Software Intensive GNSS-based Tracking Systems for Improving Law Enforcement

JYRI RAJAMÄKI
Service Innovation and Design, Leppävaara
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 Espoo
FINLAND
jyri.rajamaki@laurea.fi http://www.laurea.fi/en/leppavaara

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

Key-Words: - Chain-of-custody requirements, Crime Investigation, Global navigation satellite systems, Law enforcement, Law enforcement authority, Monitoring-of-legality, Software intensive systems, Technical tracking.

1 Introduction

Due to the economic situation, the main need of law enforcement agencies (LEAs) is to maintain their core services with significantly reduced budgets. This means that they need new innovations and automation equipment for routine tasks. Also, all information and communication technology (ICT) systems should have long life-time and new systems should be interoperable with old ones.

A Global navigation satellite system (GNSS) based sensors and systems benefits LEAs when tracking non-cooperative targets. However, management of numerous electronic tracking devices within many simultaneous crime investigations has proven to be a demanding task for LEAs. Complications have spawned many lawsuits and negative publicity. These episodes have diminished citizens' trust in a constitutional state. It has been verified by the means of participative observations that LEAs have a tendency to create two level systems: others work on the streets; others are valid at the Courts of Justice. Some European countries are well on the way towards this phase of development. The importance of transparency is emphasized within all EU administrative levels. However, LEAs concentrate only on data acquisition instead of making their operations transparent all down the line. Because of privacy protection of suspects, crime investigations and LEAs' data capture cannot be public. However, they could be so transparent that the critic and control made by citizens is possible to come true in respect of state authorities.

The European Commission has announced Horizon 2020, an €80 billion programme for investment in research and innovation. Horizon 2020 brings together all EU research and innovation funding under a single programme. It focuses on turning scientific breakthroughs into innovative products and services that provide business opportunities and change people's lives for the better. For the EU's secure societies challenges, the research priorities of the Horizon 2020 are about protecting European citizens, society and economy, assets, infrastructures and services, while not forgetting prosperity, political stability and well-being either. Organized crime and mobile organized crime groups are still considered to be some of the major challenges for the EU internal security to address. One of the key research areas in the secure societies theme of the Horizon 2020 is to fight against crime and terrorism. The research topic

FCT-05-2014 [1] concerns itself with novel monitoring systems and miniaturized sensors that improve LEAs' evidence-gathering abilities:

Investigations on the activities of criminal organizations usually require Law Enforcement Agencies (LEAs) to use electronic equipment for legal recording, retrieving and monitoring of criminal activities in a safe and unnoticed way, while keeping for both the sensors part and the monitoring station all the legal, integrity and chain-of-custody requirements that will enable the presentation of evidences obtained this way at the Courts of Justice.

Requirements for this equipment are very different from those offered by available commercial devices. Depending on the operation, the periods of time that these electronic devices have to work can range from days to months or in real time. Access to the device could be limited or impossible. Secure remote operation over radio channel (or other type of communication channel, including GSM networks) should be possible. Other requirement may apply like small size for easy concealment, low power consumption for extended time life, robustness and self- protection in addition to strong authentication mechanisms for operators and protection of the communication channels.

This paper collects together research results from four different research projects with regard to tracking of non-cooperative targets. The main research question is: How new types of satellite-based tracking sensors, mobile monitoring stations and their associated communication channels for LE operations can be understood and designed taking into account the chain-of-custody and monitoring-of-legality requirements?

2 Theoretical Framework

A global navigation satellite system (GNSS) based sensors and systems are very useful for law enforcement when tracking non-cooperative targets. Nowadays, law enforcement relies on and finds new uses for GNSS technology to assist in investigating crime and gathering evidence. LEAs ought to have forensics technology for investigations and field work. These kinds of technologies include advanced tracking systems that apply GNSS technology to track criminals and vehicles that have been tagged. This allows LEAs to keep track of suspicious activity and can help solve cases.

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

As the theoretical foundation of this study, the science of design for software-intensive system (SIS) towards new GNSS-based tracking system for improved law enforcement is proposed. A system can be defined generally as a collection of elements that work together to form a coherent whole, and SIS are systems in which some, but not necessarily all, of the component elements are realized in software [2].

2.1 Designing of Software-intensive Systems

Theory of complex systems traces its roots to the 60's when Simon wrote his book "Science of the Artificial" [3]. Fulfillment of purpose involves a relation between the artifact, its environment, and a purpose or goal. Alternatively, it can be view as the interaction of an inner environment (internal mechanism), an outer environment (conditions for goal attainment), and the interface between the two. The real nature of the artifact is the interface [2]. Both the inner and outer environments are abstracted away. The science of the artificial complex systems should focus on the interface, the same way design focuses on the "functioning." A general theory of complex systems must refer to a theory of hierarchy, and the near-decomposability property simplifies both the behavior of a complex system and its description [2].

Revolutionary advances in hardware, networking, information, and human interface technologies require new ways of thinking about how software-intensive systems (SIS) are conceptualized, built, and evaluated. Manual methods of software and systems engineering must be replaced by computational automation that will transform the field into a true scientific and engineering discipline [2]. The vision of science of design research for SIS should achieve the following essential objectives [2]:

1) Intellectual amplification: Research must extend the human capabilities (cognitive and social) of designers to imagine and realize large-scale, complex software-intensive systems.

2) Span of control: Research must revolutionize techniques for the management and control of complex software-intensive systems through development, operations, and adaptation.

3) Value generation: Research must create value and have broad impacts for human society via the science and engineering of complex software-intensive systems and technologies.

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

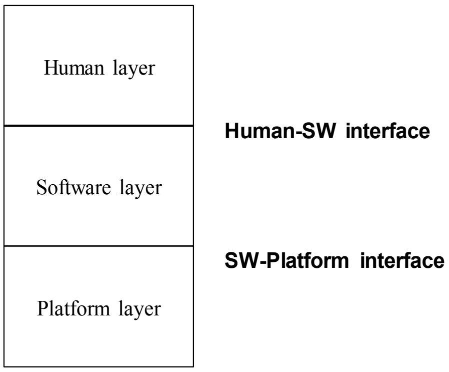

Fig. 1 Software-intensive systems layers

SIS design entails many important decisions such as the design and allocation of system behaviors (e.g., functions, actions) and system qualities (e.g., performance, security, reliability) to the different layers [2]. A particular system activity could be realized in hardware (platform), via e.g. a service call (software), by human behavior (human), or some combination of activities across all three layers, and a performance requirement (e.g., response time) for a SIS transaction could be divided and allocated as performance requirements in each of the layers. Nearly all future SIS will be connected to environmental resources and other systems via network connections and these connections lead to complex systems-of-systems architectures for providing behaviors and qualities [2]. There will be identifiable networks across all three SIS layers: physical networks support the transmission of digital and analog data among system platforms, software networks provide the middleware layers and protocols that transform the transmitted data into information that is shared among the information processing systems, and social networks provide a means of interaction and community among the human participants of the complex system [4].

2.2 Law Enforcement Technology Services

In the last two decades, modern technologies have become an inseparable part of our lives. Technologies facilitate our daily lives and nowadays it is not even possible to imagine that we can manage without them. Unfortunately, technologies facilitate daily lives not only of upstanding citizens, but of the organized crime, as well. Regrettably, organized crime often has wider possibilities to use the technological achievements than LEAs. However, in order to improve their evidence-gathering abilities, LEAs are constantly seeking new technological recording, information retrieval and monitoring solutions that would facilitate their combat against criminal organizations. The criminals' countermeasure activities, such as electronic counter-surveillance, jamming and constant changes in behavior to prevent eavesdropping or physical surveillance are continuously increasing [5]. The pressure to find new intelligent technologies, which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive, is emerging and is a high-priority task. Respecting the accountability and integrity requirements and smooth utilization of data in different phases of chains-of-custody is of utmost importance. In the current situation, the chain-of-custody is difficult to maintain due to different techniques that run on their own and are connected to different monitoring systems. This makes the LEA work very labor-intensive, so the use of new state-of-the-art technologies should enable the optimization of the use of human resources [6].

When LEAs are working in order to prevent and investigate crimes, some of the operations affect privacy of citizens. Video surveillance, audio surveillance and technical tracking are among those activities. Already in 2006, BBC News [7] listed some of the possible means for surveillance and tracking: CCTV cameras, automatic number plate recognition, radio frequency ID tags in shops, mobile phone triangulation, store loyalty cards, credit card transactions, satellites, electoral roll, national health service patients records, personal video recorders, phone-tapping, bugs and hidden cameras, worker call monitoring and cookies. Only LEAs can legally use the information from all these sources. In addition to using gathered data LEAs share information with other authorities. European integration has increased transport of illegal goods and criminals. Therefore, transmitting, tracking and other status information between nations and different organizations is becoming everyday business. For example, LEAs are using more tracking technology than ever before. The systems are network-based (GSM&TCP/IP) and they can transmit information basically anywhere. These days, technical tracking is used in even nominal cases [8].

Seeking to fight against organized crime, the EU should keep up with the development of technology. The EU should use all the benefits of the modern technologies in order to fight against criminal activities and promote cooperation among the EU Member States. In order to implement the desired goals, the European Network of Law Enforcement Technology Services (ENLETS) was established as a sub-group of the Law Enforcement Working Party of the EU Council in 2008. The main goal of this sub-group is to strengthen police activities and cooperation and increase the use of modern technologies in the process of exchanging information, knowledge or experience. Another goal of ENLETS is to develop a common single platform for the delegates of the EU Member States for information exchange. One contact person in every EU member country will be responsible for collecting information on the technological needs and for presenting those needs to ENLETS. This platform is necessary for the experts from the LEAs in order to share the news about the technology market and advice on the use of technologies in daily life of any officer. The primary goal is to use one common platform of ENLETS, which would be available for every EU member country, and in this way to avoid duplications of different systems which have already been used by some EU member countries. It is not a secret that technologies are quite expensive. For that reason, ENLETS is also trying to find possible financial solutions, concerning the implementation of technologies in the field of law enforcement. The new vision and mission for ENLETS are [9]:

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

ENLETS realizes its mission by co-operating on three levels/steps: (1) sharing of best practices, (2) co-creation of new technology services, and (3) research. Sharing of best practices that enables quick wins on the Europol Platform of Experts (EPE) is the most important task and priority of ENLETS [9]. Examples of shared best practices include: automatic number plate recognition, IT systems (open source and signals), tools for cross-border surveillance, and remote stopping of vehicles. The next step of ENLETS' technology scope is co-creation based on missing requirements within best practices. This step includes sharing (inter)national projects, such as biometrics, fraud identification, and covert surveillance multisensory tools (e.g. high-quality long-distance listening tools with chain-of-custody and privacy enhanced technology). These technology developments should be based on operational priorities with a short-to-market approach (1-2 years), industry being the developer. The third level of ENLES technology scope is the needed research that is not always in line with requirements. This is mainly carried out by the core group members of ENLETS that include The Netherlands, The U.K., Finland, Belgium, Poland and the EU's presidency country. ENLETS' role is to feed end-users' needs to EU research programmes, such as Horizon 2020. The new funding instruments 'pre operational validation' and 'pre commercial procurement' are good initiatives in Horizon 2020 [9].

2.3 GNSS-based Tracking Systems for Law Enforcement

A GNSS is a satellite navigation system with global coverage. GNSS-based navigation has become part of daily life. Timing, orientation, positioning and navigation are deeply embedded in the lives of everyone. The use of GNSS is still growing—a recent market research report predicts that the GNSS market will likely double by 2016 [10]. At the moment, only the U.S. NAVSTAR Global Positioning System (GPS) and the Russian GLONASS are global operational GNSSs. China is expanding its regional Beidou navigation system into the global Compass navigation system by 2020. The EU’s Galileo positioning system is a GNSS in its initial deployment phase. The European Commission launched its first two operational satellites in October 2011, and the Galileo system is scheduled to be fully operational by 2020 at the earliest.

The actual GNSSs vary, but generally they consist of three major segments: the space segment, the positioning equipment segment, and the control segment. For example, the space segment of GPS consists of a system of 24 space-based satellites, of which three are spares. The GPS satellite orbital radius is 26,561.7 km and each satellite has a 12-hour orbit. Precise time is provided by a redundant system of rubidium and/or cesium atomic clock boards for the space vehicle. Each GPS satellite is capable of continuously transmitting L1 and L2 signals (L1 = 1575.42 MHz and L2 = 1227.6 MHz) for navigation and timing, and L3 signal for nuclear detonation data [11]. It is also capable of receiving commands and data from the master control station, and da-ta from remote antennas via S-band transmissions.

In general, the GNSS receiver compares the time a signal was transmitted by a satellite with the time it was received. The time difference, along with the location of the satellites, allows the receiver to determine the user location. Signals from a minimum of four different satellites are required to determine the three-dimensional position. The receiver usually consists of an antenna assembly, radio frequency (RF) receiver, data processor, control/display unit, power supply, and interface unit [11].

The control segment commands, uploads system and control data to, monitors the health of, and tracks the space vehicle to validate ephemeris data. The control segment of GPS consists of a master control station located at Colorado Springs, five remote monitor stations which are located in Hawaii, Ascension Island, Diego Garcia, Kwajalein, and Colorado Springs, three ground antennas which are located at Ascension Island, Diego Garcia, and Kwajalein and a Pre-Launch Compatibility Station, which can also function as a ground antenna, located at Cape Canaveral [11].

2.4 Communication Systems

Telecommunications technologies have an important role within tracking systems: the communication segment delivers positioning data for post-processing and, further, to end-users. In most cases, the tracking device sends positioning data via mobile networks. The Internet or other networks are used to route positioning data from mobile networks for post processing, and this makes the system globally available. End-users can access their data via multiple different communication networks, as well [12].

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

In cross-border tracking operations, data is transferred via multiple telecom operators’ networks. Normally, data is not encrypted in operators’ core networks. Globally there are many different operators with different information security practices, so the end-user cannot rely on data being delivered safely. Data can be protected by establishing secure tunneling between the client and a data processing center or it can be encrypted before sending by using Secure Hash Algorithms (SHA) such as SHA-256, SHA-384, or SHA-512. By secure tunneling, data transfer can be made as secure as the chosen encryption method. The most common tunneling technique is IP Secure Architecture (IP-sec). In many cross-border operations, not a single public safety organization can work alone. Hence, co-operation is extremely critical between actors. The working parties should not simply trust and rely on their own resources. Regardless, only a few organizations possess all the required areas of expertise in a large-scale incident or disaster. Information sharing and education at the organizational level is required in order to achieve a working relationship between the actors. This requires actual and operational interoperability between the first responding organizations; also in reality and in the field – not only in the form of an official agreement but in a much larger scale [13].

With respect to European mission-critical public safety communications, TETRA or TETRAPOL is widely used and recommended. There are no other improved standards available at the moment. Data transmission over TETRA is rather slow and will not satisfy future needs. However, it is extremely reliable, regardless of its low capacity communication. Wideband data (TETRA Enhanced Data Services - TEDS) is an effort for improved data services, but TEDS falls short to current and future needs. However, a dedicated broadband public safety mobile data network independent of public mobile networks may not be available in Europe until 2020. The current situation needs complementary technologies in addition to TETRA. Research suggests that multichannel communications would solve the problem. There is a global demand for safe and secure multichannel communications, and it is expanding day by day [14].

All centralized solutions are vulnerable to many threats that include deni-al-of-service (DoS) attacks, system failures, repudiation, spoofing, tampering. Wherefore, decentralized modular communication and information management systems should be used; if one part goes down, other part works. Also, turning the services on a single operator is a risk. Utilizing parallel connections of multiple operators ensures connectivity, minimizes risks and maximizes reliability. Tracking applications need secure seamless wireless communication solutions with selectable level of quality-of-service (QoS) and wide coverage areas. Even though publically available wireless services usually provide reasonable coverage under acceptable cost conditions, most of the public providers do not offer any data service with a guaranteed QoS level. The principal improvement of QoS can be arrived at by the selection of the best possible alternatives from the set of currently identified available services, or by applying multiple communications systems parallel. The distributed systems intercommunication protocol (DSiP) allows the use of several parallel communication paths simultaneously, handles communication channel selection and hides link establishment issues from devices and/or software that wish to communicate with each other using the DSiP solution [15]. Efficient decision processes must be adopted to reach the relevant QoS. Success of such approach relies on a profound understanding of applied technologies and their performance described by their performance indicators. DSiP router's QoS option sets the desired order of the network access by desired cost-of-service (CoS) value [16].

2.5 Command & Control and Intelligence

Most new digital services for the public safety sector are supplied via stand-alone systems without in-built interoperability. There is a real lack of a coherent system that would coordinate the various technologies, and improves the system's accuracy and usability. According to Frost and Sullivan study [17], the need for interoperability between services is the key market driver with regard to first responders' communications, command and control, and the intelligence (C3I) market. The main market restraints are fragmented decision-making and budgetary allocations [17].

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

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

The end-user is not always the one actually controlling the sensor. In many cases, equipment is planted by technicians and not by LEAs who are using it. In most cases, the control of the sensor is far from optimal. There are several cases where the sharp-end equipment is running flat out and using its batteries when no-one is watching the information in real time, and the density of the information is not needed [5]. It is like running a car on a motorway in the first gear instead of sixth. The existing monitoring systems are developed for case-officers. There is a need to take into thorough consideration the organizational and procedural interoperability for example, by explaining how the prosecutors and courts can have access to the system and to the evidence.

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

2.6 Conclusions of Theoretical Framework

Fig. 2 summarizes the content of the review of the literature adopting the software-intensive system layers approach. There has been a gigantic shift from a hardware product based economy to one based on software and services. This has also been the fact with regard to law enforcement. For example, the ICT systems of a typical police vehicle already cost about the half of the costs of a new vehicle [18]. From every indication, the growth of the software layer, in size and percentage all of the overall systems will be the future trend. The software layer is a makeup of software code, information, and control within the context of an application domain. “The overlaps among these three concepts support varying methods and techniques of understanding and building the software layer of systems. For example, software architectures define structures for integrating the concept of code, information, and control for a particular application domain system” [2].

In a future world of pervasive computing and ubiquitous cyber-physical devices it is essential that IT artifacts and the integrated systems containing these artifacts are reliable, adaptable, and sustainable. Design for SIS should draw its foundations from multiple research disciplines and paradigms in order to effectively address a wide range of system challenges. The most important intellectual drivers of future science of design in SIS research will be dealing with complexity, composition, and control [2]

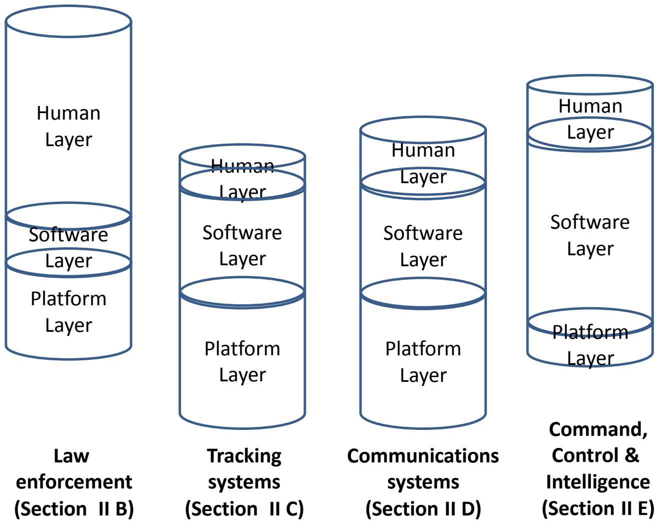

Fig. 2 Summary of literature review from SIS point of view

3 Results

3.1 Understanding GNSS for Law Enforcement

The major challenges that LEAs confront when using tracking equipment in crime investigations and preventions are [19]: (1) commercial GNSS sensors do not fulfil the needs of LEAs, (2) cross-border operations are problematic because criminal nature has internationalized but LEAs are national organizations, (3) secure mobile communications should be available worldwide, energy efficient and invisible for suspects, (4) investigation data should fulfil chain-of-custody requirements, and (5) LEAs operations should have societal acceptance and monitoring-of-legality.

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

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

LEAs' present-day ICT systems do not support cross-border cooperation. In addition to these technical challenges, the distrust between LE organizations is a tall order. Unfortunately, this distrust exists also at national level, and even between units of one organization. On the other hand, common ICT systems and operational procedures could increase the trust between parties. ENLETS' vision is to be the leading European platform that strengthens police cooperation and bridges the gap between the users and providers of law enforcement technology. The core group members of ENLETS should develop common procedures to apply new LE technology. In future, these procedures could be extended to other European countries as well as towards applying older LE technologies.

3.2 Model for Future Law Enforcement Intelligence System

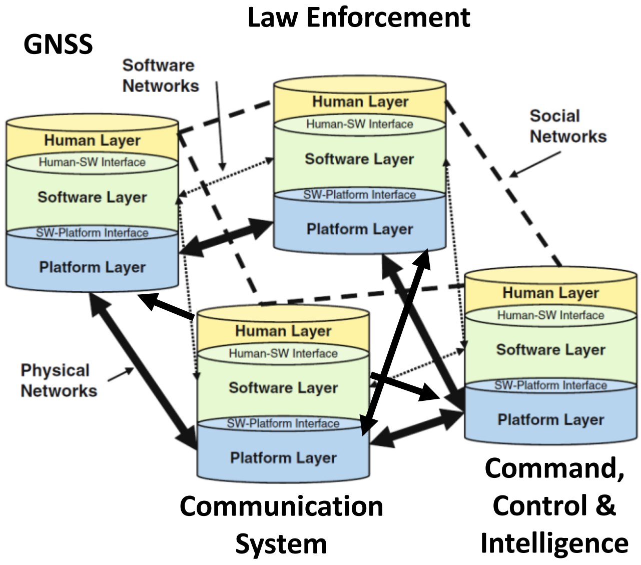

Fig. 3 SIS model for law enforcement tracking systems

Fig. 3 shows a model for LE satellite-based tracking systems and demonstrates the identifiable networks across all three SIS layers of the different systems. Before Galileo is operational, the control of GNSSs is totally outside of European LEAs' hands. Also, communication systems are controlled via telecom operators. However, applying DSiP system enables LEA to act as a virtual telecom operator.

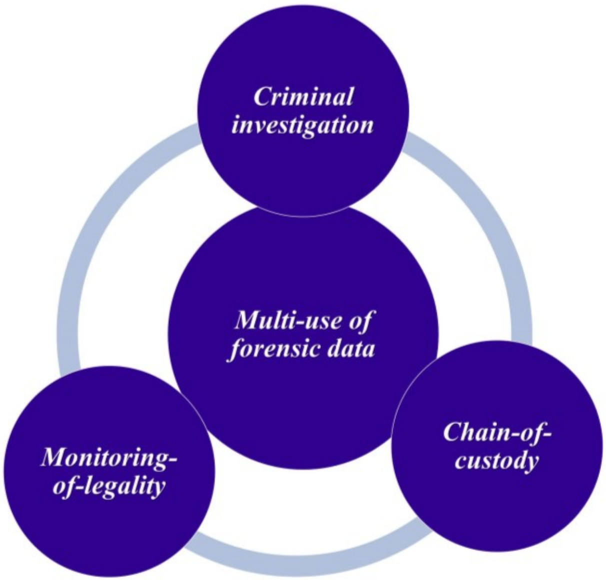

Fig. 4 Multi-use of law enforcement sensor data

Fig. 4 presents the principle of multi-use of law enforcement crime investigation and forensic sensor data that could be a part of the command, control and intelligence system of law enforcement. Integrating crime investigations, chain-of-custody and monitoring-of-legality into the same system of software-intensive systems gives many advantages. One of the key strands of integrated criminal prevention policy starts with multi-use of relevant information across sectors and borders, boosting the effectiveness and cost-efficiency of law enforcement activity. Currently however, EU and national law enforcement and other public authorities are responsible for different functionalities of criminal preventions. A political, cultural, legal and technical environment should be created for enabling information sharing and multi-use between existing and future criminal investigation, chain-on-custody and monitoring-of-legality systems. The system should ensure data security, especially information integrity and authenticity. It is also evident that the state authorities require some sort of institutionalized and standardized procedure in order to accept and trust the system. In addition, informal systems are needed to support the formal ones in order to survive the present social and political situation. According to the conventional wisdom, trust is critical in such multi-use systems and procedures.

4 Discussions

Organized crime is a real cross-border threat with the emergence of international warehouses of crime. For improving their evidence-gathering abilities, LEAs are constantly seeking new technological recording, retrieving and monitoring solutions that would facilitate their combat against criminal organizations. The criminals' counter-measure activities, such as electronic counter-surveillance, jamming and constant changes in behavior for preventing eavesdropping or physical surveillance are continuously increasing. The pressure to find new intelligent technologies, which are harder to detect, more strongly encrypted, longer-lasting, quicker to install and more adaptive, is emerging and is a high-priority task. The study of Rajamäki and Kämppi [20] provides an improved understanding of the structural characteristics and dynamic evolution of mobile communication challenges to cross-border satellite-based tracking operations carried out by LEAs. Especially machine-to-machine (M2M) communication in cross-border covert operations needs much more researched.

When preventing and investigating crimes, LEAs perform a variety of activities that affect the privacy of civilians. Video surveillance, audio surveillance, technical monitoring and tracking are among few to mention amongst many other activities. On various incidents, law enforcement is seeking more control rights, which increases concern amongst citizens and also the level of open debate increases steeply. Most of earlier studies were concentrated either to privacy issues from the citizens' point of view or on developing new forensic technologies for LEAs. Instead, Rajamäki et al. [19] provide an improved understanding about why transparency is a crucial factor for success in LEAs' technical surveillance. This paper also presents examples of current technological possibilities to create transparent and plausible monitoring for surveillance activities. Trust in LEAs has always been high in Finland. Nevertheless, there are a number of people in society who do not have any confidence in authorities, especially in police forces and their extended control. However, there is empirical and factual evidence pointing to that civilians are willing to give extended rights to authorities in extremely necessary situations. In such cases, people are more open and expecting authentic and timely information.

LEAs apply new technology in very effective ways. However, at worst, LEAs must perform many stages twice with the help of different technical tools [6]. When investigating the identity of criminals, LEAs may apply totally different technical tools than when gathering evidences for charge, because the data provided by their investigations may not be valid in court. For that reason, new tools that go beyond the state of the art are needed. Three organizational layers need attention: (1) LEA; the people that actually retrieve and store the information, (2) Prosecutors and their offices; how they get access to the information and, (3) Courts; the final destination of the retrieved information. Until now, the information gathering tools for LEAs have been engineered focusing only on the best way to retrieve information from the target. The attention paid to the legal, integrity and chain-of-custody requirements, and to social acceptance and monitoring-of-legality in connection with retrieving information has been inadequate, and guidance on the matters has existed only in manuals written by legal departments [6].

Much research exists in the field of public safety communications (PSC). The requirements of broadband data transmission are similar for public protection and disaster relief, critical infrastructure protection and military [21]. A fully decentralized PSC architecture concept that uses the Distributed Systems inter-communication Protocol (DSiP) can fulfill these requirements [14]. Here, network actors and elements are identified and authenticated by establishing physical connection. This concept also recommends group level user-authorization mechanism for each participating organization. Their respective users of command and control rooms were identified, authorized and authenticated to various data sources. The concept will be highly fault-tolerant in routine as well as crises operations. The software-based approach will be independent of heterogeneous data communication technologies, IP networks and telecommunication operator services. The solution will enable the building of an effective and lasting cyber-secure data network for multi-organizational environment. Being a fully decentralized concept, networks of individual member organizations will be virtually autonomous and unlikely to upset each other. That will allow smooth message and information exchange to enable interoperability.

5 Conclusions

For improving law enforcement, different functions are needed, such as crime investigation, chain-of-custody and monitoring-of-legality. All these systems and sub-systems have many stakeholders with different requirements. Modular approach (sensors, monitoring systems, communications) means that new technologies are easy to apply and new types of sensors could be easily included to the system. Integration of (1) investigation data, (2) digital evidence (=chain-of-custody requirements) and (3) monitoring-of-legality into the same system of SIS has multiple benefits for many stakeholders, and no duplicate work is needed. Table 1 summarizes the main stakeholder needs and benefits of new types of GNSS-sensors, (mobile) monitoring stations and their associated communication channels for LEA operation on the field taking into account the chain-of-custody requirements and the societal acceptance of these solutions.

TABLE I Stakeholders and their needs/benefits

Stakeholder	Needs/benefits
Citizens	Transparency of surveillance. Balance between surveillance and privacy. Efficient law enforcement; Value for money.
Targets	Fair, lawful, proportional and accountable surveillance.
LEAs	Better tools for recording, retrieving and monitoring of criminal activities. Better tools and processes for cross-border operations and cooperation.
Prosecutors	Chain-of- evidence requirements.
Court of law	Chain-of-custody requirements.
Legal officers	Tools for monitoring-of-legality.
Legislators	Commonly agreed balance level between surveillance and privacy. Identification of the legal barriers to the EU-wide deployment of the system of interest.
Manufacturers and private Service Providers	More business opportunities by, e.g., less fragmented markets and international standards.
Public Service Providers	More users of their services providing business continuity.
Funding Agency	An efficient return on investment ratio.

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

References:

[1] European Commission, "FCT-05-2014," .

[2] A. Hevner and S. Chatterjee, Design Science Research in Information Systems. Springer, 2010.

[3] H. Simon, The Science of the Artificial. Cambridge: MIT Press, 1978.

[4] J. L. Fiadeiro, "Designing for software's social complexity," IEEE Computer, vol. 40, pp. 34-39, 2007.

[5] J. Rajamäki and J. Viitanen, "Law enforcement authorities' special requirements for GNSS," in Proceedings of the 6th GNSS Vulnerabilities and Solutions Conference, University of Rijeka, Rijeka, Croatia, 2013, pp. 135-147.

[6] J. Rajamaki and J. Knuuttila, "Law enforcement authorities' legal digital evidence gathering: Legal, integrity and chain-of-custody requirement," in Intelligence and Security Informatics Conference (EISIC), 2013 European, 2013, pp. 198-203.

[7] BBC News Story, How we are being watched? Feb. 2006.

[8] J. Rajamäki, R. Pirinen and J. Knuuttila, Eds., SATERISK - Risks of Satellite-Based Tracking: Sample of Evidence Series. Vantaa: Laurea-University of Applied Sciences, Leppävaara Unit, 2012.

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

[10] ABI Research, "High Precision GNSS Market Set to Increase Almost 100% by 2016," ABI Research, 2011/09/29, 2011.

[11] P. J. O'Brien and J. M. Griffin, Global Positioning System Systems Engineering Case Study. Hobson Way: Wright-Patterson AFB, OH: Air Force Center for Systems Engineering (AF CSE), Air Force Institute of Technology (AFIT), 2007.

[12] J. Rajamäki, P. Rathod and P. Kämppi, "A new redundant tracking system for emergency response," in Intelligence and Security

Informatics Conference (EISIC), 2013 European, 2013, pp. 218-218.

[13] R. Akella, H. Tang and B. M. McMillin, "Analysis of information flow security in cyber–physical systems," International Journal of Critical Infrastructure Protection, vol. 3, pp. 157-173, 2010.

[14] J. Rajamaki, P. Rathod and J. Holmstrom, "Decentralized fully redundant cyber secure governmental communications concept," in Intelligence and Security Informatics Conference (EISIC), 2013 European, 2013, pp. 176-181.

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

[16] J. Holmström, J. Rajamäki and T. Hult, "The future solution and technologies of public safety communications–DSiP traffic engineering solution for secure multichannel communication," International Journal of Communication, pp. 155-122, 2011.

[17] B. Srimoolanathan. "World security market outlook," Presented at Tekes Safety and Security Programme's Annual Semina. 2012, [online]. Available: https://tapahtumat.tekes.fi/uploads/3ef8185/balaji_frost_sullivan_safety_seminar-4590.pdf.

[18] I. Tikanmäki, J. Rajamäki and R. Pirinen, Eds., Mobile Object Bus Interaction - Designing Future Emergency Vehicles. Vantaa: Laurea, 2014.

[19] J. Rajamaki, J. Tervahartiala, S. Tervola, S. Johansson, L. Ovaska and P. Rathod, "How transparency improves the control of law enforcement authorities' activities?" in Intelligence and Security Informatics Conference (EISIC), 2012 European, 2012, pp. 14-21.

[20] J. Rajamäki and P. Kämppi, "Mobile communications challenges to cross-border tracking operations carried out by law enforcement authorities," in Information Networking (ICOIN), 2013 International Conference On, 2013, pp. 560-565.

[21] G. Lapierre, "Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU?" 2011.