Towards Resilient Mission Critical Broadband Data Communications for Public Protection and Disaster Relief

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

JOHN HOLMSTRÖM
Ajeco Oy
Arinatie 10, FI-00370 Helsinki,
FINLAND
john.holmstrom@ajeco.fi
http://www.ajeco.fi/

Abstract: - Mobile broadband applications can greatly improve the effectiveness of public protection and disaster relief (PPDR) operations, however, most PPDR actors do not have these capabilities. This design science research develops a multichannel solution for critical data broadband communications based on Distributed Systems intercommunication Protocol (DSiP) software, and evaluates it in an operational environment. We also propose resilience metrics for public safety communications (PSC) and analyze how our solution fulfils their objectives, and what should be developed further. Based on our findings, we have created additions to the knowledge base with regard to multichannel communications and PSC. However, much more research and development work is needed for making mission critical broadband data communications more resilient.

Key-Words: - Resilience, Mission critical, Public safety communications, Public safety mobile broadband, Distributed Systems intercommunication Protocol, Multichannel communications.

1 Introduction

Today's smartphones have countless applications (e-mail, maps, navigation, parking, entertainment, etc.) that serve the users for better life, work and free time. However, public protection and disaster relief (PPDR) actors would have worse or, in some cases, none of these capabilities. Despite the almost endless debates about public safety communications (PSC) network infrastructure demands, it is clear that a well-functioning broadband access would be an important addition to their work, and it would be really important to help PPDR actors to use modern applications. There are vast amount of data available in open or protected data bases that could provide for excellent help. Also very simple modern applications, such as efficient office programs would be very useful whenever the officers are mobile. Also the modern command and control (C&C) applications would benefit greatly from broadband. The larger data capacities would allow for up to date maps, more interactive and quicker updating situational pictures and better and broader sharing of data between the mobile units.

For first responders, the availability of the online information is of uttermost importance. The current PSC networks, such as TETRA, Tetrapol or P25 are built to provide for high availability voice in critical situations, but also only for small amounts of data. If one tries to fetch information from criminal records, latest building drawings in case of fire, or send cardio information to a doctor in hospital, the connectivity is crucial, and one certainly cannot wait minutes for the data to be delivered which is the case when using TETRA or P25. When talking about criticality, the C&C application becomes a focal point. With an efficient C&C application one can share information about other units' location, target drawings and other various case specific information. The more instantaneous the data is, the better security it provides for the officers on the case. We have seen live situational pictures being shared from criminal sites in order to enhance co-operation and to minimize the inefficient use of mobile voice terminals. But can you rely on pictures and other important data getting transmitted when needed?

The human body is inherently resilient in its ability to persevere through infections or trauma, but our society's critical infrastructure lacks the same degree of resilience, typically losing essential functionality following adverse events [1]. Resilient systems are able to minimize the negative impacts of adverse events on societies and sustain or even improve their functionality by adapting to and learning from fundamental changes caused by those events [1]. In PSC, one network is never enough for resilience, no matter if it is a commercial or even a

dedicated network, because all networks have occasional service break downs, larger or smaller scale. It is not within any foreseen organization's or nations capabilities to build resilience required just for one network. However, a common mistake PPDR agencies make is to rely solemnly on one commercial broadband network. It almost seems like all concentration with the development is on the applications. Too often the connectivity issues are handled by a short notion "… oh and we'll use the broadband of the number one commercial operator, with a dongle or similar." By multichannel communications, utilizing hybrid dedicated and commercial networks or a combination of commercial networks brings the availability to the accepted level for PPDR use. It is then always a matter of resilience on what the approach selected in each region or country would be.

This paper presents a software solution named Distributed Systems intercommunication Protocol – DSiP that has been developed aimed at mitigating problems in multichannel communication and targeted at increasing resilience in computer networks. The solution is evaluated in real contexts in PSC and critical infrastructure protections domains.

The structure of remainder of paper: Section 2 gives a literature review with regard to resilient cyber-physical systems (CPS) and critical communications. Section 3 presents the design science research methodology and how it is applied in this study. Section 4 describes the developed solution, which is evaluated in section 5. Section 6 discusses about the usefulness of the solution as well as what new knowledge the study contributes to the body of understanding about multichannel communications and PSC. Finally, the conclusions are presented in section 7.

2 Literature Review

2.1 Resilient Cyber-Physical Systems

Modern societies are highly dependent on different critical cyber-physical systems (CPS). The growth of software (= cyber) layer, in size and percentage of the overall system is a future trend [2]. Our society's critical CPS — cyber, energy, water, transportation and communication — lacks of resilience, typically losing essential functionality following adverse events [1]. According to Linkov et al. [1], resilience, as a property of a system, must transition from just a buzzword to an operational paradigm for system management, especially under future climate change. Identifying the need for system resilience requires defining the system. Revolutionary advances in hardware, networking, information and human interface technologies require new ways of thinking about how CPS are conceptualized, built and evaluated [2]. Currently, a development of a design theory (DT) for resilient CPS is on a way so that communities developing and operating different information and security technologies can share knowledge and best practices using a common frame of reference [3].

The National Academy of Sciences identifies four event management cycles that a system needs to maintain to be resilient [4]: 1) Plan/Prepare: Lay the foundation to keep services available and assets functioning during a disruptive event (malfunction or attack). 2) Absorb: Maintain most critical asset function and service availability while repelling or isolating the disruption. 3) Recover: Restore all asset function and service availability to their pre-event functionality. 4) Adapt: Using knowledge from the event, alter protocol, configuration of the system, personnel training, or other aspects to become more resilient. The Network-Centric Warfare (NCW) doctrine identifies four domains that create shared situational awareness and inform decentralized decision-making [5]: 1) Physical: Physical resources and the capabilities and the design of those resources. 2) Information: Information and information development about the physical domain. 3) Cognitive: Use of the information and physical domains to make decisions. 4) Social: Organization structure and communication for making cognitive decisions. Linkov et al. [6] combined the event management cycles and NCW domains to create resilience metrics for cyber systems. Their approach integrates multiple domains of resilience and system response to threats through integrated resilience metrics; however, study of systems as multi-domain networks is relatively uncommon. Links across domains are likely to affect the network's resiliency and should be assessed using network science tools [7].

According to DT for resilient CPS [3], resilience in cyber domain means that a system or infrastructure is able to adapt to changing conditions based on run-time situational awareness and a priori risk analysis. Situational awareness involves being aware of what is happening around one to understand how information, events, and one's own actions affect the goals and objectives, both now and in the near future. The most important enablers of situational awareness are observations, analysis, visualization, and cyber-policy of the government. Security technologies include all technical means towards cyber security, such as secure system architectures, protocols and

implementation, as well as tools and platforms for secure system development and deployment. Security management and governance covers the human, organizational and cognitive aspects of information security. Its focus areas include: 1) Security policy development and implementation, and 2) Information security investment, incentives, and trade-offs. Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization's information assets that do preserve [3].

2.2 Critical Communications

2.2.1 Mission and Safety Critical

The Forum for Public Safety Communications Europe (http://www.psc-europe.eu) defines mission and safety critical as follows:

Mission critical: "A function whose failure leads to catastrophic degradation of service that places public order or public safety and security at immediate risk. These systems are paramount to the operation of a nation's public safety and critical infrastructure services and are therefore specified to have particular and adequate inbuilt functionality, availability, security and interoperability."

Safety-critical decision: "A decision that results in either lives being saved or serious injury being avoided."

PSC must be simple to use, reliable, interoperable, secure, cost-effective, and ubiquitous [8]. Critical data transmission over TETRA or Tetrapol is rather slow and will not satisfy future needs. Wideband TETRA Enhanced Data Service (TEDS) is an effort towards improved data services [9], but TEDS falls short of current and future needs. The long term goal is to conduct critical voice and data communications using broadband technology, but a reasonable time window for the transition from TETRA/Tetrapol to broadband begins with the availability of critical voice services over Long Term Evolution (LTE) early next decade and ends when the current TETRA network reaches its end of life — somewhere in the first half of the 2030s [10]. To design resilient LTE networks, moving from a highly centralized to a distributed system is proposed [11]. However, one network is never enough for resilience.

2.2.2 Dedicated Networks

Dedicated networks are built for a specific purpose – other than for public use, for example PSC, telecommunication networks for railways and power utilities, emergency telephone systems along the roads, and telecom systems for oil, gas and electrical power utility companies. In the 1980s and 1990s, most dedicated networks were built using the same technology what was used in the commercial networks. The exceptions were the railways – for which GSM-R (GSM-Railway) was defined as a standard - and the PSC networks, for which specific technologies were developed, TETRA and TETRAPOL in Europe as well as APCO P25 in North America [12]. These regional or even countrywide implementations have been paid with the taxpayers' money and the argumentation for the need has been along the lines like "this is the only mission critical solution you can trust your life on". However, no solution is 100% sure and despite not much communicated, the known fact is that the existing digital PSC networks are far from being perfect. A good question today is if really a dedicated network is even needed for the voice services? There exist novel push to talk possibilities, various mobile virtual network operator (MVNO) approaches and such that could even replace the existing networks. If we select dedicated PSC networks, we should consider the cost versus benefit. On the other hand, the current paradigm for PSC provisioning based on dedicated technologies, dedicated networks, and dedicated spectrum no longer constitutes the main approach for introducing PPDR mobile broadband and, hence, new paradigms and innovative solutions are needed [13].

2.2.3 Hybrid Network

A combination of TETRA and LTE can be considered as a medium term migration strategy for all critical communications users [14]. According to the Finnish study [10], the most economical solution to establish a communications network for critical users is based on a hybrid of dedicated network(s) in incident-rich areas where the population is located and to rely on commercial networks in the scarcely populated areas, provided that there is coverage available. However, to rely solemnly on one commercial broadband network and technology is never enough. Especially in critical situations like human stampede or natural disasters, networks could break down while remaining physically intact [15]. Resent research [16] suggests that multichannel communications, utilizing hybrid dedicated and commercial networks or a combination of commercial networks realized by different technologies (e.g. LTE, satellite technology) brings the availability to the accepted level for PPDR use. There is a global demand for safe and secure multichannel communications, and it is expanding day by day.

3 Method

Design Science Research (DSR) is a suitable research paradigm for developing solutions, since in DSR a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence, where the designed artifacts are both useful and fundamental in understanding that problem [2]. Moreover, these artifacts are demonstrated to improve manager's capability to "change existing situations into preferred ones" [17].

Consequently, we have used DSR, by following its methodology [18], which comprises the following activities: 1) Problem identification and motivation; 2) Solution objectives definition; 3) Design and development; 4) Demonstration; 5) Evaluation and 6) Communication.

DSR foresees several ways to evaluate the artifacts developed [19] from which we have chosen case studies in the field. Our case studies' primary goal is to determine how the artifact behaves in a comprehensive manner and in a real environment [20] since, research that is based on DSR cannot only focus on the development of the artifact and should demonstrate that the artifact can be effectively used to solve real problems [21].

4 Artifact Description

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 [22]. Efficient decision processes must be adopted to reach the relevant QoS. The success of such an approach relies on a profound understanding of applied technologies and their performance described by their performance indicators. A DSiP router's QoS option sets the desired order of the network access by desired cost-of-service (CoS) value [23].

4.1 DSiP

The Distributed Systems intercommunication Protocol (DSiP) forms multiple simultaneous communication channels between network peers: if one communication channel is down, other channels will continue operating. DSiP makes communication reliable and unbreakable by using several physical communication methods in parallel when needed.

Software applications, equipment and devices can communicate using the DSiP-software protocol that appears to them as a single unbreakable data channel. Satellite, TETRA, mobile data (e.g. 2G/3G/4G), computer networks and radio-modems and other technologies may be used simultaneously and in parallel.

DSiP manages the selection of communication channels and overcomes link establishment issues. In addition to maintaining multiple communication links DSiP also solves incompatibility issues via protocol translation barriers being an invisible layer for end-users' applications, hardware and software. It provides scalable modularity, data integrity, security, and versatility to data communications systems of many sizes. The DSiP software uses both IP and non-IP based communication links when required. DSiP is capable of converting classical polled systems into event-driven systems. The last mentioned feature improves response time and speed – a feature sought after in for example Power Grid and Smart Grid applications. DSiP may also compress data, which is useful with low-capacity communication channels.

Virtual Private Networks (VPN) can be tunneled through the DSiP communication system. This feature makes it possible to maintain constant communication without re-authentication of VPN-sessions during channel switching when a communication channel is at fault. The DSiP-software system brings many significant benefits and useful functions. The DSiP system (1) increases reliability and security; (2) is resistant to network Denial of Service (DoS) and Man in the Middle (MITM) attacks; (3) decreases the risk of virus- and malware infusions via the communication channels; (4) results in less system downtime and lower maintenance requirements; (5) contains authenticated, peer-verified and encrypted communication; (6) allows combination and parallel use of TETRA- and mobile data communication; (7) has the capability of interfacing with many different kinds of hardware and software like radar, Automatic Identification System (AIS), Radio Direction Finders, and Closed-circuit television (CCTV) equipment; (8) has native interfaces to various protocols used in electrical utility installations such as DNP3, IEC60870-5-101/104, Modbus, National Marine Electronics Association (NMEA) and other protocols and (9) includes network monitoring and management tools improving overall system performance.

Mobile multichannel communication improves communication reliability and quality, for example in PPDR applications. Police cars, ambulances and fire engines benefit from uninterruptable secure communication. DSiP provides a uniform, reliable and maintainable communications services platform

capable of withstanding time because it is not tied to any existing modem or data transfer technology. The system is not dependent on any particular telecom operator's services or communications protocols.

4.2 Quality of Service and Cyber-secure Communications

IP traffic and its packets have methods for controlling priority and quality only in the IPv4 protocol suite. The IP QoS, however, has not standardized implementations among network operators. Customers using DSiP have enhanced controlling possibilities for data flow and traffic, including (1) control priorities—important information is routed first, less important information later; (2) control over network timeouts—no undetermined delays or waits; (3) control of the usage of communication and bandwidth—DSiP always "knows" the condition of all routes; (4) better control over maintenance and configuration; (5) the DSiP telemetry system with its built-in congestion control and (6) routing services based on cost- and service factors enabling certain, less important traffic to be filtered, such as the used low-capacity communication.

The decentralized architecture based on DSiP is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent of different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables the building of a practical and timeless cyber-secure data networks for multi-organizational environments, which, being fully decentralized, is hard to injure.

A communication solution realized using the DSiP-software solution may be used by several different organizations being virtually fully separated, but if required, being able to exchange messages and other information making the organizational information used in interoperation.

4.3 Key elements and functionalities of DSiP

As mentioned earlier, DSiP is protocol solution entirely based on software. There are fundamentally two types of software elements in the solution: Software based virtual DSiP-routers and network peers i.e. DSiP-nodes. Figure 3 depicts the blueprint of the solution. The nodes constitute interface points (peers) with the DSiP routing solution, and the DSiP-routers drive traffic engineering and transport in the network. The virtual DSiP-routers establish multiple authenticated and encrypted, sometimes parallel, connections according to configuration parameters, between each other. The nodes establish multiple simultaneous connections to one or more routers in the system. All connections are strongly encrypted and peer-verified based upon usage of certificates which can be either public or private. All elements in the DSiP-routing solution are known. As routers may use multiple parallel connections between each other and as nodes may make multiple parallel connections between themselves and one or more routers, the solution results in a true mesh-like structure between the network peers (nodes).

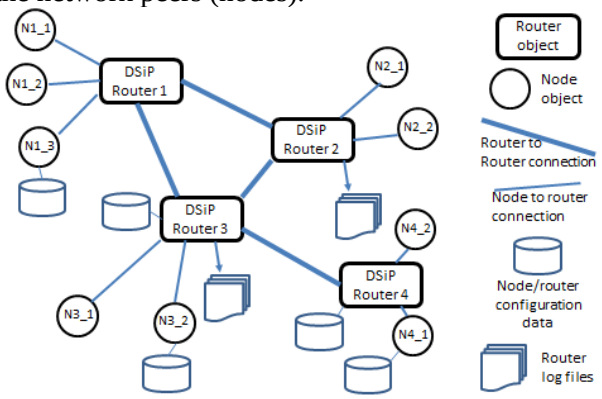

Fig. 1. Blueprint of DSiP network solution

The virtual DSiP-routers in the routing network are typically distributed into different physical locations. The nodes are typically located at the "ending points" in a network such as, but not limited to, for example, emergency service vehicles, control rooms, computers and laptops or other mobile devices. The connection establishment is always constructed from the node towards the router element and one router to another router in a preconfigured manner.

The system may feature a third element, called configuration server software, from where nodes may read new configuration data should the underlying physical transport layer request change or configurations need to be done.

The nodes and routers maintain multiple parallel physical connections between each element in the DSiP routing solution. As the node is responsible for maintaining connectivity to the virtual routers, it removes the complex burden of link establishment and routing from the external equipment and software that use the system. Consider, for example, a vehicle computer in an emergency service vehicle. This computer either contains a DSiP-node that uses multiple wireless modems, or it connects to a vehicle router-hardware containing a DSiP-node and multiple modems. The DSiP-node is performing the tunneling of the user applications' IP-traffic from the vehicle to the control room and vice versa, thus mitigating complex routing issues in-between network peers. The DSiP solution is capable of transparently maintaining the connections and

communications between users' systems or applications or hardware without this functionality having been programmed into the applications—DSiP is thus fully transparent to its users. For example, a user may run VPN client software in his laptop and create an uninterruptable VPN-session by communicating through the DSiP-routing solution.

The nature of the VPN demands that it must usually establish its connections over a single physical communication line. If this line has a problem or breaks up, the user must re-authenticate his or her VPN session over another physical media. When DSiP is used, the user can use his or her VPN client or server to establish a VPN session over multiple physical connections—should one or more have problems, the VPN session remains intact as the DSiP tunnels the session through itself. This feature is of utmost importance in critical applications.

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

The transport layer in the DSiP routing solution may use IP networks. However, DSiP is not limited to the use of IP—it can use proprietary, non-IP networks as well. This feature adds to the security and robustness of a DSiP routing solution. The DSiP can interconnect peers in an IP network by using non-IP connections. In addition to the aforementioned, DSiP is a tunneling protocol. It can interconnect private typically not operator-routable networks having a 10- or 192-based IP address ranges, through regular tele-operator service networks.

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

All addressing in a DSiP-network solution is based upon individual node-, organization- and routing-cloud-numbers. The ending points in DSiP routing solutions do not need to "know" the IP addresses or locations of their counterparts. The addressing scheme, in addition to a concept called DSiP-translation barrier, makes it possible to interconnect users from different organizations with different IT-policies because the DSiP may constitute a service-providing network and not just a "pipe" or "tunnel" from one network to another. The translation barrier functionality residing in the DSiP-nodes may be used for fetching data from core networks and filtering access to the core in much the same way as HTML and PHP are used in browsing applications. A typical multi-user, multi-policy DSiP routing solution may look like the one in Figure 2.

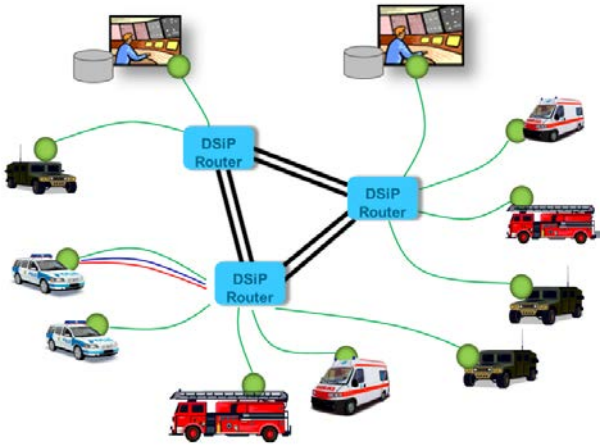

Fig. 2. Multi-user DSiP network solution

Maintaining an IP network is a tedious and often difficult task requiring thorough understanding of IP-firewalls, manageable-routers and switches. It can be highly risky to parameterize a firewall as a faulty firewall rule may endanger a complete network. The DSiP solution mitigates this task. The IP network maintainer or creator may set up his or her network and tune firewalls and routers locking the tested/hardened IP-routing. Then the DSiP can be used as a logical traffic-engineering layer on top of the robust IP-network. Features in DSiP such as the implementation of RADIUS 802.1X and LDAP-functionalities may provide additional security measures for a network maintainer. DSiP contains interfaces for organizational LDAP- and RADIUS-servers.

Different actors needing secure and reliable communication may have different (performance) needs. The nature of secure and reliable critical communication depends on the serving actors. Consider for example a scenario where an electricity transmission system operator detects a problem in the main power grid, and the load and power plant must

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

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

5 Evaluation

In September 2012, Louhi Security Oy security-audited the DSiP solution, giving it high credentials. The purpose of the audit was to locate and identify potential cyber-risks in the DSiP system. The audit was conducted based on methods from the OSSTMM (Open Source Security Testing Methodology). Both commercial and open source tools were used in the audit. According to the audit, DSiP system provides a high level of reliability and security for applications demanding uninterruptable communication and extended usability.

DSiP is already in pivotal use in some PPDR and critical infrastructure protection applications, for example for controlling and operating high and mid-voltage power grids. Unfortunately, the evaluation data from these mission and safety critical solutions are classified.

DSiP has been evaluated for example in the Celtic-Plus project called MACICO - 'Multi-Agency Cooperation in Cross-Border Operations' project developed a concept for interworking of security organizations in their daily activity, dealing with cooperation of security organizations that do not use (in their day-to-day job) the same radio network, but in some missions could take benefit of a share of their respective infrastructure.

As a part of the MACICO project, a proof-of-concept study applies DSiP in combining multiple telecommunication channels in Supervisory Control and Data Acquisition (SCADA) systems [24]. SCADA systems are used for controlling power stations and protecting power distribution. Therefore, secure data transfer between the control center and power stations is critical. Current telecommunication networks used for the SCADA do not provide the capacity required for real time video streaming, and standard Internet connection does not provide the required reliability and security, but DSiP combines all these telecommunications resources into a single system [24]. Another study discusses using DSiP as a highly redundant and secure data PSC, addresses interoperability and other issues both between different services and different systems used by the same service, and describes what kind of benefits DSiP solution can offer [25]. A master's thesis based on theoretical evaluation compares DSiP to other solutions available [26]. DSiP has been implemented in operative systems for SCADA-command and control and also in coastal surveillance in Finland since 2007 and France, however the nature of these application are classified. Power Grid implementations have been presented in Proof-of-Concept applications in Hong Kong and the Philippines.

The DSiP based solution was in use at the Viksu 2014 camp. Viksu 2014 was an international camp for junior firefighters that was held from June 29 to July 5, 2014 in Pori, Finland. Over 2,800 attendees from volunteer fire brigades participated in the camp. During the camp, a scenario exercise related to communication and performance in exceptional circumstances was held. The objective of the scenario exercises was to examine practices in crisis situations and seek for ways to make use of modern technology solutions in improving performance efficiency. The technological solutions used in the scenario exercises were using a temporary TETRA network and TETRA phones, satellite connection and an Android application in helping to gather situational awareness information.

The original plan was to build a temporary, local TETRA network for the camp organization and to connect it with the Government's Official Radio Network in Finland (VIRVE) using an Inter-System Interface (ISI) that provides a terminal with the

possibility to roam in another TETRA network. For security reasons and due to lack of time, connecting the local TETRA network of Viksu 2014 to the VIRVE network was not possible, and those networks were used separately. Therefore, the main interoperability problems in voice communications were related to people and organizations, not technology, and thus the objectives of the demonstration were steered more towards the communicative aspects. This meant that data-based technological solutions to be used at the demonstration became more important.

The Eye Solutions system for visual surveillance was used at the camp in order to get situational awareness information. The system was gathering live audio and video feeds from the field to the camp security management using the cameras and microphones of contemporary smartphones. The system consists of a PC that is used to administrate the system, some screens to monitor the situation, Android smartphones to gather the live information from the field, and Ajeco's multichannel 4Com router implementing the DSiP protocol as well as software DSiP-clients in the Android handsets. The system administration software is browser and java based and was run local on a PC. The smartphones can be remotely controlled by the administration software. The situational awareness system of Eye Solutions and the reliability of communication through the DSiP system were tested in the camp by Ajeco personnel and Laurea University of Applied Sciences' students. Six students from Laurea UAS collected data for their theses during the camp by planning and executing the scenario exercises, observing camp organizations' communication and performance, comparing the outcomes to safety and security plans, and interviewing the personnel. The demonstration showed that in addition to providing multichannel communication, non-reputability, encryption, and security, the DSiP architecture provides means for solving complex compatibility issues providing interface and process ontology and methods [27].

6 Discussion

6.1 Multichannel Communications

The inarguably most common method or protocol for data communication today is the IP-protocol developed in the mid 70's. The IP-protocol and more precisely its TCP-transport layer however lack the capability for maintaining a socket connection over several physical communication channels simultaneously. The TCP-transport layer cannot be used for simultaneous IP-socket connections using multiple physical communication channels between a source and destination without the help of additional software.

There are several aspects depending on application requirements and needs when considering multichannel communication. For example; should the multichannel communications solution be optimized for maximized data transfer capacity, should it be optimized for minimum latency or should it be optimized for maximized availability? It may be extremely difficult to combine the best of all features into to a single universal solution due to the large spectrum of use-cases. Consider for example the type of information that needs to be transmitted. Some information is atomic (e.g., a GPS-location) and some information is a continuous stream (e.g., a live video feed) – the type of information to be transmitted will affect how the multichannel communications solution should handle the data transfer. In simple terms; all data in IP-networks is based upon transmitted datagram packets. Some applications require that the sequence of the transmitted datagrams is known and maintained whereas other applications are not sensitive to which order the separate datagrams arrive. A video-application receiving a stream of datagrams requires that the datagrams arrives in the same sequence as they were transmitted, or at least, the datagram sequence numbering must be known. However, a GPS-location is an atomic piece of information that fits into a single datagram, hence there might not be any requirement for knowing the sequence of multiple datagrams of this type of information.

A multichannel communications system may consist of multiple communication paths of various types. For example, mobile data, WLAN-networks and satellite-links may be utilized. All the aforementioned communication methods have specific characteristics in terms of bandwidth capacity, latency and cost in terms of monetary units. Mobile data is general term which is not defining any specific metrics regarding capacity, latency or cost. One can say that mobile data and mobile data cannot be compared at all regarding the metrics. For example, a telecom's operator may offer two LTE mobile data communications subscriptions that have very different characteristics in terms of latency and capacity.

Technical differences in communication channels affect the way they should be used in combinatorial applications e.g. multichannel communication applications. The expression "parallel use" of

communication channels may mean different things in different implementations.

People can use parallel communications paths simultaneously if they want; they can collect and integrate information coming from different sources to a certain extent. However, computers face difficulties in multichannel communication because the IP protocol used for data transfer cannot bind a socket over two or more physical connections simultaneously. This is one of the most serious shortcomings in multichannel communication: IP is not 'good' at multi-channeling. There are several attempts at solving the computers multichannel problems, this paper will not discuss these in detail, but it is important to mention for example MPTCP – a multipath TCP stack (see http://www.multipath-tcp.org/) and certain multichannel VPN solutions intended for maintaining multiple simultaneous connections between computers in a network. The word 'resilience' in the context of uninterruptable communication should refer to the ability of maintaining working communication paths between computers in a network under all circumstances including cyber-attacks and technical problems – a mere addition of multiple communication paths or VPN-tunnels between computers do not solve the overall problem. A resilient computer network should have no single points of failure.

Creating a multichannel communication solution utilizing Virtual Private Network (VPN) techniques solves some problems of a resilient communications network requirement, while on the other hand, it ties the solution to the VPN system. The real challenge for us is to overcome the fact that the VPN solution covers only a fraction of the total need.

The IP protocol has some control of priority and quality of service (QoS) (QoS is implemented only in the IPv4 protocol, IPv6 has no QoS). However, (network) services should adjust to the physical transfer capacity. For that reason, low capacity lines can transfer only high priority data.

Centralized communications solutions may be vulnerable to many threats, which may include denial-of-service (DoS) and man-in-the-middle (MITM) attacks, system failures, repudiation, spoofing and tampering. Therefore, decentralized modular communication and information management systems should be used; if one part goes down, other part works. Also, turning to the services of a single (network) operator is a risk. Utilizing parallel communication channels provided by several (network) operators minimizes risks and maximizes reliability ensuring constant connectivity and communication.

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

A 'good' public protection and disaster relief (PPDR) data communications solution should contain and provide at least the following topics: 1) Handling of dynamically changing IP-addresses as in the Mobile-IP solution, 2) Handling of peer-to-peer security as in IPsec, 3) Configurable and maintainable routing as in OSPF and MPLS, 4) Multichannel communications capabilities, 5) Network congestion control, 6) Non-reputability, 7) Interoperability, 8) Authentication with strong encryption, 9) Centralized key-management and distribution, 10), and 11) Access control mechanisms.

To summarize; there exists partial solutions addressing separate elements in a working multichannel system. However, only the DSiP-solution contains most of the needed elements in a single maintainable packet. For example, Mobile-IP handles the problem of dynamically changing IP-addresses in a mobile system, IPsec may be handled by a VPN solution and OSPF and MPLS are separate technologies. Matters like non-reputability, congestion- and priority control remain to be resolved by other means.

6.2 Resilience

According to Linkov et al. [1], "although the number of climatic extremes may intensify or become more frequent, there is currently no scientific method available to precisely predict the long-term evolution and spatial distribution of tropical cyclones, atmospheric blockages and extra-tropical storm surges; nor are the impacts on society's infrastructure in any way quantified. In the face of these unknowns, building resilience becomes the optimal course of action for large complex systems [1]." Several frameworks for studying and developing resilient infrastructures exist (e.g., [28]), but they focus mostly on theoretical aspects.

Mobile communication networks are critical examples of large complex systems/infrastructures for today's society and contribute to its security and safety. In critical situations, mobile communication infrastructure is particularly vulnerable to threats linked to a wide range of security issues and failures caused by natural hazards as well as overload and blocking. That is contrary to the desired behavior in catastrophe scenarios, as the infrastructure is meant to provide emergency call functionality and communication for the rescue teams [15]. While traditional usage scenarios even for major events are well researched, there is a lack of knowledge on how to make mobile networks more resilient to unpredictable load in disaster events [15].

Table 1 adapting the resilience metrics of Linkov et al. [6], presents our findings (requirements) how mobile PSC networks can be made more resilient. Unfortunately, our resilience matrix is not yet a complete one.

DSiP being a software solutions, increases the cyber layer of the PSC system making cyber security issues even more important. Table 2 summarizes how DSiP fulfils or fails the requirements presented in Table 1.

7 Conclusions

Climate change is likely to pose particular threats to critical infrastructures, for example floods, heavy storms, increased strains on materials and equipment, higher peak electricity and communications loads, transport, electricity and communications disruptions, and increased need for emergency management. Furthermore, changes in how Power Grids operate with implementations towards Smart Grids, all increase the need for secure and uninterrupted communication. Thirdly, Internet-of-Things (IoT) increase the need for secure communication immensely while at the same time Cyber Threats are simultaneously increasing. Public safety communications is an example of the critical cyber-physical systems vital for our society. The current trend is that the 'cyber layer' of all CPS is increasing, and this is true also with PSC that is increasingly vulnerable to cyber-attacks that can cause damages disproportionate to the sophistication

Table 1. Resilience matrix of PSC

	Plan and prepare for	**Absorb**	**Recover from**	**Adapt to**
Physical	Software, configuration data and communication certificates should be encrypted and locked to each individual physical device. Communication should be enabled only after user identification. Both hardware and users should be identified and authenticated.	Control room equipment and power feed should be redundant. Network peer devices should be kept available at distributed locations. Configuration of spare units and software should be automated. Satellite and radio communication should be considered in case of trunk network failures,	Investigate and repair malfunctioning controls or sensors. Assess service/asset damage. Assess distance to functional recovery. Safely dispose of irreparable assets.	Review asset and service configuration in response to recent event. Phase out obsolete assets and introduce new assets.
Information	Configuration, authentication and critical parameter data should be held encrypted, supervised and separate from actual routing functionality.	Configuration, authentication and critical parameter data should be held encrypted, supervised and separate from actual routing functionality. Log- and systems signals should be studied. NOC and SOC should be activated.	Log- and systems signals should be studied. NOC and SOC operating parameters may need adjusting.	Multichannel network operating parameters may need changes after attacks. Network topology changes might need adjustments. IP-address ranges may need adjustments.
Cognitive	Network Operations Center (NOC) and Security Operations Center (SOC) should learn and "know" the behavior of use under normal conditions.	The communication system should adapt itself to the new situation when under attack. Routing should be automatically redirected to circumvent technical clogging in the networks.	Review critical points of physical and information failure in order to make informed decisions.	Review management response and decision making processes. Determine motive of event (attack).
Social	User identification is equally important as hardware identification. Authorization mechanisms for users should be planned.	User restrictions may apply. Service restrictions may apply. Communications resources may decrease, therefore network and user services must be prioritized.	Follow resilience communications plan. Determine liability for the organization.	Evaluate employees response to event in order to determine preparedness and communications effectiveness.

Table 2. DSiP against resilience metrics

	Plan and prepare for	**Absorb**	**Recover from**	**Adapt to**
Physical	Software, configuration data and communication certificates are encrypted and locked to each individual physical device. Communication is enabled only after user identification. Both hardware and users are identified and authenticated.	Power feed, spare parts etc. are a matter of agreement. The DSiP Configuration Server mitigates installation of "cold" spare parts.	The DSiP-system analyzes the quality of used and unused links by measuring metrics such as capacity and latency. The system will revert to default after the problems have disappeared.	Review asset and service configuration in response to recent event. Phase out obsolete assets and introduce new assets.
Infor-mation	Configuration, authentication and critical parameter data are encrypted, supervised and separate from actual routing functionality.	Configuration, authentication and critical parameter is held encrypted, supervised and separate from actual routing functionality. The system maintains logs and real time monitoring of the network.	Log- and systems signals should be studied. NOC and SOC operating parameters may need adjusting.	Multichannel network operating parameters may need changes after attacks. Network topology changes might need adjustments. IP-address ranges may need adjustments. This is done via the DSiP systems configuration servers and tools.
Cognitive	DSiP-implementations may contain interfaces to Network Operations Center (NOC) and Security Operations Center (SOC).	The communication system should adapt itself to the new situation when under attack. Routing is automatic and redirected to circumvent technical clogging in the networks.	Review critical points of physical and information failure in order to make informed decisions.	Review management response and decision making processes. Determine motive of event (attack).
Social	User and hardware identification are realized. Authorization mechanisms exist	User restrictions may apply. Service restrictions may apply. Communications resources may decrease, therefore network and user services must be prioritized.	Follow resilience communications plan. Determine liability for the organization.	Evaluate employees response to event in order to determine preparedness and communications effectiveness.

and cost to launch the attack. It is clear that, in order to reduce the risk and impact of these threats and to increase the safety and wellbeing of citizens, PSC must become more resilient against physical (natural and man-made) and cyber threats. However, discussions of resilience found in the literature are often focused on one operational domain (e.g., physical, information, cognitive, or social) and do not represent interconnections among system components to inform across these domains [6].

We have developed a multichannel solution for critical data broadband communications based on DSiP software. To do it, we have followed the DSR strategy. We have evaluated the solution with the data collected during the MACICO project and demonstrated it at the Viksu 2014 camp. We have proposed resilience metrics for PSC and analyzed how our solution fulfils/fails their objectives. Based on the findings during our DSR study, we have created additions to the knowledge base with regard to multichannel communications and PSC. However, much more research and development work is needed for making mission critical broadband data communications more resilient.

References

[1] I. Linkov, T. Bridges, F. Creutzig, J. Decker, C. Fox-Lent, W. Kröger, J. H. Lambert, A. Levermann, B. Montreuil, J. Nathwani, R. Nyer, O. Renn, B. Scharte, A. Scheffler, M. Schreurs and T. Thiel-Clemen, "Changing the resilience paradigm," *Nature Climate Change*, vol. 4, pp. 407-409, 2014.

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

[3] J. Rajamäki and R. Pirinen, "Critical infrastructure protection: Towards a design theory for resilient software-intensive systems," in *European Intelligence and Security Informatics Conference (EISIC)*, 2015.

[4] National Academy of Sciences, "Disaster resilience: a national imperative," 2012.

[5] D. Alberts, "Information age transformation, getting to a 21st century military. DOD Command and Control Research Program," 2002.
[6] I. Linkov, D. Eisenberg, K. Plourde, T. Seager, J. Allen and A. Kott, "Resilience metrics for cyber systems," *Environ Syst Decis*, 2013.
[7] T. Abdelzaher and A. Kott, *Resiliency and Robustness of Complex Systems and Networks. Adaptive, Dynamic and Resilient Systems.* Florida: Auerbach Publications, 2013.
[8] C. Backof, "Public Safety Communications in Emergencies [From the Editor]," *Vehicular Technology Magazine*, IEEE, vol. 8, pp. 4-4, 2013.
[9] M. Nouri, V. Lottici, R. Reggiannini, D. Ball and M. Rayne, "TEDS: A high speed digital mobile communication air interface for professional users," *Vehicular Technology Magazine*, IEEE, vol. 1, pp. 32-42, 2006.
[10] J. Vinkvist, T. Pesonen and M. Peltola, "Finland's 5 Steps to Critical Broadband," *RadioResource International*, 2014.
[11] K. Gomez, L. Goratti, T. Rasheed and L. Reynaud, "Enabling disaster-resilient 4G mobile communication networks," *IEEE Communications Magazine*, vol. 52, pp. 66-73, 2014.
[12] M. Peltola, "Evolution of Public Safety and Security Mobile Networks," 2011.
[13] R. Ferrus, R. Pisz, O. Sallent and G. Baldini, "Public Safety Mobile Broadband: A Techno-Economic Perspective," *Vehicular Technology Magazine*, IEEE, vol. 8, pp. 28-36, 2013.
[14] A. Calderon and R. Abadias, "Land Mobile Radio: Following a Realistic Path Toward Broadband for PPDR Services," *Vehicular Technology Magazine*, IEEE, vol. 8, pp. 37-45, 2013.
[15] K. Meier, D. Wehrle, K. Rechert and D. von Suchodoletz, "Testbed for mobile telephony networks," in *Sixth International Conference On Availability, Reliability and Security (ARES)*, 2011, pp. 661-666.
[16] P. Kämppi, J. Rajamäki, S. Tiainen and R. Leppänen, Eds., *MACICO - Multi-Agent Co-Operation in Cross-Border Operations*. Vantaa: Laurea, 2014.
[17] H. Simon, *The Science of the Artificial*. Cambridge: MIT Press, 1978.
[18] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A design science research methodology for information systems research," *J. Manage. Inf. Syst.*, vol. 24, pp. 45-77, 2007.
[19] A. Dresch, D. P. Lacerda and Antunes Jr, José Antônio Valle, *Design Science Research*. Springer, 2015.
[20] A. Hevner, S. March, J. Park and S. Ram, "Design Science Research in Information Systems," *MIS Quarterly*, vol. 28, pp. 75-105, 2004.
[21] M. C. Tremblay, A. R. Hevner and D. J. Berndt, "Focus groups for artifact refinement and evaluation in design research," *Communications of the Association for Information Systems*, vol. 26, pp. 1, 2010.
[22] 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, .
[23] 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.
[24] J. Ahokas, T. Guday, T. Lyytinen and J. Rajamäki, "Secure and Reliable Communications for SCADA Systems," *International Journal of Computers and Communications*, 2012.
[25] J. Ahokas, J. Rajamäki and I. Tikanmäki, "Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations," *International Journal of Communications*, pp. 120-127, 2012.
[26] J. Ahokas, "Secure and Reliable Communications Solution for SCADA and PPDR Use," 2013. Master's Thesis, Theseus.
[27] J. Simola, E. Jokinen and J. Rajamäki, "How situational awareness can be improved by using real-time video? Case: simulated natural disaster at the Viksu 2014 camp," I*nternational Journal of Systems Applications, Engineering & Development*, vol. 9, 2015.
[28] G. Di Marzo Serugendo, J. Fitzgerald, A. Romanovsky and N. Guelfi, "A metadata-based architectural model for dynamically resilient systems," in *Proceedings of the 2007 ACM Symposium on Applied Computing*, 2007, pp. 566-572.