threats; denial of service (DOS) attacks, viruses, worms, pharming, cross scripting, and social engineering.

In some commercial satellite-based tracking solutions, the data center is hosted by the service provider, so a user cannot be sure how the positioning data is hosted. There are many open questions, like: where is the data center located, what *kinds of protection mechanisms are used, what is the professional level of personnel, and is there is any co-operation with governments? Therefore, the user has to be aware of what service is chosen.*

Commercial satellite-based tracking service providers have made matters easy by reusing smartphones as tracking devices. The user only needs to download a tracking application to the smartphone to use it as a tracking device. Smartphones can be compared to computers, and they can have security vulnerabilities depending on the operating system used.

New operating systems for smartphones, like iOS by Apple and Android by Google, are fascinating, but they are vulnerable too. Many security threats for these operating systems have been reported. As the number of smartphones grows, they become more interesting targets for the hackers too. Dedicated devices for satellite-based tracking are available, but their security vulnerabilities have not been investigated here. End-users can access their positioning data via the Internet, and their computers are vulnerable to all typical threats. How well their equipment is protected and maintained is fully dependent on the user. This can be a security risk for satellite-based tracking systems if an attacker gains access to a hosting server by using stolen user accounts.

The system can be protected by using existing technology and using the known best practices. The data transfer path can be protected with secure tunneling, or by encrypting data messages with a security algorithm. The data processing center needs professional personnel and good security equipment. Personal computers and smart phones can be protected with security suites that are offered by many software houses.

As discussed in this paper, a satellite-based tracking system is quite a complicated system from the information security point of view. It contains parts of wireless and wired communication, and it is obvious that it contains information security risks if the system is not built properly. Securing the satellite-based tracking system, the data path is especially *important if the system is used to deliver sensitive positioning data*

One of the SATERISK project's focus areas is the reliability of tracking devices on motor vehicles. Interestingly, BBC news reported in February 2012 that the British Automobile Association AA is aiming to launch a new insurance policy which uses satellite navigation technology to track driver performance (Lee, 2012). According to the report, the system is monitoring speed, braking severity, cornering and the types of roads used. The approach is seen to become commonplace by the Association of British Insurers. The Association for British Drivers is slightly worried.

Jamming of navigation and tracking systems is a vulnerability directly connected with the topic above. The study by Happonen, Viitanen, Kokkonen, Ojala and Rajamäki (2009) offers some sights on signal interference and jamming detection. According to the study, jamming may be either intentional on non-intentional. The bad news is that equipment for short-range jammers can be easily acquired at a low price. The good news is that at least GSM jamming is quite easily detectable. The study gives some advice for preparing with countermeasures. Finally, the article warns us that positioning and tracking systems may create risks, and risk assessment is needed.

Happonen, M., Viitanen, J., Kokkonen, P., Ojala, J. & Rajamäki, J. (2009). Jamming Detection in the Future Navigation and Tracking Systems. In Proc. 16th Saint Petersburg International Conference of Integrated Navigation Systems. St. Petersburg, 314-317.

Abstract: Currently, satellite navigation and tracking have become an everyday routine, and they are still growing while the EU's new satellite system Galileo will be operative in 2013. Positioning, navigation and tracking are used to decrease risks, especially in logistics and to optimize work flow, but does it always work that way? Can international legislation about tracking, or lack of it, cause problems when tracking abroad? With technical aspects, are your tracking systems good enough to increase the security of your crown jewel, or are you just giving extra hints to thieves? For answering these questions, the SATERISK research project was started in 2008. It aims at a situation where laws on *positioning and tracking and the financial risks posed by their usage will not prevent the use of m2m tracking across state and union borders. An essential part of the project is to study signal interference in tracking and find ways to improve tracking devices and user habits in the future to avoid them. This paper focuses mainly on that topic.*

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 with an effort less than one hour. Systems may be a target of cyber terrorism, cybercrime or cyber vandalism. One act against such phenomenon is to add the awareness of technical risks perhaps even inherently included in information systems in general.

3.3 Recognising and Analysing Technical Risks

Jyri Penttinen

Satellite-based navigation and tracking have become a part of everyday life. Tracking devices have become inexpensive, the coverage of the mobile network has grown, and development in the personal gadgetry field has enabled the expansion of satellite-based tracking applications. Profits of the satellite-based tracking applications are frequently advertised, but unfortunately the risks and misuses are too often ignored. That was one of the main reasons why the SATERISK project was founded.

The lack of a satellite signal is still the most common risk in satellite-based navigation. While becoming more popular, manmade interference and misuse for criminal purposes have generalised. Unrecognised risks can be fatal for critical business applications – like cash in transit, fleet management and road tolls. For that reason, it is important to recognise risks related to satellite-based navigation and tracking systems. This section deals with the possible technical risks in the field of satellite-based tracking systems– how to recognise risks and countermeasures used to avoid them.

Markus Happonen’s master thesis “Recognizing risks of satellite-based tracking” (Happonen 2010) deals with some of the fundamentals in satellite-based navigation and tracking applications. The main goal for this study is to point out crucial risks in that topic. Happonen emphasises the importance of recognising whether the interference is unintentional or intentional. Finding and locating interference devices today is still close to impossible. In consequence of that issue, Happonen describes ways to improve tracking devices and user habits to avoid intentional interference by developing countermeasures for tracking applications.

Happonen, M. (2010). Recognising Risks Of Satellite-based Tracking. Master thesis. Theseus. Espoo: Laurea.

Abstract: Within the last two decades, popularity of the satellite-based navigation has boomed from military application to common aid in driving and safety equipment for children. People have become even too dependent on technical aid while the risk of their usage is too often forgotten. This is an especially serious risk in companies and the public sector, where positioning and tracking is used to improve security and productivity. To avoid these problems, the SATERISK project was founded.

The requirements analysis was the first phase of the SATERISK project and this master thesis is the natural continuum for it. This thesis focuses to present those publications made for the SATERISK project, where thesis writers have had taken part in the project. Personal approach for the task is mainly technical due to writer's background and therefore, for example, the juridical part is really limited.

The first publication in the master thesis is about signal interference and countermeasures for them. Not all interference is intentional, but, for example, terrain and road tunnels may cause signal loss. Therefore, recovery and countermeasures for these situations should be considered beforehand. It is absolutely important to know if the interference is manmade or unintentional, especially in transportation of valuable goods.

The second and third publications were about time-critical data communication between multinational organizations. This problem is common in law enforcement environment. Criminals are working more often abroad due to the European *integration, but law enforcement authorities do not have common protocols and procedures on how to pass information between each other. Especially machine-to-machine (M2M) communication is not researched yet.*

The study by Kämppi and Guinness (2010) describes functionality and structure of satellite-based tracking - knowing how satellite-based tracking operates is important before considering all possible risk scenarios. Modern satellite-based tracking system is a multi-dimensional system, including a diverse set of technical segments. Kämppi and Guinness describe vulnerabilities in different parts of the satellite-based tracking system. Their paper proposes a developed risk analysis tool to categorise possible threats by severity and probability. The risk analysis tool helps to understand dependencies and interdependencies between technical segments, the requirements of the application and business as an integrated part of the risk analysis process. Kämppi and Guinness demonstrate the tool throughout different risk analysis cases. It was found that risk scenarios are very dependent on use cases.

Kämppi, P. & Guinness, R. (2010). Technical Risk Analysis for Satellite Based Tracking Systems. Integrated Communications, Navigation and Surveillance conference 2010. Herndon, pp. M3-1 – M3-16.

Abstract: Satellite-based tracking is one of the most rapidly growing business areas in the world, and there are already many commercial applications available like fleet management or equipment theft alert. Service providers advertise benefits for the customer, but they rarely mention the technical risks inherent in a tracking system. Modern satellite-based tracking systems require communication and functionality on many levels, so they are vulnerable to many technical risks. This paper describes the system overview of satellite-based tracking; several risk analysis methods cover the main technical risks of a satellite based tracking system, and demonstrates usage of the developed risk analysis tool.

The study by Kämppi, Guinness and Urpila (2010) focuses on performance of the satellite-based tracking system – how the system performs in real life and presents measured metrics for reliability and accuracy. The performance is tested by constructing a field test environment and using several usage cases in Finland. Results of the technical risk described in the second paper also give precept to field testing. Kämppi and colleagues point out that more testing is still needed – especially in an international environment with lower mobile network coverage.

Kämppi, P., Guinness, R. & Urpila, T. (2010). Field Testing for Satellite-Based Tracking Systems. 61st International Astronautical Congress 2010. Prague, Czech Republic.

Abstract: Satellite-based tracking is a rapidly growing business area in many parts of the world. Tracking devices have become inexpensive, mobile network coverage has grown, and the internet has become part of our everyday life. This evolution has enabled the proliferation of satellite-based tracking applications. The basic principle behind satellite-based tracking is that a tracked device is positioned by GNSS satellites, and the positioning data is delivered for post-processing via mobile networks and the internet. This system is complex, and field testing provides an effective way to test system reliability and performance with real applications. In this research, analysis was performed on the reliability and accuracy of satellite-based tracking using commercially available systems during various routes in several regions in Finland. A smart phone was transformed into a tracking device by installing a tracking application. Data created in the mobile device was sent over mobile networks to the third-party GPS tracking service. Later, data from both the GPS tracking server and the mobile phone were downloaded and analyzed. Use cases included different activities like car driving, sailing and bicycling. We found that the system performs very well and basic functionality is very stable. Practical testing, however, did reveal that the smart phone is not able to perform as well as a dedicated GPS receiver. Also, we discovered that the position of the GPS module in the mobile device greatly affects the sensitivity, and in certain models, this sensitivity changes based on whether the keyboard is exposed because the GPS module is directly beneath the keyboard. Lastly, we found a few security vulnerabilities that have not been found in theoretical risk analysis. This study describes the main structure of the satellite-based tracking system, presents known technical

risks, describes the test setup we used, and gives results on the performance of the satellite-based tracking system.

Pasi Kämppi's master thesis "Grounded View to Technical Risks of Satellite-Based Tracking Systems: A Multimethodology Research" concentrates on the most critical technical risks for satellite-based tracking systems as well. The article also contains a general technical description of the satellite-based tracking system. Kämppi also expresses his concern about the introduction of the new navigation systems Galileo and COMPASS. The new systems operate on the same frequency as the existing navigation systems GPS and GLONASS. That might cause interference if the systems are not designed properly.

Kämppi. P. (2011). Grounded View to Technical Risks of Satellite-Based Tracking Systems: A Multimethodology Research. Master thesis. Theseus. Espoo: Laurea.[2]

Abstract: Satellite-based tracking is a rapidly growing business area in many parts of the world. Tracking devices have become inexpensive, mobile network coverage has grown, and the internet has become a part of our everyday life. This evolution has enabled the proliferation of satellite-based tracking applications.

Satellite-based tracking is used with many business-critical applications like fleet management or the tracking of cash in transit. Very often only the benefits of the satellite- tracking solutions are advertised while the risks and weak points are forgotten. A proposal was made for the SATERSIK project to investigate legal, usability and technical risks in satellite-based tracking. The project got funding from the Finnish Funding Agency for Technology and Innovation (TEKES) and began in 2008. The SATERISK project is headed by Laurea University of Applied Sciences and it is made in cooperation with the University of Lapland and partners in the private sector.

[2] This master thesis won the best thesis of the year 2011 award in Finland. In 2011, about 20.000 students graduated from universities of applied sciences and 20 awards were honored.

The primary objective of this research was to find the most significant technical risks for satellite-based tracking systems and the emphasis was on ICT. The secondary objective was to generate internationally recognized R&D research work and publications. This report does not examine legal or usability issues for satellite-based tracking systems.

This research work followed the multimethodological approach for IS research. In the multimethodological approach theory building, observation, experimentation and systems developing phases are integrated during the research process. The research work was evaluated according to seven guidelines for IS design research. The framework also encourages the researcher to use several research and evaluation methodologies. During the research process several research and evaluation methodologies were used such as qualitative risk analysis, grounded theory, simulation and field testing.

This research report contains four international publications that were published during the years 2009 and 2010. The first and second publications cover information security related issues for satellite-based tracking systems. The system is complex and it is vulnerable to many threats. The third publication presented a technical risk analysis procedure, with a list of possible technical risks and the results of three simulated risk analysis cases. It was found that the risk profiles are very dependent on use cases. The last publication investigates how the satellite-based tracking system performs in real life and presents measured metrics for reliability and accuracy.

This report concludes the research work and presents a description of the satellite-based tracking system, describes research methodologies and summarizes all publications.

The satellite-based navigation system is very complex and there are many vulnerabilities and threats in different technical levels of the system. The studies made in the SATERISK project and described in this section enhance the understanding of the possible risks and gives valuable tools to avoid possible threats. It is likely that there would emerge new risks in the future in the field of satellite-based tracking. It is important to continue international cooperation and investigations to recognise the most severe and topical risks.

References

Driessen, B. (2012). Eavesdropping on Satellite Telecommunication Systems. Cryptology ePrint Archive: Report. Draft February 8. Available on: http://eprint.iacr.org/2012/051.pdf

Ekhgolm, K. & Karhula, P. (2012). Ihmisten valvonta lisääntyy salakavalasti. Vieraskynä. Helsingin Sanomat 26.1.2012 (in Finnish).

Happonen, M. (2010). Recognising Risks Of Satellite-based Tracking. Master thesis. Theseus. Espoo: Laurea.

Happonen, M., Viitanen, J., Kokkonen, P., Ojala, J. & Rajamäki, J. (2009). Jamming Detection in the Future Navigation and Tracking Systems. In Proc. 16th Saint Petersburg International Conference of Integrated Navigation Systems. St. Petersburg, 314-317.

Kämppi. P. (2011). Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multimethodology Research. Master thesis. Theseus. Espoo: Laurea.

Kämppi, P. & Guinness, R. (2010). Technical Risk Analysis for Satellite Based Tracking Systems. Integrated Communications, Navigation and Surveillance conference 2010. Herndon, pp. M3-1 – M3-16.

Kämppi, P., Guinness, R. & Urpila, T. (2010). Field Testing for Satellite Based Tracking Systems. 61st International Astronautical Congress 2010. Prague, Czech Republic.

Kämppi, P., Rajamäki & J. Guinness, R. (2009a). Information Security in Satellite Tracking Systems. In Proc. 3rd International Conference on Communications and Information Techonolgy. Athens, 153-157.

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

Lee, D. (2012). AA to launch sat-nav tech tracked insurance policy. BBC News. Available at: http://www.bbc.com/news/technology-16969509

Park Communications (2008). In memory of Dr. Mark Weiser. Available at: http://www2.parc.com/csl/members/weiser/

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. Available at:
http://works.bepress.com/robert_sprague/1

Weidlich, A., Beenken, P. (2012).MSC Booklet Paper: Cypersecurity. Munich Security Conference. Available at:
http://www.securityconference.de/Program.425+M503439d852f.0.html

4 Operational Risks

Jyri Rajamäki

The SATERISK project has widely studied operational risks 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. This section presents the SATERISK project's main results in this field. The section is divided into two parts. The first part elaborates the risks that law enforcement authorities face when they exploit tracking. The second part introduces some aspects of GNSS usage in the private sector.

4.1 Law Enforcement Authorities - Transparency and the Information Flow

Organised crime is a real threat in Europe 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. 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 are connected to different monitoring systems. This makes the LEA work very labour-intensive, so the use of new state-of-the-art technologies should enable the optimisation of the use of human resources.

In the Public Safety Communications Europe Conference, Rajamäki and Holmström (2012) present the results of the SATERISK project with regard to trans-European LEA operations.

Rajamäki, J. & Holmström, J. (2012). Tracking cross-border criminals with satellites – SATERISK project. PSCE Conference, May 30-31, Helsinki, Finland.

Organised 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. slow and / or hindered information exchange, endangering the success of entire investigations. The SATERISK project (2008-2011) has focused on risks and challenges of satellite-based tracking in cross-border operations.

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.

The two studies of Viitanen, Happonen, Patama and Rajamäki (2009, 2010) focus on cross-border surveillance operations. They deal with time-critical data communication between multinational organisations. 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 yet researched.

Viitanen J., Happonen M., Patama, P. & Rajamäki J. (2009). International and Transorganizational Information Flow of Tracking Data. 8th WSEAS International Conference on Security and Privacy. Tenerife, Canary Islands, Spain.

Abstract: European integration has increased the transport of illegal goods and other criminal activity. Therefore, the transmitting of tracking and other status information between nations and different organizations should become an everyday business. The goal of this paper is to find possible bottle necks in international cooperation between authorities and to find possible solutions for them. The following area can be considered as a part of the Finnish SATERISK research project that aims for a situation where laws on positioning and tracking and the financial risks posed by their usage will not prevent the use of m2m tracking across state and union borders. The target of the paper is to present administrative and technical solutions to improve multiorganizational tracking solutions. Namely, the goal is to make it possible to create a timely situational picture in joint multinational and interagency operations. This paper will provide guidance for preparing appropriate plans and doctrine proposals for joint operations and training. Also, technical solutions and bottlenecks are briefly covered in this paper.

Viitanen, J., Happonen, M. Patama, P. & Rajamäki, J. (2010). Near Border Procedures for Tracking Information. WSEAS TRANSACTIONS on SYSTEMS. Issue 3. Volume 9. pp. 223 – 232.

Extended abstract: In the past decade, tracking has become an essential and valuable tool for authorities to prevent and investigate crimes. At the same time, criminal nature and *organized crime have internationalized, mostly due to European integration. Within the last decade, criminals have also become more technically oriented. Some countermeasures for tracking applications have been found from the hands of criminals and therefore international cooperation between officials becomes even more vital.*

The change has been rapid and therefore law enforcement authorities (LEAs) have failed to create protocols and procedures to deal with international tracking issues. This paper addresses the problems of LEA with regard to cross-border operations and explains how they differ from other operations. It focuses on the operational level of action and addresses issues across the range of LEA operations.

Its goal is to reveal the need for technical help and doctrinal guidance focused on tasks on or across borders. It examines the special considerations required when conducting operations in or over the complex modern border environment. Many of these problems are also present in non-national or state borders, but also in other governmental borders.

It is always more efficient to prevent than to repair damages. Unfortunately, preventing is even more difficult than crisis management, due to information and time criticality. Currently, the Geographical Information System (GIS) is mostly used for analyzing situations after they have happened or trying to make logistics more efficient, but not for preventing unwanted events from happening.

The military has become accustomed to utilizing GIS. Also, some LEAs are good at this, but the trouble remains on the borders, be it a nation-state or juridical border. The European Council held a special meeting on October 15th - 16th 1999 in Tampere on the creation of an area of freedom, security and justice in the European Union. The meeting called for joint investigation teams to be set up without delay, with a view to combat the trafficking in drugs and human beings, as well as terrorism. In 2005 and 2006, there were only two joint investigation groups. These were post-event investigation teams, trying to find out what happened, although in the long run that will also help with prevention.

Furthermore, LEA officers need to have 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, legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way raises two problems: (a) how to ensure the accountability of law enforcement officers making use of such intrusive techniques and (b) 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. The studies Viitanen, Patama, Knuuttila, Rajamäki and Ruoslahti (2010), Viitanen, Patama, Rajamäki, Knuuttila, Ruoslahti, Tuohimaa and Tikanmäki (2011), Tuohimaa, Tikanmäki, Rajamäki, Viitanen, Patama, Knuuttila and Ruoslahti, (2011) and Ovaska, Tervahartiala, Tervola, Johansson and Rajamäki (2012) deal with these research questions.

Viitanen, J., Patama, P., Knuuttila, J., Rajamäki, J. & Ruoslahti, H. (2010). Towards transparent authority of power in law enforcement. The 12th Annual Conference of the Finland Futures Research Centre and the Finland Futures Academy: Security in Futures – Security in Change, 3-4 June, Turku, Finland.

Abstract: While law enforcement is applying for more jurisdiction-based rights to reach new frontiers in the privacy intrusive field, public concern is rising to open discussion. Does law enforcement really need broader ways to use surveillance, and are they enforcing already given rights in ways which is described in legislation? This concern is often brought in discussion against rising power of surveillance state. "Mike" McConnell, former director of the United States National Intelligence, has said: "we all want security, but will not give up our privacy" and "so we have to rethink intelligence, reshape it, and we are not there yet". McConnell also said that "Any bureaucracy can do evil" and "there must be oversight". The 2006 European Union anti-terrorism directive required telecommunications companies to retain phone data and Internet logs for a minimum of six months in case they are needed for criminal investigations. However the Federal Constitutional Court of Germany ruled that the law violated Germans' constitutional right to private correspondence and failed to balance privacy rights against the need to provide security. There is no question that there *are problems between security, privacy, and trust. In this paper we propose solutions to some of them.*

Thinking about trust building between citizens and LEA, there are even more difficult things than phone data. This is because in phone data, there is always a log file in the system and there will be a trace. If LEA is using their own room audio or technical tracking systems, there will be no log marks outside LEA's own systems. And LEA is still widely using some stand-alone systems, where no log marks are created. Is the LEA considering the ways and technology of how to retrieve or get information too much, and too little on how to get the citizens to approve it? Finnish futurologist Mika Mannermaa has written a book (2008) named 'Every Brother'. 'Every Brother' society is presented as a 'soft surveillance, knowledge and non-forgetting' one. According to Mr. Mannermaa, the important difference between 'every brother' and Orwell's 'big brother' is that surveillance is commonly agreed and transparent. Mannermaa outlines an important point in his book: "when information society's first stage deepens to 'ubiquitous network society', single sided enforcement and surveillance is straining people".

These nonlinear, nontransparent systems are a handicap even for the LEA. LEA is doing everything by the law, but they cannot prove it because the end use and methods cannot be audited by an outsider. LEA can only claim that they are doing the right thing. In this paper, we are showing how it is, if it is possible to create multi directional surveillance and develop transparent authority power.

As a part of this surveillance authorizing process, we could also see methods of open acceptance process in technologies, which are used to conduct these intrusive operations. By opening this process of technology development to a publicly accepted review process, we could reach a level of assurance in a wider scope. In surveillance, security is important and security through obscurity is not enough.

Viitannen, J., Patama, P., Rajamäki, J., Knuuttila,J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. (2011). How to Create Oversight in Intelligence Surveillance. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications, March 24-26, Meloneras, Gran Canaria, 52-56.

Abstract: To prevent and investigate crimes, Law Enforcement Agencies (LEAs) are conducting various operations, which are affecting the privacy of citizens. These activities include video surveillance, audio surveillance and technical tracking. Currently, LEAs have the power to conduct these operations based on legislation. While law enforcement is applying for more rights based on jurisdiction, public concerns are rising up and open discussions growing. Does a LEA really need broader ways to use surveillance, and are they enforcing the rights they already have in ways which are described in legislation? These concerns are often brought in discussion against rising power of the surveillance state. Is it possible to find a balance between a LEA's operational security needs and individuals' freedom? This paper outlines a scenario on how common ground can be found with a constructive approach facilitated by advanced technology. The first part of this study shows the need for transparency, because without it, there may not be new legislation that LEAs could get. We have evidence that Citizens are willing to give more power to authorities if usage of these intrusive means is more transparent and better monitored by the public. The second part of the study shows examples of today's technological possibilities to create transparent and plausible monitoring for surveillance activities. How would it be possible to credibly show people that powers are used according to the law? In this part, we describe a system evolving ubiquitous but transparent surveillance, and what kind of difficulties there might be.

***Tuohimaa, T., Tikanmaki, 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*, Issue 5, Volume 5, 602-609.**

Abstract: People are increasingly worried about the developments in information technology, especially when it concerns their privacy. Nowadays, it can be proved that personal information is very difficult to protect - especially on the Internet. Scientific studies show that the key risk of security is people. There are people who develop computer systems, and those who use information technology. Privacy and security protection can be seen as a basic human right. Confidence in the Law Enforcement Agencies (LEAs) has always been high in Finland. Despite this, there are people in society who do not trust LEAs at all - especially when it comes to different kinds of surveillance by the police.

Development and the speed of different kind of information are really fast, and one of the main problems is the law retardation. How many people are even thinking about what kind of a walking data bank they are with, for example mobile phones, bonus- and credit-cards? In fact, in this society, there is always someone who knows who you are, how you live, who your friends are, where you are, what you do, what you buy, what your hobbies are and what kind of lifestyle you have. But the main concern in this matter is not how anyone other than the authority gets such information - but what LEA is doing with the information they get.

However, people are willing to give more rights to authorities if usage of these intrusive means is more transparent and better informed to the public. Today there are technological possibilities to create more transparent and credible monitoring for surveillance activities and in this paper is given an example of that.

Ovaska, L., Tervahartiala, J., Tervola, S., Johansson S. & Rajamäki, J. (2012). How Transparency Improves the Control of Law Enforcement Authorities' activities? European Intelligence and Security Informatics Conference 2012. August 22-24, Odense, submitted for publication.

Abstract: Many countries want to improve law enforcement. 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 than before to low enforcement authorities (LEAs) if 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 part of the developing of the surveillance authoring process is developing of open acceptance process for the technology. Both security and transparency are important in surveillance operations and they must be at a sufficient level.

4.2 GNSS Usage in Private Sector

As a part of the SATERISK project, many of Laurea's undergraduate students have studied the usage of global navigation satellite systems in the private sector. The following pages contain the abstracts of selected bachelor theses.

Vaarakallio, J. (2010). Galileo-satelliittipaikannusjärjestelmä ja sen mahdollisuudet yrityksen näkökulmasta. (Galileo Global Navigation Satellite System and its Potential from a Company's Point Of View) Thesis. Theseus. Espoo: Laurea (in Finnish).

Abstract: The European Commission and European Space Agency are carrying out the Galileo project in order to create a new European global navigation satellite system. The Galileo positioning system is intended to be more precise and provide more comprehensive services than the earlier *systems. It will be an alternative and a supplement to the already existing GPS and GLONASS positioning systems. The basic signal service will be open to everyone while the higher accuracy services will be restricted to commercial and military use.*

Galileo has been under development since the 1990s and there have been numerous stages in its planning and execution. Difficulties with the financing and decision making have complicated the project and postponed the implementation of the system by several years. Galileo is expected to be operational in the year 2014.

The purpose of this thesis was to define what Galileo is and how a company or an organization that utilizes satellite navigation would make use of its potential. Six interviews were conducted with the representatives of companies that use satellite navigation in their business models. The interviews were used to gain insight into the effects of Galileo on the revenue, employment and operations in the aforementioned companies.

The conclusion of this thesis was that the companies are still waiting to gain more detailed technical knowledge of Galileo's usability. In the event that Galileo will perform up to expectations such as the improved accuracy, the companies expect it to allow new working methods and product development. After the interviews, in the beginning of May 2010, updated technical information of Galileo's frequencies was published. The companies can be expected to use this information in their operations. However, it is likely to take years for new services based solely on Galileo to be on the market.

Pelkonen, T. (2012). Paikannuspohjaisten pelien tietoturva pelaajan kannalta - case Geokätköily ja Foursquare (Data security of positioning-based games from the player's point of view - cases Geocaching and Foursquare). Thesis. Espoo: Laurea (in Finnish), submitted for evaluation.

The author of this thesis became interested in data security issues of position-based games during her internship within the

SATERISK project. The target of this thesis it to find out what are the challenges of entertainment use of positioning. One of the main points of this work is to search for new viewpoints for uses of positioning. For that reason, this work is looking at data security and positioning problems from the user's point of view.

The study was executed as a case-study-based research. The study was realised utilizing various written sources from literature to electronic publications. Also, different kinds of player forums and social media platforms were used as well as methods like observation, testing and trying (especially in the field of Geocaching).

This thesis studies two different games that utilise positioning: Geocaching and Foursquare. Both games were new to their eras, introducing new ways of position gaming. These games are very different from each other even though they use same technology and devices. The problems had a lot of common aspects which made the researching and comparing even more interesting.

Geocaching is a modern treasure hunting game which was produced as co-production, so it doesn't have a single designer. Players create new things inside the game and the borders created inside the game. Positioning is a concrete part of the game, so players face coordinate and positioning problems continuously. On the other hand, Foursquare is a new field in the social media. It is a game where players compete for the virtual ownership of real places. Even though Foursquare is an independent game, it is used with other popular social media applications like Twitter and Facebook. It makes the application look less like game, but on the other hand, it offers all kinds of new opportunities inside the game.

While the study progressed, new data security problems and challenges were found, for example usage of passwords, credit card information, privacy problems and identity thefts. Many of these risks are completely up to players themselves; do they want to go through a little trouble to secure their own personal information. On the other hand, it is not known what data security level the service provider has. What if someone breaks into the server – what happens to the credit card information and identities? For example in Geocaching, all information of *every active user is stored by one American company with less than 10 workers.*

Position-based games broke the fundamental idea of gaming. They demand that the players move physically, offering new types of community and new ways to affect the game for the players and completely new ways to advertise to the companies. The future of this type of gaming seems bright and we will see many more positioning games in the future.

Kääpä, J. (2010.) Paikannuslaitteen käyttö autonlämmittimen etähallintaan, Case uTrace Evaluation Kit (Using a Positioning Device to Remote Control a Car Heater, Case uTrace Evaluation Kit). Thesis. Theseus. Espoo: Laurea (in Finnish).

Abstract: The purpose of this thesis is to examine whether the uTrace Evaluation Kit positioning device is suitable for remote controlling a car heater. The objective is that there is no need for a standalone controlling device, if the same features can be accomplished with the uTrace.

Remote controlling is done with text messages, and the uTrace positioning device utilizes its GSM modem in sending and receiving them. This method is compared to short-range radio frequency remote controlling technologies. A prototype that is able to control a power state of another device was implemented in the thesis.

The method of the thesis is constructive research. This research uses existing knowledge of the uTrace Evaluation Kit to expand its intended use. The main characteristics of the device are introduced only briefly, this thesis solely examines the functionality of the uTrace Evaluation Kit device's GSM modem and the device's connectivity to other equipment. Finding the right commands to remote control the uTrace Evaluation Kit was also the objective of this thesis.

The research resulted in the outcome that the uTrace Evaluation Kit positioning device is suitable for remote controlling a car heater. However, it also produced a list of *subjects that need further examination. These subjects are introduced in the end of this thesis.*

Aho, A. (2009). Google Mapsin käyttö karttapalvelun toteutuksessa (Usage of Google Maps to develope a map application). Thesis. Theseus. Espoo: Laurea (in Finnish).

Abstract: The goal of this Bachelor's thesis is to evaluate the usage of Google Maps in developing a map application by determining the features of Google Maps and by comparing Google Maps to other corresponding map applications on the Internet. The usage of Google Maps is also evaluated by determining the features of Google Maps API and the experiences of software developers.

Google Inc. is an American company, which is focused on miscellaneous services on the Internet. Google's search service is at the moment one of the most popular and famous search services. In 2005 Google published Google Maps, which is a free interactive map service on the Internet. With Google Maps you can e.g. view street maps, driving directions and local business information, including business locations and contact information. Map24 and Yahoo! Maps are corresponding map services, that have been used in comparison with Google Map in this study.

In summer 2005 Google published Google Maps API, with the help of which software developers can embed a map service, which is based on Google Maps, on their own web page. Google Maps API is an interface, which consists of JavaScript classes that are used from JavaScript code executed in web browser. With API software developers can modify the map service to better suit their needs, e.g. they can add their own controls, targets and routes on the map.

The theoretical part of this thesis describes the evaluation and the general features of the map services on the Internet. Also the features of Google Maps and Google Maps API with concrete coding examples are described.

The aim of the comparison with Map24 and Yahoo! Maps was to find out the strengths and weaknesses of Google Maps.

Furthermore the usability of Google Maps was analyzed by heuristic evaluation. User experiences were acquired by a semi-structured interview with two software developers, who had implemented a map service by using Google Maps API.

The comparison of Google Maps with Map24 and Yahoo! Maps pointed out, that Google Maps is better in many cases. For example Google Maps had the best search results, its maps were one of the clearest and the updating of the maps during zooming and panning was the fastest. The heuristic evaluation didn't find any serious usability problems. The users' opinion was that Google Maps is easy to use and their experiences with Google Maps and Google Maps API were positive.

Google Maps is a cheap and easy way to implement a map service. Google Maps API is a safe choice for implementing a map service, because it has many users and through an active user forum a support in problem situation is obvious. Google Maps and Google Maps API are under continuous development and new features are added constantly. The frequent new revisions ensure that the known problems will be fixed.

References

Aho, A. (2009). Google Mapsin käyttö karttapalvelun toteutuksessa. Thesis. Theseus. Espoo: Laurea (in Finnish).

Kääpä, J. (2010.) Paikannuslaitteen käyttö autonlämmittimen etähallintaan, Case uTrace Evaluation Kit. Thesis. Theseus. Espoo: Laurea (in Finnish).

Mannermaa, M. (2008) Jokuveli – Elämä ja vaikuttaminen ubiikkiyhteiskunnassa (Some brother society). Helsinki: WSOYpro (in Finnish).

Ovaska, L., Tervahartiala, J., Tervola, S., Johansson S. & Rajamäki, J. (2012). How Transparency Improves the Control of Law Enforcement Authorities' activities? European Intelligence and Security Informatics Conference 2012. August 22-24, Odense, submitted for publication.

Pelkonen, T. (2012). Paikannuspohjaisten pelien tietoturva pelaajan kannalta – case Geokätköily ja Foursquare. Thesis. Espoo: Laurea (in Finnish), submitted for evaluation.

Rajamäki, J. & Holmström, J. (2012). Tracking cross-border criminals with satellites – SATERISK project. PSCE Conference, May 30-31, Helsinki, Finland.

Tuohimaa, T., Tikanmaki, 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, Issue 5, Volume 5, 602-609.

Vaarakallio, J. (2010). Galileo-satelliittipaikannusjärjestelmä ja sen mahdollisuudet yrityksen näkökulmasta. Thesis. Theseus. Espoo: Laurea (in Finnish).

Viitanen J., Happonen M., Patama, P. & Rajamäki J. (2009). International and Transorganizational Information Flow of Tracking Data. 8th WSEAS International Conference on Security and Privacy. Tenerife, Canary Islands, Spain.

Viitanen, J., Happonen, M. Patama, P. & Rajamäki, J. (2010). Near Border Procedures for Tracking Information. WSEAS TRANSACTIONS on SYSTEMS. Issue 3. Volume 9. pp. 223 – 232.

Viitanen, J., Patama, P., Knuuttila, J., Rajamäki, J. & Ruoslahti, H. (2010). Towards transparent authority of power in law enforcement. The 12th Annual Conference of the Finland Futures Research Centre and the Finland Futures Academy: Security in Futures – Security in Change, 3-4 June, Turku, Finland.

Viitannen, J., Patama, P., Rajamäki, J., Knuuttila,J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. (2011). How to Create Oversight in Intelligence Surveillance. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications, March 24-26, Meloneras, Gran Canaria, 52-56.

5 Risks Occurring from Legislation

Seija Tiainen

Risks from legislation, or lack of legislation in some cases, have been interesting issues in the SATERISK project. The University of Lapland, in their joint SATERISK research project, concentrated in regulation and legal problem areas, such as privacy protection, information security, state sovereignty & safety, and responsibility & liability issues. The studies have also had a geographical focus: national, EU & Schengen Region, and Russia. The University of Lapland has published its own SATERISK book (Viikari, 2011) including articles and publications produced in the project. Legal issues could not be excluded from Laurea's part of the SATERISK project either: they gave guidelines for the activities of all users of satellite-based tracking, from authorities to private navigators. When analysing risks in satellite-based tracking, we must always know and take into consideration the existing legislation (if it only exists). This section includes two abstracts of master theses be completed within the SATERISK project. Jussi Ojala is another of the two original inventors and architects of the research idea behind the SATERISK project.

Ojala, J. (2010.) Tekninen seuranta poliisin salaisena pakkokeinona (Technical Tracking as Covert Coercive Measure for Police to Collect Information). Master thesis. Theseus. Espoo: Laurea (in Finnish).

Abstract: In the Coercive Measures Act (PKL, 450/1987), the methods and measures that pre-trial investigation authorities can use and which entitles them to interfere in human rights protected by law are defined. According to the Coercive Measures Act (PKL 5a:1 § 3.3) technical tracking means tracking a vehicle or goods with an attached radio transmitter *or other such device or mechanism. According to the Police Act (PoL 28 § 1.3) technical tracking means tracking the movements of a vehicle or goods.*

The aim of this thesis has been to clarify the legislation in force regarding technical tracking as a part of technical surveillance. The examination indicates that 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 the Coercive Measures Act and are used in a pre-trial investigation, and those measures which are prescribed in the Police Act and are used for information gathering purposes in a phase of crime prevention.

In this thesis it has also been clarified what the officers in charge of the investigation should take into consideration when they are dealing with technical tracking as a covert measure. 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.

In the thesis also a functioning of legality control concerning covert coercive measures and especially technical tracking has been under evaluation. According to that evaluation the quality of legality control 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 quite small-scale.

One of the most significant sources has been the committee report by the Ministry of justice 2009:2. The purpose of the report has been to act as a basis for the new Pre-trial Investigation Act, Coercive Measures Act and Police Act. The report has been critically assessed in this thesis and it has been concluded that if the proposed changes get into the legislation as such, it 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. The reform of legislation would also reflect especially on the execution of technical tracking *of vehicles and to use of the extraneous information obtained by covert coercive measures for an offence other than that for which the investigation is carried out.*

There is only a little evaluation of the methods of application of legal rules in this item because there are no comments available from the Parliamentary Ombudsman or Deputy Ombudsman and neither are there legally valid decisions of the Supreme Court or Court of Appeal regarding technical tracking. Comparing to, for example, wiretapping, there is only a little information from scientific research regarding the use of technical tracking. There is definitely need for a survey of these items.

Kokkonen, P. (2010). Paikannus merellä lain ja tekniikan näkökulmista (Tracking at Sea from the Law and Technology Perspectives). Master thesis. Theseus. Espoo: Laurea (in Finnish).

Abstract: Positioning-based services have increased dramatically in recent years. These services offer a wide range of new opportunities, such as employees or property, locating, positioning-based marketing and consumer services, such as different navigation, guidance and map services. The spatial effective and legitimate utilization of course requires knowledge of legislation in this field. In this study, the aim is to give a picture of related tracking and typical legal problems through a case study. Place "Information" means information that indicates a connection or terminal geographic location. The case may be, for example, a mobile phone or leased property on your geographical location or the location of base station positioning satellite positioning system (GPS) means. The mere transmission of messages used in the base station location information is not knowledge but also the identification data. At the European Union level, the basis for spatial processing for the legal regulation was formed in 2002 on the Electronic Communications Privacy Directive (2002/58/ETY). The Directive was implemented in Finland less than two years later, the Electronic Communications Privacy Act (516/2004, SVTSL). Geographic information is governed by Chapter 6. Provisions are intended to enable the processing of location data locating the target *without compromising privacy. Also the maritime law and the laws on personal data must take into account the context of tracking when national boundaries are exceeded. The study is part of the SATERSIK project. The study complements SATERSIK'S project by bringing in legal point of tracker view of research and technical point of view of empirical data in the marine environment and the positioning of overrunning. The results can be summarized in such a way that I found on the boundary conditions for localization, the law, the technical environment and geography perspectives.*

References

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

Ojala, J. (2010.) Tekninen seuranta poliisin salaisena pakkokeinona. Master thesis. Theseus. Espoo: Laurea (in Finnish).

Viikari, L. (ed.) (2011). SATERISK: Tutkimusraportti 2008-2011. University of Lappland. Lapin yliopistopaino (in Finnish).

6 New Services and Risks in the Future

Seija Tiainen and Robert Guinness

Technological progress and different positioning devices and systems are becoming more common. They will also bring new opportunities for new kinds of applications that use positioning and satellite-based tracking. Users of new services will be traditional actors, authorities and other public-sector operators, commercial service providers, individuals, as well as criminals. Other unpredictable new actors my also present themselves. A wide range of smaller and more intelligent tracking devices and various kinds of sensors offer new possibilities for the use of positioning information, both authorized and unauthorized. New use will create challenges for the activities' legislators.

The development of new technology and applications will provide new directions for the future and for future risks, as well as the future drivers of change: political, economic, ecological, etc. They provide opportunities for new kinds of applications and services, but also create new risks and challenges to the use of satellite-based tracking.

6.1 New Services

In Europe, Galileo will be a springboard to new services. The Galileo Programme achieved a significant milestone on 21 October 2011 with the launch of the first two In-Orbit Validation satellites for the Galileo constellation. The plan is to build up an "Initial Operational Capability" (IOC) for Galileo by around 2014. Two additional In-Orbit Validation satellites are planned for launch during 2012.

These four satellites will provide a satellite constellation large enough for testing purposes. As more satellites are added to the constellation in the following years, Galileo will achieve greater coverage (in space and time) of positioning and navigation services. After launching a total of 18 satellites, the programme would declare “Initial Operational Capability” because the coverage will be good enough to provide a useful service.

After that, the programme plans to launch another 12 satellites to achieve Full Operational Capability (FOC) with 30 satellites. The length of time between IOC and FOC is mainly not an issue of technological development, but more about how quickly the European Commission will procure and launch satellites. The plan calls for FOC by around 2019.

The launch of the two In-Orbit Validation (IOV) satellites in the end of 2011 is certainly an important step in this programme. A more important step, however, will occur sometime next year when they launch the two additional IOV satellites. This will bring the constellation up to four satellites, which will allow the European Space Agency to perform some detailed tests of the positioning capabilities.

The IOV satellites are essentially the same design as the fully functional satellites that will be launched later on in the programme. The only difference is the IOV satellites have a lower power capability, which means a weaker signal will be seen on the ground. This appears to have been a cost-saving choice to go with a lower power capability for the testing phase.

From the SATERISK perspective, it is important to note that if a GNSS receiver is compatible with Galileo, then additional GNSS satellites will provide benefits for positioning coverage, especially in areas where some of the sky is obscured (i.e. urban environments). As to whether Galileo’s Safety-of-Life Service or other special services will provide any additional value, the answer is difficult to ascertain. In any case, it is likely that such added value will not be realised until near the end of this decade.

Given the history of the Galileo programme — and the history of many large space projects — it is still quite likely that the stated dates will be adjusted further into the future. There is always the chance for launch failures and other technical or political challenges. As the programme advances, however, there will be less likelihood of major delays. One reason is that successful launches usually also help to shore up political support. Observers will certainly be watching to see whether Galileo successfully completes the

In-Orbit Validation phase next year. After that, one could ironically say the programme will be on much “firmer ground”.

The study by Rajamäki and Kämppi (2011) states that European public protection and disaster relief operators can only be self-dependent if their tracking is based on Galileo, the only European global navigation satellite – supported by other GNSS systems. The study by Rajamäki (2012a) supports this finding. Also, the power consumption of the tracking device could be a critical factor, especially during emergencies, in sparsely populated areas and in surveillance operations (Rajamäki & Kämppi, 2012; Rajamäki, 2012a, Rajamäki, 2012b). Combining a device’s power consumption optimisation with utilising energy harvesting from ambient vibrations, wind, heat or light and new high-energy rechargeable battery technologies, a multiplied running time could be achieved. After presentation of the study by Rajamäki and Kämppi (2011), a revised paper was requested: it (Rajamäki, Kämppi, Timonen & Savikumpu, 2012) has been made and sent for a reviewing process.

Rajamäki, J. and Kämppi, P. (2011). Secure and Reliable Satellite-Based Tracking System for Emergency Management. The International Emergency Management Society / Disaster Control and Emergency management, TIEMS DCEM 2011 workshop, June 13-14. Espoo.

Abstract: A Geographic Information System (GIS) offers a great deal of assistance in emergency management. Satellite-based tracking has long been considered a technology that compliments GIS operations. However, current satellite-based tracking systems have serious technical flaws and vulnerabilities. The SATERISK project yields information about the present and the future risks of satellite-based navigation and tracking systems. This paper presents a detailed modular system-level description for the satellite-based tracking system evolved within the SATERISK project including control, space, tracking, communication, data processing, end-user and external applications segments. The paper further discusses and suggests how the technical vulnerabilities of satellite-based tracking systems could be avoided, taken in e.g. a hybrid tracking segment and multichannel communication paths.

Rajamäki, J. (2012a). Optimized Power Consumption of GNSS Devices Enables Improved Safety and Security Response in Remote and Sparsely Populated Areas. Risks, Danger and Safety - Spring Symposium on Tourism Safety and Security, April 16-18. Rovaniemi.

Abstract: Satellite-based tracking system combines navigation and telecommunication technologies. Tracked devices use Global Navigation Satellite Systems (GNSS) for positioning, and the data is delivered for post-processing via mobile networks. Smart phones are the most common GNSS-receivers and their technology burgeons. Also, many companies are developing tracking sensors. However, the majority of sensors consume a dreadful amount of energy for long-lasting mobile use. Most sensors are "stupid" requiring commands for almost all tasks. Some "smart" sensors exist for technical surveillance and information gathering targeted at law enforcement agencies. With artificial intelligence (AI), the tracking sensors are able to adjust according to the behaviour of the target also making sensors more power efficient. A multi-talented, intelligent and smart tracking sensor can monitor the environment, e.g. light conditions, temperature, vibration, GNSS location and cell location. This information helps to visualize happenings at scene. Sensors' own AI-brains make necessary decisions, generate alerts and facilitate help in tough situations.

The SATERISK project has studied risks associated with GNSS-tracking, more specifically whether the use of tracking generates additional risks. For example, a GNSS-device battery may die during a long-distance hike that leaves hikers with no way to navigate in the wilderness. Excessive trust in GNSS-technology could end in disaster. However, GNSS-tracking systems enable many possibilities for improved safety and security response in remote and sparsely populated areas, especially if their energy consumption is optimized. The end-user should be the development target for the whole efficiency chain, from the sensor to the information. It is essential, as a big part of the power consumption relies on how equipment behaves. The next step will be to look for energy harvesting, through other means which enables smart sensors for lasting performance.

Rajamäki, J. (2012b). Law Enforcement Authorities Special Requirements for GNSS. 6th GNSS Vulnerabilities and Solutions Conference Programme, May 21- 24 2012, Baška, Krk Island.

Abstract: Professional criminals are aware that Law Enforcement Authorities (LEAs) are gathering information about them, their actions and whereabouts. They have learned to find a tailing car among other traffic. GNSS-based tracking is a good tool for LEAs, because a small device under the car is harder to find than a tailing car. But criminals are learning: they have learned to check their vehicles and use other countermeasures. Therefore, LEAs need new tracking sensors which are resilient to these countermeasures.

Many companies are developing tracking sensors based on commercial GNSS and GSM chipsets and software. Their miniaturizing progresses mostly concentrate on hardware size ignoring the software. For that reason, a majority of the tracking sensors on the market consumes too much energy for LEAs' use. For civilian use, battery duration of 16 hours is enough, because the transmitter can be recharged over-night. In professional LEA usage, this development leads to a situation where the actual tracking sensor is small enough, but batteries are bulky, being difficult to conceal. Energy can be sometimes taken from a car's network, but nowadays criminals keep watching their cars more carefully so the deploy time of tracking sensors is usually too short for that. With modern cars' CAN-bus electrical and alarm systems make this even harder. For these reasons, battery-based operation is the best option, but most tracking sensors are able to operate only a couple of weeks with the same batteries. If an operation lasts for a month, the batteries must be changed. The time needed for changing batteries and spent with the target is much more dangerous than remote operation of sensors. Also, disguising sensors is difficult if batteries must be changed every now and then. In some cases, risks are so high that LEAs must drop using tracking. Current tracking sensors are "stupid" in a sense that they need commands from operators for almost all tasks. Usually a sensor includes only motion detectors; if the motion of the tracking sensor stops, sending of position information also stops until the motion continues. In many cases, no case officer is watching

the tracking information at night time. So, if something unexpected happens, the sensor's behaviour is not optimal.

Criminals are already using countermeasures e.g. jamming to prevent LEAs from tracking. Jamming is a transmission of interfering radio signals that disrupt communications by decreasing the signal-to-noise ratio. The concept can be used against wireless data, like the signals from GNSS-satellites to disrupt information flow. The current sensors cannot distinguish jamming from a normal situation, where the satellites are not visible to the tracking device. This means that when the criminals are using jamming, LEAs have no way of detecting if the disappearance of position information is due to the lack of satellite visibility, due to some malfunction in the equipment or due to jamming.

6.2 Risks in the Future

With regard to the SATERISK project, Laurea's undergraduate students Miikka Ohisalo, Otto Tiuri and Tatu Urpila started their research work by studying today's satellite-based tracking-related risks within the field of transportation and logistics. They then expanded the work to concern the future. The group produced two non-public reports that were delivered to the SATERISK partners. This work has been the basis for the two publications introduced later in this section.

The goal of the study by Ohisalo, Tiuri, Urpila and Rajamäki (2012) was to imagine "what is possible in the future". From those future scenarios, they were to find out what kinds of risks may be generated, including also the alternatives that seem to be very improbable and unreal. Risk scenarios were presented from the point of view of logistics, society and satellite-based tracking. A wide range of risk sources was analysed: natural disasters, crisis and conflicts, technical, commercialisation of satellite systems and new kinds of services. Natural disasters, like solar storms or volcano eruptions, might interfere with GNSS systems. Spring 2010 showed how strong an effect an ash cloud from the Icelandic volcanic eruption could be: it stopped air traffic in Europe for many days. The study by Ohisalo, Tiuri, Urpila, Kämppi and Rajamäki (2011) continues the task, for example, by going through technical risks more precisely. Technically, there may be a variety of new risks in the future. The age of satellites is limited and renewing of the technology requires huge investments. Experts evaluate that in addition to satellites, over 300.000 pieces of space debris are orbiting the Earth. There is congestion in the sky and collisions with satellites are possible. New services and methods of using satellite-based tracking may also generate expected and unexpected risks. For example, in Finland, the usage of GNSS for congestion charges and toll systems has been studied for a long time. In 2012, the Minister of Transportation has established a toll system working group – and one of its main tasks is to clarify the risks.

Ohisalo, M., Tiuri, O., Urpila, T. & Rajamäki, J. (2011). Future Risks of Satellite-based Tracking. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11). Meloneras, Canary Islands, 40-45.

Abstract: This study investigates if in the future, some special risks concerning satellite-based tracking and navigation occur. To find out possible future risks, future research methods such as scenarios were being used. Forecasting the future is impossible, but the risks found are based on events that have already occurred or scientific research of interesting phenomena. The risks found concern natural disasters, technical errors and political and economic situations worldwide.

Ohisalo, M., Tiuri, O., Urpila, T., Kämppi, P. & Rajamäki, J. (2011). Risks and vulnerabilities of future satellite-based tracking systems. International Journal of Geology. Issue 4. Volume 5. pp. 142-149.

Extended abstract: This study, belonging to the SATERISK project, introduces possible risks of satellite-based tracking and navigation generally and especially from a logistics point of view. This paper presents multiple diverse risks, some of which might sound even unreal or unlikely to occur. The concept of risks plays an important role in future studies and in all future thinking. To find out possible future risks, future research methods such as scenarios and weak signal *identifications were being used. The future will most likely bring multiple new risks to the field of satellite-based tracking. 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 expanding market in the future. A variety of the services is growing and the customer has to use more time and effort to find the best and most reliable alternatives.*

References

Ohisalo, M., Tiuri, O., Urpila, T., Kämppi, P. & Rajamäki, J. (2011). Risks and vulnerabilities of future satellite-based tracking systems. International Journal of Geology. Issue 4. Volume 5. pp. 142-149.

Ohisalo, M., Tiuri, O., Urpila, T. & Rajamäki, J. (2011). Future Risks of Satellite-based Tracking. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11). Meloneras, Canary Islands, 40-45.

Rajamäki, J. (2012a). Optimized Power Consumption of GNSS Devices Enables Improved Safety and Security Response in Remote and Sparsely Populated Areas. Risks, Danger and Safety - Spring Symposium on Tourism Safety and Security. April 16–18, Rovaniemi.

Rajamäki, J. (2012b). Law Enforcement Authorities Special Requirements for GNSS. 6th GNSS Vulnerabilities and Solutions Conference Programme. May 21- 24, Baška, Krk Island.

Rajamäki, J. & Kämppi, P. (2011). Secure and Reliable Satellite-Based Tracking System for Emergency Management. The International Emergency Management Society / Disaster Control and Emergency management, TIEMS DCEM workshop. June 13-14, Espoo.

Rajamäki, J., Kämppi, P., Timonen, T. & Savikumpu, J. (2012). Secure and Reliable Satellite-Based Tracking System for Emergency Management. Int. J Emergency Management, submitted for publication.

7 Conclusions and Further Research

Jyri Rajamäki, Juha Knuuttila, Robert Guinness and Rauno Pirinen

The goal of the SATERISK project was to study risks associated with satellite-based tracking, and specifically whether the use of satellite-based tracking generates additional risks. The project analysed risks using different approaches: legal, technical and how the tracking is used. It also studied future requirements and potential risks in the future.

The main sponsor of the SATERISK project was the Finnish Funding Agency for Technology and Innovation, Tekes. Other partners were Finnish industry and governmental partners. The project included collaboration with universities internationally, including the University of Arizona and Portsmouth, and some Russian Universities.

Laurea was concentrating in risks connected to technical solutions and equipment or generated by the way of using the tracking. Risks were analysed mainly from the tracker's point of view. Laurea was also studying aspects needed in the future when new satellite systems like Galileo and new end-user systems and mapping and tracking solutions are in use.

According to one SME partner, the main impact of the SATERISK project so far has been that the topic 'risks of satellite-based tracking' has received more widespread attention. This intelligence-gathering and surveillance provider was filled with a foreboding of problems to come with today's commercial satellite-based tracking services. Because of the SATERISK project and its results, the company's customers have become more aware of the risks that come with using these services. This has increased the demand of their proprietary surveillance products and concepts, designed to mitigate these risks.

7.1 Spin-Off Research Projects from SATERISK

Jyri Rajamäki and Juha Knuuttila

Public protection and disaster relief operators use satellite-based tracking for improving real-time awareness. A research project proposal “MAYFLY”, in which the target was also to improve real-time awareness, was processed during the SATERISK project. The MAYFLY project was going to study the usage and future possibilities of micro-aerial vehicles. The MAYFLY project never started, but its preliminary studies were the basis for Laurea’s participating in the FP7 projects PERSEUS and AIRBEAM.

PERSEUS

The PERSEUS (Protecting EuRopean SEs and borders through the intelligent Use of surveillance) project addresses the call for an integrated European system for maritime border control. Its purpose is to build and demonstrate an EU maritime surveillance system integrating existing national and communitarian installations, and enhancing them with innovative technologies. By means of two large-scale demonstrations, the PERSEUS project will prove its feasibility and will set the standards and grounds for the future development of EU maritime surveillance systems.

The new maritime surveillance system is expected to increase the effectiveness of the current systems by creating a common maritime information sharing environment for the benefit of the network including National Coordination Centres, Frontex and the European Maritime Safety Agency (EMSA). The project also envisages collaboration with non-European countries and international agencies such as NATO or the International Maritime Organisation (IMO), among others.

This system-of-systems will use all the information provided by the European and national agencies. The data will be integrated and processed for better quality, thus obtaining filtered, reliable and more useful information. In particular, the PERSEUS project is meant to support the implementation of EUROSUR.

AIRBEAM

The AIRBEAM (AIRborne information for Emergency situation Awareness and Monitoring) project proposes to form a situation awareness toolbox for the management of crisis over a wide area, taking benefit of an optimised set of aerial (unmanned) platforms, including satellites. The number of unmanned air- and space-borne platform available and their associated sensors present a new set of challenges to end users involved in the effective management of emergencies and actions of law enforcement.

Within the scope of crisis management, the project intends to provide official public users from each Member State with the means to specify their own needs and to assess the technical solutions provided by unmanned aerial platforms. Through intense collaboration between industrial partners, stakeholders and end users, the AIRBEAM project will define an ambitious yet realistic concept of use.

By running scenarios that will be properly selected and defined by the end users within the project in a simulated environment, the increased capabilities for situation awareness will be assessed methodically. Various platform and sensor mixes will be compared using key performance indicators among which is cost effectiveness.

Live demonstrations with multiple civil unmanned aerial platforms will complete these ground simulation exercises in demonstrating to end users the potential and maturity of the coordinated use of multiple platforms.

7.2 Connections between Laurea's Security Projects

Jyri Rajamäki and Juha Knuuttila

The SATERISK project has also affected other projects that focus on technology, equipment and applications used by public protection and disaster relief. On-going projects include MOBI and MACICO, and the OPULENSING project proposal has been sent forward. Connections between these projects are shown in figure 2.

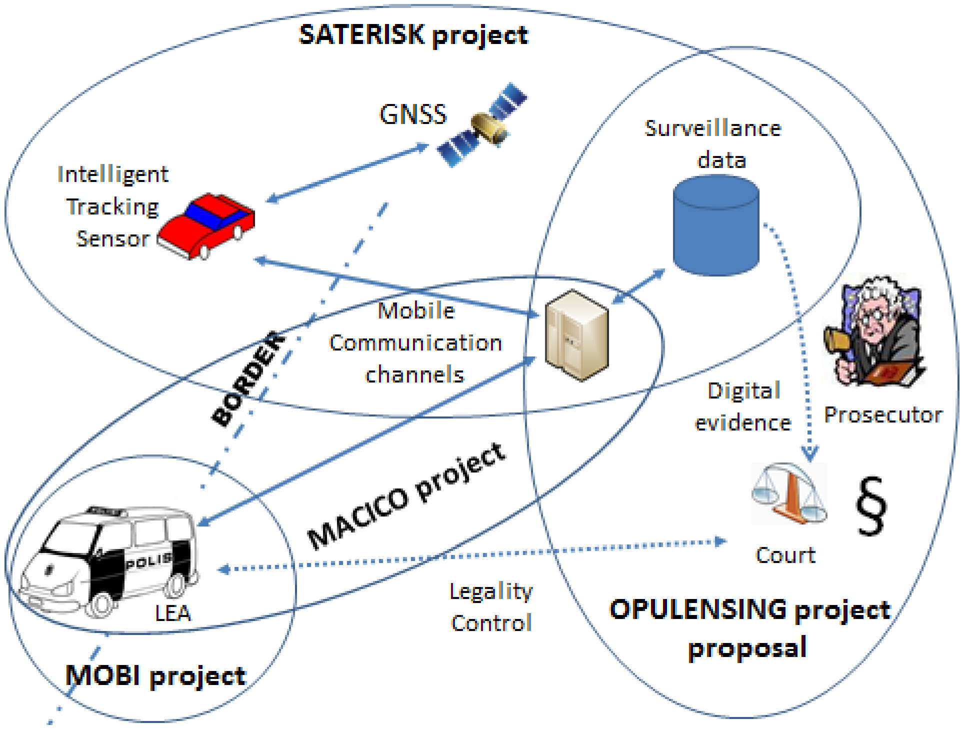

Figure 2: Connections between Laurea's security projects

MOBI

During recent decades, the amount of technical devices and applications in authorities' vehicles has been increasing. All this has generated new problems with air bags, power supply and cables etc. Documentation of applied solutions has been variable, and there has been no standardisation, which is needed in this field, particularly because of the diversity of the equipment suppliers.

The objective of the MOBI (Mobile Object Bus Interaction) project is to enhance the ICT integration of emergency vehicles and create a base for an emergency vehicle concept suitable for export. It will address the above issues through a user-centred program of research that will culminate in new recommendations and designs for an integrated platform for use in authorities' vehicles, including police, fire and rescue, and customs, and border control.

MACICO

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

The way to organise this foreign use of a radio network is to be defined and validated by security organisations. The work of the project will be carried out in cooperation with the public safety authorities. Requirements for these communications will be led by concrete use cases. Interworking at the border will then address TETRA (TErrestrial Trunked RAdio) -Tetrapol, TETRA-TETRA, and Tetrapol-Tetrapol interworking as well. From these requirements, the definition on the way to deploy terminals to foreign organisations, the way to organise and to deploy the solutions including gateways, will be defined in any of the interworking cases.

The project is innovative because it addresses not only the interoperability issue, but also the complete procedure that accepts foreign users on a security radio network (which is a priori forbidden for them) and looks for a solution that keeps the intrinsic security mechanisms of such networks.

OPULENSING

The OPULENSING project, if accepted, will concentrate on privacy issues with regard to tracking information acquired by LEAs. The aim of the project is to integrate the following hardware and software elements with relevant regulation: (1) technical intelligence gathering, (2) legal control and (3) the service provided by the project. This integration enables transparent and reliable business that supports investigation and strengthens legal process.

The results of the SATERISK project will be very relevant in this project as well. From these developments, it is clear that risk analysis of satellite-based tracking will only increase in importance, as tracking and localisation services become more widespread and more critical to operations of safety and security professionals.

7.3 Further Academic Work

Robert Guinness and Rauno Pirinen

Robert Guinness, Smart Spatial and Contextual Thinking, Tampere University of Technology

The topic of my PhD research is “smart spatial and contextual thinking.” The goal is to use spatial and contextual information to determine the situation or “context” in which a user is situated. This goal is closely related to the task of *activity recognition* but can also include recognition of other parameters, such as environmental factors and social interactions.

The primary sources of the spatial and contextual information used in this research are the sensors available in modern smartphones. These include accelerometers, magnetometers, gyroscopes, barometers, light sensors, microphone, wireless signal receivers (e.g. WLAN and Bluetooth), and GPS receivers. In addition, the use of other low-cost sensing systems that can be installed in indoor environments (office, home, transportation hubs, shopping malls, etc.) will be investigated.

There are a wide number of applications related to this research. Some examples include: improving home health and wellness care for the elderly and disabled, creating efficient and “smart” office environments, controlling high-security environments, and intelligent transportation systems. Applications in several of these areas will be prototyped in order to validate and demonstrate the developed methods.

SATERISK is an important predecessor to this research because SATERISK has highlighted the limitations of relying solely on GNSS for location-based services. These limitations can be overcome by utilising additional sensors, however, *contextual awareness* is often necessary in order to determine the optimal set of sensors to be employed in a given situation.

The study of SATERISK has significant implications for further research in perspective of actualisation and dissemination of real R&D in higher education. The first implication addresses the cooperation and activities of regional R&D collaboration in higher education. This research question would be: how would collaboration in regional R&D be understood, designed, defined and actualised in higher education? This question would extend to: (1) what are the characteristics and relations of the dynamic and core capabilities in a region; (2) how would the regional capabilities be linked to the competences, activities of schools, and R&D; (3) how could future research be used more effectively in exploring potential and novel R&D and operational environments, such as living labs and environments of last-mile research; (4) how could enough shared vision be built in a region, the regional development network consists of actors with different backgrounds and aims; (5) how can we build a portfolio of strategies in a region to enable a successful future R&D path to take place; and (6) how should the significance of regional innovation networks be thoroughly analysed as part of regional, national, and sectorial innovation systems with cooperation and learning activities?

Second, several implications in the actualisation of SATERISK address the interests in management-leadership concepts and models, which would support imagination-creativity-innovation activities in higher education and boost cooperation in its networks. Education within R&D requires a close and trust-based collaboration between personnel and management, as well as with students and participants of work communities, which have an increasing role in collaboration and R&D activities. The development of organisational culture, agility-profile relations, elasticity, creativity boosting, and trust-commitment-based management between all actors would then be in the interests of future research. In these actualisation standpoints, the implications of SATERISK include two relatively different views: (1) how to understand the everyday line management (as budget responsibility and management) in this situation and (2) how to conduct and save agility-, trust-, motivation-, creativity- and vision-based profiles, triggers, drivers, and enablers in higher education with its collaborative networks (as vision-based and motivation-based leadership boosting).

Third, the study has implications for further research for a deeper understanding in the measuring of results and impacts as evaluation design of higher education. The future research question would include: (1) how to understand conceptualisation of information and its quality in the union of regional innovation networks, higher education and R&D, and then (2) how to measure achieved impacts such as longitudinal impacts over regional actors in the perspectives of learning by success, learning by feedback and learning by failure. It is particularly difficult to identify the effect of the lead instructors on the students' creativeness. The learners often worked together and guided activities, such as scaffolding effects from the background. The actualisation of SATERISK undertakes that instructors contributed to creativeness within the community, but measuring of mutual influences is challenging; regardless, is it necessary, in the perspective of the assessment of learning, because the results can be reported and often demonstrated in the end.

7.4 Epilogue

Robert Guinness

It is widely accepted that satellite-based tracking is very robust and unparalleled compared to alternative / previous tracking methods. Significant risks and limitations, however, do exist and must be considered when implementing specific applications and services. This project has investigated such risks and limitations, and a sampling of the relevant risks includes:

- Signal blockage and multipath effects in urban areas
- Intentional or unintentional radio signal interference
- Information security of the tracking payload
- Tracking device failures / limitations
- Communication service interruptions / limitations
- Legal restrictions

SATERISK has also highlighted the fact that a full analysis of relevant risks must be analyzed on an application/use-case specific level. Even then, such analysis is largely limited to a qualitative nature. Generalized risk analysis, although useful, will largely be limited to "awareness raising" and to providing a survey of issues to be considered when developing new systems / devices / applications /services.

New and modernized GNSS will mitigate some risks, but will also make receiver design more complex. Mutli-GNSS systems hold promise for a more robust positioning solution, but it remains to be shown whether such receivers will meet the stringent size, power, and cost constraints of many applications and thus offer a realistic alternative to GPS-only receivers.

Another topic that was raised during the SATERISK project was whether or not a two-way communication link from GNSS would be necessary for certain applications, and if so, can such a solution compete with existing telecommunication alternatives? This is an important topic for further study, especially given the plans for Galileo's search and rescue service.

From a pedagogical standpoint, GNSS (and satellite-based tracking in particular) provide a wealth of interesting subjects for UAS students at both the bachelor's and master's levels, ranging from theoretical to practical. During the SATERISK project, field testing and application development were popular with Finnish UAS students, as well as international exchange students who took part in SATERISK research. Several student projects were conducted in close collaboration with companies, and not surprisingly we found this to be the ideal case in terms of authentic hands-on learning and preparation for working life.

Although the SATERISK project comes to a conclusion, research related to satellite-based tracking and GNSS is far from complete. Several participants in the SATERISK project will continue with PhD studies in related areas (the present author included). In addition, several related research projects have already been initiated at Laurea UAS and elsewhere. A good example is the DETERJAM project of the Finnish Geodetic Institute, which is researching GNSS jamming from a detection and mitigation perspective.

Providing a robust positioning solution is central to so many applications that it is impractical to cover them all in one volume or investigate them all in one project. In conclusion, GNSS provides an accurate positioning solution for many environments and situations, but it is safe to say that it does not and will not provide accurate positioning in all environments or all situations. Thus, there is a need for alternatives and to GNSS that will augment and improve a system's overall positioning capability. System designers and end-users alike will be well served to keep these points in mind, and hopefully this volume will serve as a poignant reminder.

List of Publications

Journals

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

Ohisalo, M., Tiuri, O., Urpila, T., Kämppi, P. & Rajamäki, J. (2011). Risks and vulnerabilities of future satellite-based tracking systems. International Journal of Geology. Issue 4. Volume 5. pp. 142-149.

Pirinen, R. (2011). Externally Funded Research and Development Projects in Perspective of Learning. International Journal of Engineering Pedagogy (iJEP), 1(3), 27-36.

Pirinen, R. (2009). Actualization of Learning by Developing (LbD): an Analysis. International Journal of Emerging Technologies in Learning (iJET), 4(3), 46–58.

Tuohimaa, T., Tikanmaki, 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, Issue 5, Volume 5, 602-609.

Viitanen, J., Happonen, M. Patama, P. & Rajamäki, J. (2010). Near Border Procedures for Tracking Information. WSEAS TRANSACTIONS on SYSTEMS. Issue 3. Volume 9. pp. 223 – 232.

Peer-Reviewed Conference Papers

Happonen, M., Viitanen, J., Kokkonen, P., Ojala, J. & Rajamäki, J. (2009). Jamming Detection in the Future Navigation and Tracking Systems. In Proc. 16th Saint Petersburg International Conference of Integrated Navigation Systems. St. Petersburg, 314-317.

Kämppi, P., Guinness, R. & Urpila, T. (2010). Field Testing for Satellite Based Tracking Systems. 61st International Astronautical Congress. Prague.

Kämppi, P. & Guinness, R. (2010). Technical Risk Analysis for Satellite Based Tracking Systems. Integrated Communications, Navigation and Surveillance conference 2010. Herndon. M3-1 – M3-16.

Kämppi, P., Rajamäki, J. & Guinness, R. (2009a). Information Security in Satellite Tracking Systems. In Proc. 3rd International Conference on Communications and Information Techonolgy2009. Athens. 153-157.

Ohisalo, M., Tiuri, O., Urpila, T. & Rajamäki, J. (2011). Future Risks of Satellite-based Tracking. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications. Meloneras, Canary Islands, 40-45.

Pirinen, R. (2008). Integrative Learning Environments in perspective of Regional Development. Proceedings of Pascal International Conference, University of Limerick, 28–30 May.

Pirinen, R. (2011). Learning within Externally Funded Research and Development Projects in University of Applied Sciences: An Analysis. 2011 14th International Conference on Interactive Collaborative Learning (ICL). 175 – 182.

Pirinen, R., Tarkkanen, J., & Teräs, J. (2009). Integrative Action Models in Regional Development, Applied Triple Helix. Proceedings of Triple Helix XII Conference, 17–19 June, Glasgow.

Rajamäki, J. (2009). Elasticity of Research Objects as of Great Concern to Innovative LbD Projects. Case: SATERISK. The Learning by Developing – New Ways to Learn, Conference Proceedings, Laurea publications, D•7, Vantaa. 195-206.

Rajamäki, J. & Fred, M. (2011). Externally Funded Research Development and Innovation Projects as Learning Environments – Case: SATERISK. In Proc. The International Technology and Development Conference. 4130-4139.

Viitanen J., Happonen M., Patama, P. & Rajamäki J. (2009). International and Transorganizational Information Flow of Tracking Data. 8th WSEAS International Conference on Security and Privacy. Tenerife, Canary Islands, Spain.

Viitanen, J., Patama, P., Knuuttila, J., Rajamäki, J. & Ruoslahti, H. (2010). Towards transparent authority of power in law enforcement. The 12th Annual Conference of the Finland Futures Research Centre and the Finland Futures Academy: Security in Futures – Security in Change, 3-4 June, Turku, Finland.

Viitannen, J., Patama, P., Rajamäki, J., Knuuttila,J., Ruoslahti, H., Tuohimaa, T. & Tikanmäki, I. (2011). How to Create Oversight in Intelligence Surveillance. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications, March 24-26, Meloneras, Gran Canaria, 52-56.

Conference Presentations and Submitted Papers

Ovaska, L., Tervahartiala, J., Tervola, S., Johansson S. & Rajamäki, J. (2012). How Transparency Improves the Control of Law Enforcement Authorities' activities? European Intelligence and Security Informatics Conference 2012. August 22-24, Odense, submitted for publication.

Rajamäki, J. (2011). Vulnerabilities in Satellite-Based Tracking Systems. Plenary Lecture, the 9th WSEAS International Conference on APPLIED ELECTROMAGNETICS, WIRELESS and OPTICAL COMMUNICATIONS (ELECTROSCIENCE '11), Meloneras, Canary Islands.

Rajamäki, J. (2012a). Optimized Power Consumption of GNSS Devices Enables Improved Safety and Security Response in Remote and Sparsely Populated Areas. Risks, Danger and Safety - Spring Symposium on Tourism Safety and Security. April 16–18, Rovaniemi.

Rajamäki, J. (2012b). Law Enforcement Authorities Special Requirements for GNSS. 6th GNSS Vulnerabilities and Solutions Conference Programme. May 21-24, Baška, Krk Island.

Rajamäki, J. & Holmström, J. (2012). Tracking cross-border criminals with satellites – SATERISK project. PSCE Conference. May 30-31, Helsinki.

Rajamäki, J. and Kämppi, P. (2011). Secure and Reliable Satellite-Based Tracking System for Emergency Management. The International Emergency Management Society / Disaster Control and Emergency management, TIEMS DCEM workshop. June 13-14, Espoo.

Rajamäki, J., Kämppi, P., Timonen, T. & Savikumpu, J. (2012). Secure and Reliable Satellite-Based Tracking System for Emergency Management. Int. J Emergency Management, submitted for publication.

Theses

Aho, A. (2009). Google Mapsin käyttö karttapalvelun toteutuksessa. Thesis. Theseus. Espoo: Laurea (in Finnish).

Happonen, M. (2010). Recognising Risks Of Satellite-based Tracking. Master thesis. Theseus. Espoo: Laurea.

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

Kämppi. P. (2011). Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multimethodology Research. Master thesis. Theseus. Espoo: Laurea.

Kääpä, J. (2010). Paikannuslaitteen käyttö autonlämmittimen etähallintaan, Case uTrace Evaluation Kit. Thesis. Theseus. Espoo: Laurea (in Finnish).

Ojala, J. (2010). Tekninen seuranta poliisin salaisena pakkokeinona. Master thesis. Theseus. Espoo: Laurea (in Finnish).

Pelkonen, T. (2012). Paikannuspohjaisten pelien tietoturva pelaajan kannalta – case Geokätköily ja Foursquare. Thesis. Espoo: Laurea (in Finnish), submitted for evaluation.

Vaarakallio, J. (2010). Galileo-satelliittipaikannusjärjestelmä ja sen mahdollisuudet yrityksen näkökulmasta. Thesis. Theseus. Espoo: Laurea (in Finnish).

Viitanen, J. (2009). SATERISK-projektin suunnittelu ja vaatimusmäärittely. Master thesis. Theseus. Espoo: Laurea (in Finnish).

List of Authors

Name	Position at Laurea	Position at the project
Aho, Anne	Student	Bachelor's thesis worker
Aro, Mari	Student	Technical editor
Erling, Tapani		Partner
Fred, Minna	Senior lecturer	Researcher of Living Labs
Guinness, Robert	Project worker	Researcher of GNSS
Happonen, Markus	Graduate student, Lecturer	Project member, Master's thesis worker
Holmström, John		Partner
Johansson, Sari	Graduate student	Participator
Knuuttila, Juha	Principal lecturer	Accountable project leader
Kokkonen, Pertti	Graduate student	Master's thesis worker
Kämppi, Pasi	Graduate student	Project member, Master's thesis worker
Kääpä, Jukka	Student	Bachelor's thesis worker
Ohisalo, Miikka	Student	Project worker
Ojala, Jussi	Graduate student, Senior lecturer	Project manager Feb. - April 2009, Master's thesis worker
Ovaska, Leila	Graduate student	Participator
Patama, Pasi	Graduate student	Member of steering group, Representative of Trevoc
Pauli, Stigell		Member of steering group, Representative of Tekes
Pelkonen, Tiia	Student	Bachelor's thesis worker
Penttinen, Jyri	Graduate student	Participator
Pirinen, Rauno	Principle lecturer	Integrator of student-centred activities
Pitsinki, Heikki	Graduate student	Participator
Rajamäki, Jyri	Principal lecturer, Project director	Project owner, Scientific supervisor, Member of steering group
Ruoslahti, Harri	Senior lecturer	Researcher
Savikumpu, Jonna	Graduate student	Participator

Name	Position at Laurea	Position at the project
Tervahartiala, Jutta	Graduate student	Participator
Tervola, Sofia	Graduate student	Participator
Tiainen, Seija	Senior lecturer	Project manager May 2009 ->
Tikanmäki, Ilkka	Graduate student, Senior lecturer	Participator
Timonen, Timo	Graduate student	Participator
Tiuri, Otto	Student	Participator
Tuohimaa, Tuomo	Graduate student	Participator
Urpila, Tatu	Student	Research intern 2010.
Vaarakallio, Joonas	Student	Bachelor's thesis worker
Viitanen, Jouni	Graduate student, Senior lecturer, Lecturer	Project member, Master's thesis worker