LAUREA AMMATTIKORKEAKOULU Uuden edellä

Secure and Reliable Communications Solution for SCADA and PPDR Use

Ahokas, Jari

2013 Leppävaara

Laurea University of Applied Sciences
Laurea Leppävaara

Secure and Reliable Communications Solution for SCADA and PPDR Use

Jari Ahokas
Information Systems
Thesis
June, 2013

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojärjestelemäosaamisen koulutusohjelma

Jari Ahokas

Tietoturvallinen ja luotettava verkkoratkaisu infrastruktuurin ohjausjärjestelmille sekä viranomaiskommunikointia varten

Vuosi 2013 Sivumäärä 34

Samankaltaiset vaatimukset turvalliselle ja luotettavalle verkolle pätevät niin viranomaisten keskinäiseen kommunikointiin kuin infrastruktuurin ohjausjärjestelmiin (SCADA). Eurooppalaisilla viranomaisorganisatioilla on yhteneväiset vaatimukset viranomaisverkolle. Yhtenäinen verkko molemmille käyttökohteille luo synergiaetuja ja mahdollistaa järjestelmien keskinäisen kommunikoinnin myös valtakunnanrajoista välittämättä. Tässä tutkimuksessa esitellään erittäin luotettava ja turvattu kommunikointiverkko molempiin käyttötapauksiin. Kommunikaatioväylät ovat jaettuja verkkotasolla mutta silti turvallisia ja täysin eristettyjä muusta liikenteestä.

Keskeytymätön sähkönjakelu on äärettömän tärkeää nyky-yhteiskunnalle. Suojattu tiedonsiirto ohjauskeskusten ja sähköasemien välillä on kriittistä katkeamattoman sähkönjakelun turvaamiseksi. Turvallisuuden lisäämiseksi videovalvontaa tarvitaan sähköasemilla. Nykyiset verkot eivät kykene välittämään samanaikaisesti SCADA komentoja ja videokuvaa.

Tavanomainen Internet-yhteys ei ole riittävän luotettava ja turvallinen SCADA käyttöön. Multi-Agency Cooperation In Cross-border Operations (MACICO) projektin tavoitteena on toteuttaa uudenlainen ratkaisu jonka avulla yhdistää erilaisia tietoliikenneverkkoja, kuten TETRA, satelliitti, sähköverkkodata ja 2G/3G/4G verkot. Yhdistetyt verkot näkyvät turvallisena ja luotettavana tiedonsiirtoväylänä viranomaisten kommunikaatiojärjestelmille, SCADA yhteyksille sekä videokuvan siirrolle.

Vaaditun tietoturvatason saavuttamiseksi verkon pitää tukea monikanavaisia salattuja yhteyksiä sekä verkon on kyettävä priorisoimaan liikennettä ennalta määriteltyjen säänöstöjen pohjalta. Distributed Systems intercommunication Protocol (DSiP) pystyy toteuttamaan kaiken tämän samassa ratkaisussa. DSiP mahdollistaa monikanavaisen tietoturvallisen verkon rakentamisen sekä viranomaiskäyttöön että SCADA käyttöön.

Huolimatta siitä että yhteydet ovat tietoturvallisia ja luotettavia, on yhä olemassa joitakin haasteita verkkojen käytössä. Tämä tutkimus tuo näitä haasteita esille ja tarjoaa ratkaisuja näihin. Samalla tarkastellaan vaihtoehtoisia ratkaisuja yhteyksien turvaamiseen ja näitä verrataan ehdotettuun DSiP ratkaisuun.

Tässä raportissa on mukana kolme kansainvälisillä tiedefoorumeilla vuonna 2012 julkaistua raporttia. Kaksi ensimmäistä raporttia käsittelevät SCADA ohjausjärjestelmien yhteyksien turvaamista ja kolmas raportti keskittyy viranomaisverkkojen turvaamiseen. Tämä loppuraportti noudattaa monimentelmätutkimuksen periaatteita tietojärjestelmien tutkimusalalla. Työtä on peilattu tietojärjestelmä tutkimuksen seitsemää ohjenuoraa vasten.

Asiasanat, SCADA, viranomaisverkko, tietoturva, verkot, Distributed Systems intercommunication Protocol, DSiP, MACICO, monikanavaiset verkot

Laurea University of Applied Sciences
Leppävaara
Master of Business Administration
Information Systems

Abstract

Jari Ahokas

Secure and Reliable Communications Solution for SCADA and PPDR Use

Year 2013 Pages 34

Public Protection and Disaster Relief (PPDR) and Supervisory Control and Data Acquisition (SCADA) systems have similar needs for secured and reliable communications. All European PPDR organizations have similar requirements. A common network for both PPDR and SCADA creates synergy and makes interoperability within systems and cross borders possible. This report presents a highly redundant and secured communications network solution for both of the actors. The network level is shared between multiple actors but all communications can be secured and isolated from the other types of traffic.

Uninterrupted power distribution is extremely vital for modern society to function. Secured data transfer between control centers and power stations is critical for controlling and protecting power distribution. For added security live video stream is needed for monitoring the power stations. Current communications networks used with SCADA do not offer required features for transferring video stream in the same network as SCADA control commands.

A standard Internet connection does not offer the required reliability and security level for SCADA communications. Multi-Agency Cooperation In Cross-border Operations (MACICO) project aims to produce a new way of combining multiple telecommunication channels, such as TETRA, satellite, power line communications and 2G/3G/4G networks to create a single redundant secure and faster data transfer path for usable for PPDR and SCADA systems and at the same for video surveillance systems.

In order to provide the required level of reliability the communications network must support multi-link encrypted channels and the network must be able to prioritize traffic based on predefined parameters. Distributed Systems intercommunication Protocol (DSiP) is able to offer all of these features in a single unified solution. This enables building modern cyber-secure data network for both PPDR organizations and SCADA usage.

Even if the communications channels are secured and reliable, still some issues must be considered. This research report discusses these challenges and offers solutions for these. Also alternative solutions for securing the communications channels are discussed and compared to the proposed DSiP solution.

This research report includes three international publications published in year 2012. The first and second papers cover SCADA communications and the third paper focuses on PPDR challenges. The research work followed the multimethodological IS research concept. The work was evaluated by the seven guidelines for IS design research.

Keywords: SCADA, PPDR, Secure Communications, Distributed Systems intercommunication Protocol, DSiP, MACICO, Cross-Border Operations, Multichannel networks

Table of Contents

List of Publications

P[1] J. Ahokas, T. Guday, T. Lyytinen, J. Rajamäki, Secure Data Communications for Controlling Electric Power Stations and Distribution Systems, 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12), Proceedings Title: Mathematical Modelling and Simulation in Applied Sciences, Series Title: Mathematics and Computers in Science and Engineering Series | 1, Rovaniemi, Finland, Apr 18-20, 2012, ISSN: 2227-4588, ISBN: 978-1-61804-086-2, pp. 108-113, Paper URL: http://www.wseas.us/e-library/confernces/2012/Rovaniemi/INEE/INEE-00.pdf, Publisher: WSEAS Press

P[2] J. Ahokas, T. Guday, T. Lyytinen, J. Rajamäki, Secure and Reliable Communications for SCADA Systems, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, p ISSN: 2074-1294, p. 167-174, Paper URL: http://naun.org/multimedia/UPress/cc/16-296.pdf, Publisher: NAUN Press

P[3] J. Ahokas, J. Rajamäki, I. Tikanmäki, Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, E-ISSN: 1998-4480, p. 120-127, Paper URL: http://naun.org/multimedia/UPress/cc/16-295.pdf, Publisher: NAUN Press

P[4] J. Rajamäki, J. Ahokas, P. Rathod Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System. 2nd International Conference on INFORMATION TECHNOLOGY and COMPUTER NETWORKS (ITCN '13). Antalya, Turkey October 8-10, 2013. Under review.

List of Abbreviations & Symbols

ADSL	Asymmetric Digital Subscriber Line
CIP	Critical Infrastructure Protection
DoS	Denial of Service
GPRS	General Packet Radio System
Internet	Global system of interconnected computer networks
IS	Information Systems
IT	Information Technology
LTE	Long Term Evolution
MACICIO	Multi-agency cooperation in cross-border operations
MOBI	Mobile Object Bus Interaction -project
NERC	North America Electric Reliability Corporation
PKI	Public Key Infrastructure
PLC	Power Line Communications
PPDR	Public Protection and Disaster Relief
QoS	Quality of Service
SCADA	Supervisory Control and Data Acquisition
SDSL	Symmetric Digital Subscriber Line
SSL	Secure Sockets Layer
TDMA	Time Division Multiple Access
TEKES	Finnish Funding Agency for Technology and Innovation
TETRA	Terrestrial Trunked Radio
UMTS	Universal Mobile Telecommunications System
VDSL	Very-high-bit-rate Digital Subscriber Line
VIRVE	Viranomaisradioverkko, Government Official Radio Network
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access

1 Introduction

The need for secure and reliable communications for Public Protection and Disaster Relief and securing vital public infrastructure SCADA control is more and more important for the modern society to function. The PPDR requirements for communications share almost identical functional requirements as the infrastructure controlling systems.

Many vital infrastructure components such as electricity distribution network and water treatment plants are operated remotely by using SCADA control systems. Uninterrupted and disaster tolerant secured communications channels are needed for the continued operation at all circumstances. An added security requirement comes from the requirement of protecting the premises from unauthorized access by monitoring and using access control systems and at the same by monitoring weather conditions and other nature phenomenons. In order to fulfill this requirement a surveillance system like live video monitoring is needed. This research project is a part of a larger MOBI project that is funded also by TEKES. Even larger MACICO project includes the MOBI research project. MACICO will develop a concept for interworking of security organizations in their daily activity (MACICO project information).

There have been many papers and thesis written discussing about the DSiP solution. DSiP technology has been introduced by Dr. Jyri Rajamäki in many of the previous publications. The basics of the DSiP system operation is explained in these papers in much greater detail. The latest thesis was Public Protection and Disaster Relief services ICT-systems developing and integration by Taina Hult in 2012 at Laurea University of Applied Sciences. The previous papers did not cover particular use cases for the DSiP and comparing it at the same time to other alternative solutions for securing communications or providing alternative communications channels.

The primary objective in this research was to evaluate available methods of securing communications in PPDR and SCADA usage. The aim of the research was to find out how to have secure reliable communication channels and what were the alternative methods for achieving similar level of protection and reliability. Actual end to end test scenario with the suggested solution was out of scope for this research project. Also designing new hardware or software artifacts were out of scope for the research.

As a secondary objective for these publications it was to produce R&D research work to be published in international forums thus meeting the goals of Laurea University of Applied Sciences educational programs.

This thesis was constructed by using the framework for Information Systems design research. The IS design framework gives seven guidelines for researchers constructing, presenting and evaluating their research work. The framework also motivates the researcher to use varying research and evaluation methodologies to achieve high quality research results. (Hevner et al 2004.) In this research the framework is offered to the audience for understanding the IS design research concept.

This thesis contains three publications that were published internationally in the year 2012. These publications cover securing communications and providing reliable fault tolerant communication paths. Different aspects of security and communications methods are covered and several alternative methods for reliable communications are introduced. After comparing all of these communications solutions available a conclusion is made: the DSiP system provides the required level of reliability and security without the need to change or redesign applications already in use.

The following chapter offers basic information about different communications networks, what are the alternatives for securing the communications channels used and how reliable the channels are in general. The third chapter discusses in more detail research methods used in this thesis. The fourth chapter summarizes all of the publications [P1, P2, P3] results and the fifth chapter presents the conclusions of this research and gives suggestions for further research work.

2 Communication Networks and Security with SCADA and PPDR

Secure and reliable communications are essential building block for SCADA and PPDR usage. In the following sections these communications channels and security measures are briefly introduced for the purpose of evaluating and understanding what is available for use and what are the features and/or limitations of each of the presented methods. For research purposes it is necessary to in general level understand the alternatives available for communication networks and securing the networks.

Using only one network for communications can be considered a risk especially for PPDR usage. In the USA Office of Emergency Communications is aiming for Nationwide Public Safety Broadband Network, FirstNet, to be based on LTE network technology (Office of Emergency Communications 2012). LTE networks are vulnerable to wireless interface jamming using low cost relatively simple devices as described in Virginia Tech preliminary research (Wireless @ Virginia Tech 2012). If networks build on LTE technology were to be compromised, existing 2G and 3G networks would still operate without problems - but those older networks are gradu-

ally being phased out. This fact emphasis the need for uninterrupted and secured multichannel communications – with several alternative channels in order to produce a highly reliable cyver-seure communications network. (Rajamäki at al 2013.)

2.1 Available Communications Channels

There are several alternative communications networks available for communication between the PPDR actors and the same channels are also suitable for SCADA communications. Traditionally SCADA systems have used analog propriety radio based communications systems. PPDR communications have also used propriety methods for communications. These are usually non-compatible with normal commercial networks and also with each other, it might be that firefighters and the police force have incompatible networks. SCADA communications can be accomplished also with fixed line connections which are for obvious reasons quite useless for PPDR usage at the field. Fixed location PPDR command and control center does benefit from fixed networks as these can provide more bandwidth and lower latency.

2.1.1 Propriety Radio

Propriety radio uses private radio channels normally using analog frequency modulation techniques. These have limited bandwidth and lower quality compared to digital radio networks. Range of a single cell might be larger than with digital radio. Radio channels are busy and free undisturbed frequencies are not easily available, also the same radio channels cannot be used worldwide for regulatory reasons. Resistance to errors and reliability is an issue with propriety radio communications because of analog radio technology limitations in error correction etc. Also the carrier network itself is a subject to wiretapping and could be considered unsafe in nature.

2.1.2 TETRA

TETRA was originally developed for official use such as police force or fire fighters. It has slow data transfer capabilities with speeds in GPRS class and somewhat limited functionality compared to other current commercial networks. It offers built-in security for communications since end user devices are authenticated with the network. Communication networks might not be compatible across borders, because of different radio frequencies or other communications parameters at the network level. One transmission cell can cover much wider area when compared to 4G/LTE technologies because of using lower frequency band. (Korhonen 2003.)

Apart from the video coding synchronization mechanisms (e.g. MPEG-4, H.263), the TETRA system uses a synchronization technique known as frame stealing to providing synchronization to end-to-end encrypted data (Stavroulakis 2007).

2.1.3 GSM aka 2G

The Global System for Mobile communications (GSM) is a wireless telecommunications standard for digital cellular services that can be used for a communications system also in sparsely populated areas. The original standard was optimized for voice communications and provided only circuit-switched data connections at a bit rate of 9.6 kbps. Later enhancements made higher bit rates and packet switched GPRS data possible. GSM is based on TDMA technology and is widely used around the globe. Used radio frequencies are different in different continents but modern end user devices can handle all frequency bands. (Korhonen 2003.)

2.1.4 3G

The 3G networks are popular but there might be problems when a cell is heavily utilized by a large number of clients. Cell range is more limited than with GSM and service might not be available in rural districts. 3G is an abbreviation for the 3rd Generation system for mobile communications. 3G consists of a family of standards under the framework of International Mobile Telecommunications for the year 2000 (IMT-2000). The European version is known as The Universal Mobile Telecommunications System (UMTS). The other main standards are CDMA2000 and Mobile Wi-Max. The third generation is characterized by the convergence of voice and data with mobile Internet access, multimedia applications and high data transmission rates. (Korhonen 2003.)

2.1.5 4G LTE

LTE is a fast network but with small cell coverage. It is most likely not available in areas where power stations are located, being sparsely populated areas. For PDDR usage 4G has an issue with security, 4G networks can be easily disturbed by DoS attack, with relatively cheap equipment. 3GPP LTE or 3G LTE (Long Term Evolution) is the 3GPP work item on the long term evolution (LTE) of the air interface of UMTS (evolved UTRA) and its associated radio access network (evolved UTRAN). LTE will offer even higher peak data rates with a reduced latency. LTE will be a completely packet-optimized radio-access technology. 3GPP LTE improves spectral efficiency, allowing for a large increase in system capacity and reduced cost per gigabyte. (Dahlman et al 2008.)

2.1.6 Satellite

Satellite communications are expensive for data transfer but have very wide coverage. Communications speed is a problem, especially with upstream communications. Fast and reliable connection might require large receiver antennas. Connection speed and the whole communication itself is also subject to weather conditions such as heavy snowing. (Maini & Agrawal 2011.) For PDDR usage limitations include the satellite connection not working inside tunnels, inside buildings, dense forests or between high buildings in a city area.

2.1.7 Fixed lines

There are several technologies and line speeds available such as ADSL, E1, SDSL, T1, VDSL and fiber optics. Any of these networks can be used for SCADA communications and video surveillance since all of these networks carry IP traffic. Reliability especially in home use grade ADSL connections is not enough for mission critical applications but economically these are quite tempting. Also the cost of e.g. fiber optics can be seen as a limiting factor.

Power line communications is also a suitable technology especially for power station data collection purposes. For SCADA communications this is not a viable solution as an only communications channel for obvious reasons: when a command is given to disconnect current from the power line all communications are lost thru that line. The same effect occurs if the power line is out of service by weather conditions or by other technical failure. (Ferreira & al, 2010.)

2.2 Securing Communications

There are various methods available for securing natively unsecured IP communications channels. Here is some basic information on some of the methods available. Most of these are VPNs based on a PKI certificates or pre shared keys. These security measures are focused on IPv4 communications but can be adapted into IPv6 environments.

2.2.1 VPN

This is the classical and proven solution for securing communications. Fault tolerance is not normally built into VPN solutions. VPN protocols are not multichannel aware by default but there are propriety solutions available. For example Stonesoft Oyj, located in Finland, develops Stonegate firewall that is multichannel aware Multi-link VPN solution. The security level depends on selected encryption algorithms and authentication methods. VPN tunnels might

use IP protocols and TCP/UDP ports that are not open for communication in every carrier network.

2.2.2 SSL VPN

SSL communications works virtually with every IP-network. It accepts multiple paths for transport and is able to re-sequence packets. It runs on top of HTTPS protocol and works with TCP/IP protocol. SSL connections are session aware and normal TCP resend acks are used. The level of encryption depends on used certificates, the length of the encryption key. SSL VPN is also known as IP-HTTPS with Microsoft 2012 server Direct Access implementation. IP-HTTPS is able to handle IPv4 NAT and is also able to tunnel IPv6 traffic thru IPv4 only network.

2.3 Reliable Communications

Fault tolerant communications can be achieved by using several different communications networks at the same time. This requires that the application is aware of the networks and capabilities for handling multiple routes to a single destination. Most of the solutions require application recoding and redesign to utilize alternative network routes.

Quality of Service (QoS) definition can be problematic since (mainly commercial) networks might not support end-to-end QoS tagging at all. Defining QoS required DiffServ schemas can be a daunting task if and when there are more than couple of protocols and networks in use as number of possible combinations grow exponentially. IPv6 implementation has QoS features built in and offer end to end definitions in every carrier network.

2.4 Usages for Secured and Reliable Communications

In modern society there are many usages for trustworthy communications. Technological advances in telecommunication has enabled many more possibilities for new usage scenarios. It is important to the researcher to understand possible usage scenarios and to aim to develop a new way of using previous and newer systems together.

2.4.1 Transforming SCADA Communications More Reliable and Secure

SCADA systems are critical to modern society since these systems control nuclear power plants, power distribution and other basic infrastructure functions such as water treatment plants. By adding several communications paths by using alternative public and private networks with strong security measures the SCADA systems control become more reliable.

For added security perimeter surveillance and live video stream are important. Security threats can be unauthorized personnel accessing a power station or extreme weather conditions.

Supervisory Control and Data Acquisition (SCADA) generally refers to the control system of the industry, where SCADA is a computer system that controls and monitors a process. This process can be infrastructure, facility or industrial based. SCADA systems are also used for monitoring and controlling physical processes like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society. (Scada Information; Daneels & Salter 1999.)

2.4.2 PPDR Networks

Public authorities require highly fault tolerant and secure methods for communications. In disaster recovery situations many of the normally available networks might be unavailable and secondary communications channels are vital. Also government networks such as VIRVE can suffer from network outages thus justifying satellite communications as an alternative network.

PPDR usage also benefits from a network that is able to prioritize voice traffic over other IP traffic and when network allows provide high bandwidths for video etc. in order to rescue centers to analyze the situation more thoroughly.

Mobility is an important issue with PPDR usage, all devices must be power efficient and suitable for vehicle usage and/or operate as a hand held devices. Additional requirement is that the devices should be able use networks in areas that have challenges with network coverage, the devices must be multi network capable.

Secure and reliable wireless communication between first responders and between first responders and their Emergency Control Center is vital for the successful handling of any emergency situation, whichever service (Police, Fire, Medical or Civil Protection) is involved. (Ahokas, Rajamäki & Tikanmäki 2012.)

Regarding the next generation of services for first responders, the ETSI MESA project (ETSI Project MESA) has examined what would be possible if wireless broadband capacity was available; i.e. if some of the technologies that have revolutionized the commercial transport of information (both wired and wireless) in recent years were applied in the PSC market. Figure 1 shows project MESA generic core network architecture picture for public services networks.

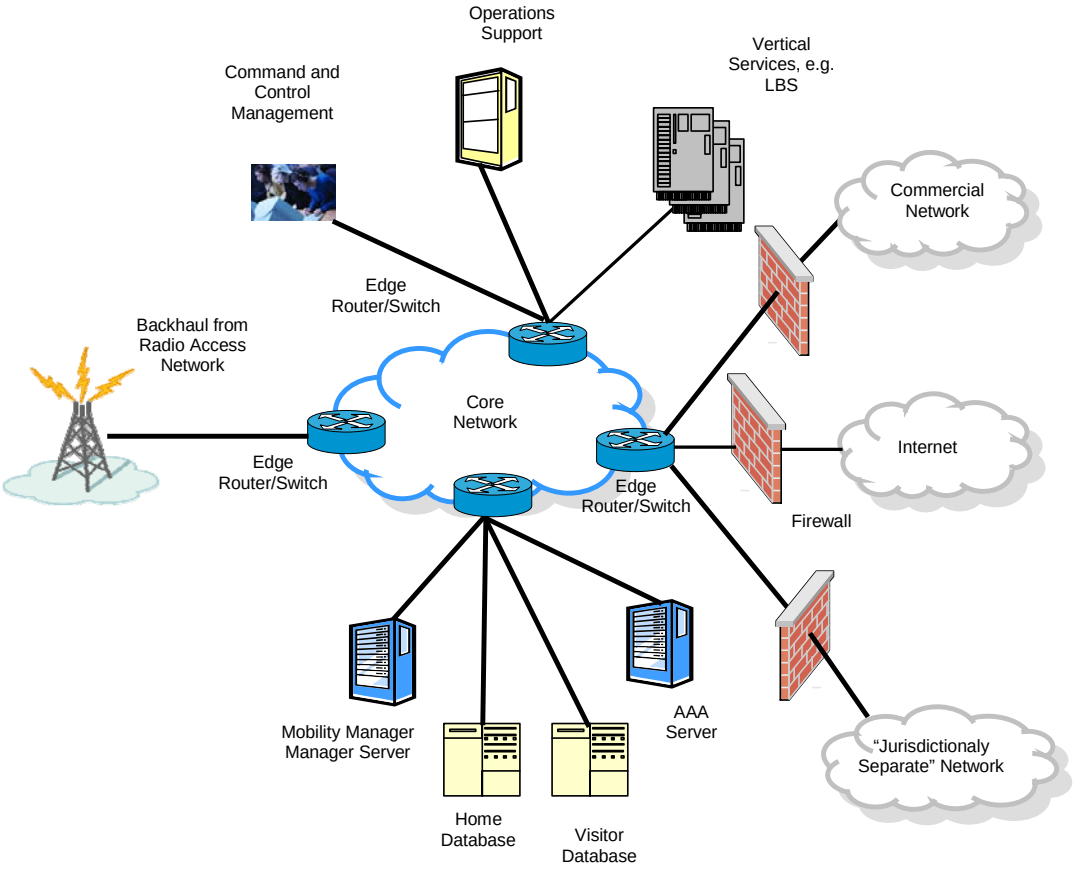

Figure 1 Project MESA network architecture (ETSI Project MESA)

3 Research Process

The objective of this research was to evaluate suitable solutions for securing both PPDR and SCADA communications. In practice this research project evaluates several solutions and compares different aspects of each solution. We took the role of systems analysis and just evaluated different solutions. The objective was not to develop any new previously unused techniques.

The researcher must be able to find and use suitable methods for his/hers research problem. "A research methodology consists of the combination of the process, methods, and tools that are used in conducting research in a research domain" (Nunamaker at al 1991.) There is a risk that researchers have wrong questions to ask if they do not have adequate understanding of research question thus invalidating the research work. In figure 2 diagram of the multi-methodological approach is presented. (Nunamaker at al 1991.)

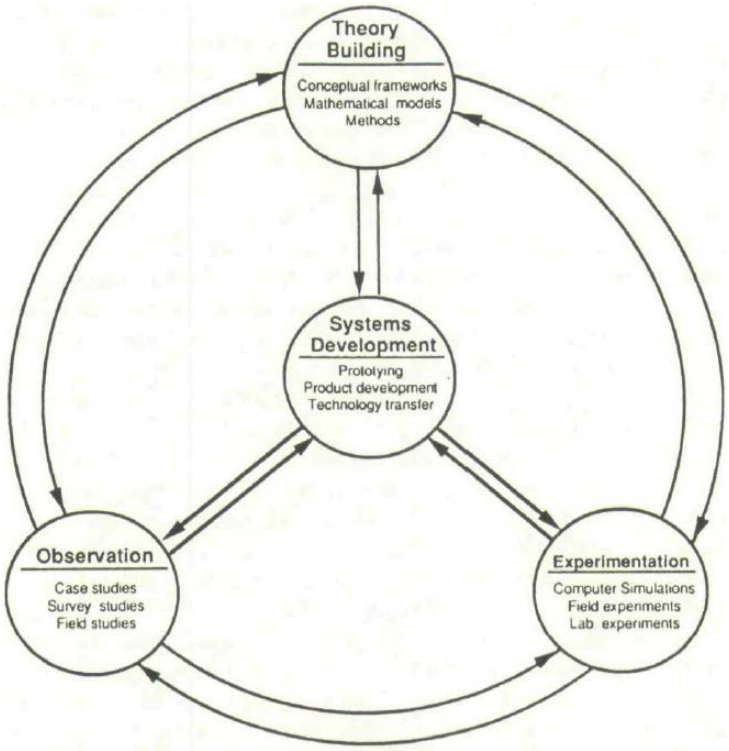

Figure 2 A multimehodological approach to IS framework (Nunamaker et al 1991)

Theory Building

Nunamaker at al (1991) state that "Relevance refers to potential insights and impacts on practical applications; this suggests that theory building or basic research contributes to the body of knowledge in a research domain but produces nothing (no system) that takes advantage of this new knowledge." Theory building includes development of new ideas and concepts.

This phase was included in all of the publications, acting as a building block for the publication itself. Theory building was mainly development of new ideas and concepts in the publications. Producing something new by combining something older already previously available knowledge.

Observation

Observation is often used when is relatively little known about a research area and there is a need to get a general view of the research domain. Typical methods are case studies, field studies and sample surveys that are unobtrusive research operations. (Nunamaker at al 1991.)

Case study method was used in P1 while collecting data about SCADA and power station usage. In publications [P2, P3] previously collected information was used for refining the artifact developed.

Experimentation

This includes methods such as laboratory and field experiments or simulations. Results can be used for refining theories. Experimentation can be used when more information is needed of the subject matter. (Nunamaker at al 1991.)

The publications have experiments documented, especially publication [P3] where an actual physical use case is described. In publications [P1, P2] is an experiment on SCADA control without DSiP briefly described.

Systems development

For the research work systems development contains the following five stages: concept design, constructing the architecture of the system, prototyping, product development and technology transfer. If the developed theories, concepts and systems are judged useful they are transferred to organizations which represents an ultimate success for those theories. (Nunamaker at al 1991.)

As stated earlier actual development work of a new system was not done during the research. The objective was to find secure and reliable communications solution for SCADA and PPDR usage. Evaluated solutions were already available and the most suitable solutions was selected. Field testing described in publication P3 will most likely require some development work.

3.1 Research Process Evaluation

IS design research can be seen as a problem solving guideline. It is used to solve actual business problems and to create a technological solution, being either a physical device or a program or a new procedure, to solve the problem at hand.

Hevner, March, Park & Ram (2004) present a research framework for IS design research. The purpose of the framework is to give guidelines for the researchers how to conduct, evaluate and present their research work. This framework also helps the audience to understand IS design research in general. The form of the artifact is not defined strictly, it could be a program or a method or similar. (Hevner at al 2004.)

Hevner at al (2004) present seven useful guidelines to be followed for effective and rigorous design science research. The purpose of the guidelines is to assist researchers, reviewers, editors and readers to understand design science research. (Hevner at al 2004.) The following sections present the guidelines briefly and give short explanation how the guidelines were used during the research process.

Guideline 1: Design as an Artifact

Design-science research must produce a viable IT artifact in the form of a construct, a model, a method, or an instantiation. It must be described so that it can implemented and applied to the appropriate domain. (Hevner at al 2004.)

For this research project the guidelines were given by the MACICO and MOBI projects. The main guideline being finding a suitable communications solution fulfilling the requirements set by the definition documents. The form of the artifact was not predefined but it is evident that it must be in a form of physical device and software combination.

Guideline 2: Problem Relevance

The objective of design-science research is to acquire knowledge that enables the development of technology-based solutions to unsolved, important and relevant business problems. A problem can defined as the differences between a goal state and the current state of a system. (Hevner at al 2004.)

The review process of the publications has established that the publications in question are scientifically relevant thus being published. The research questions in the publications [P1, P2, P3] are extracted from actual real world problems.

Guideline 3: Design Evaluation

The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods. (Hevner at al 2004.)

1. Observational	Case Study: Study artifact in depth in business environment Field Study: Monitor use of artifact in multiple projects
2. Analytical	Static Analysis: Examine structure of artifact for static qualities (e.g., complexity) Architecture Analysis: Study fit of artifact into technical IS architecture Optimization: Demonstrate inherent optimal properties of artifact or provide optimality bounds on artifact behavior Dynamic Analysis: Study artifact in use for dynamic qualities (e.g., performance)
3. Experimental	Controlled Experiment: Study artifact in controlled environment for qualities (e.g., usability) Simulation – Execute artifact with artificial data
4. Testing	Functional (Black Box) Testing: Execute artifact interfaces to discover failures and identify defects Structural (White Box) Testing: Perform coverage testing of some metric (e.g., execution paths) in the artifact implementation
5. Descriptive	Informed Argument: Use information from the knowledge base (e.g., relevant research) to build a convincing argument for the artifact's utility Scenarios: Construct detailed scenarios around the artifact to demonstrate its utility

Table 1 Design Evaluation Methods (Hevner et al 2004)

International conferences and publication reviewers have evaluated the publications. Field testing is currently in progress at LUAS, actually implementing the DSiP system in a police vehicle for testing purposes.

Guideline 4: Research Contributions
Effective design-science research must provide clear and verifiable contributions. Research must answer the question "What are the new and interesting contributions?". (Hevner at al 2004.)

In this research the results are descriptive and functional. Descriptive being basic knowledge of communications networks and information about SCADA, surveillance systems and PPDR communications. Functional contribution in the publications being DSiP usage in new use case scenarios.

Guideline 5: Research Rigor
Design-science research emphasis on rigorous methods in both the construction and evaluation. Overemphasis on rigor in behavioral IS research has often resulted in a corresponding lowering of relevance (Lee 1999). Rigor can be achieved by using the available knowledge databases efficiently. (Hevner at al 2004.)

The most important use of the knowledge database is to use it as source for skilled researcher to develop theory or artifact. All three publications used knowledge databases for comparing and evaluating technical details to develop a theory and an artifact.

Guideline 6: Design as a Search Process
The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment. (Hevner at al 2004.)

For this research project the main target was to find a suitable solution for securing critical infrastructure management communications. As the problem setup itself did not set any specific requirements that would have forced the research team to use a specific solution, the most appropriate solution was chosen. After that the focus of the research work was easily set to the DSiP. Limiting factors for this research were time and available resources for conducting a full scale testing.

Guideline 7: Communication of Research
Design-science research must be presented effectively to both technology-oriented as well as management-oriented audiences. Technology audience requires enough detailed information

to build the artifact by themselves and management audience requires adequate information to evaluate if the artifact is suitable for their organization. (Hevner at al 2004.)

The results of the publication P1 were presented in a conference & conference journal and publications [P2, P3] in a journal. Extensive communication and team work with colleagues provided self-evaluation and ensured that the communication of the research work for different audiences was suitable for their requirements and thus added rigor to the research process.

The time scale of the research process is presented in figure 3. In the figure there is no information given on non-published material that has been written in October 2012 and January 2013. Also this material is not included, quoted nor described in this research report as it has not been published. Publication [P4] is also omitted from the figure because the review process of the publication [P4] was not yet completed at time this report was submitted for review process and published.

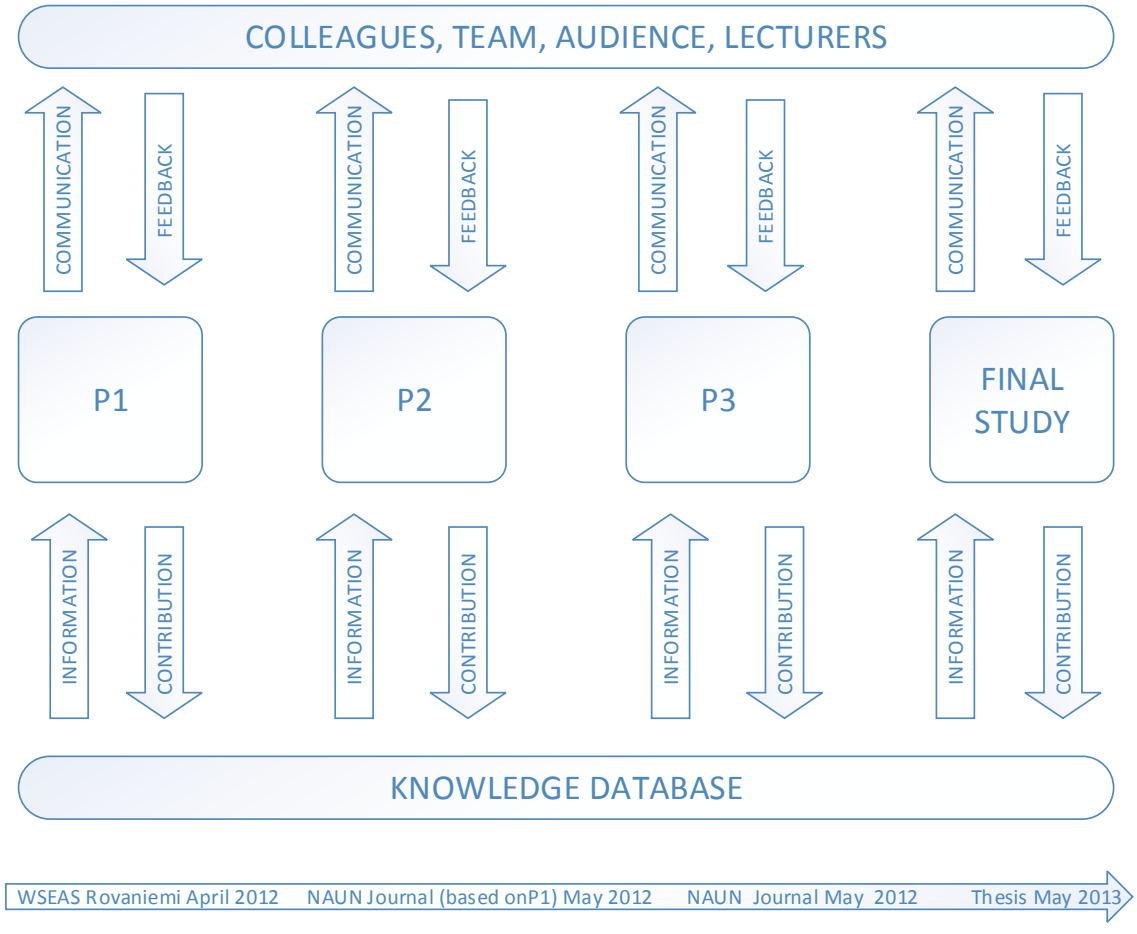

Figure 3 Schedule of the research process

4 Summary of Publications

In this chapter a brief summary of the publications is given. The full publications are included as appendices in this thesis. The problem space is explained and a common solution for both problems is given. Also a description of author's role in each publication is given in this chapter.

4.1 Secure Communications for Controlling Electric Power Stations and Distribution Systems

As earlier stated: SCADA systems are used for controlling infrastructure components like power stations and power distribution grids. For this a protected, fast, low latency and uninterrupted communications is a requirement. Publications [P1, P2] discuss communication alternatives and different methods to secure SCADA communications with reliable connections.

Many of the currently used SCADA systems use propriety communications channels. More reliable network based on alternative multiple paths is needed for added features, reliability and security. Networks used with SCADA could be GSM, 3G, LTE, satellite, ADSL or virtually any IP network with suitable features. The communications solution must be able to vividly adopt itself to changes in the underlying data transport layers e.g. services of the communication solution must be controllable according to available bandwidth of a communication channel. Another very important task is to control the priorities of the transported messages; Site surveillance and SCADA-command & control must be thoroughly contemplated before implementation. (Ahokas at al 2012b.)

For SCADA control signals bandwidth is not important in general but reliability is. Variation in response time (ping latency) and low jitter (variation of latency) are critical for time sensitive process controlling such as factories. This being vice versa for video surveillance where bandwidth is required for high quality video stream. Just securing the communications channel is not enough, also more bandwidth is needed for live video surveillance and access control systems.

Combining the different requirements in a single easy to implement solution is a challenging task. Several solutions are available but these mainly focus on resolving one single issue and do not analyze & solve the problem at hand as a whole. In order the DSiP solution to function, all communications must be carried over IP protocol. For power stations, this sets a requirement of using devices converting traditional serial port based traffic to IP based traffic. Existing equipment can be converted to IP traffic by using a serial to IP converter, or a RS-232 to Ethernet by other name. Installing new natively IP enabled equipment thus replacing older RS-232 equipment might not be economically viable solution since SCADA systems can have a

relatively long life span. For some of the older power stations, there is a minor additional cost from building IP network, usually standard Ethernet based technology. (Rajamäki at al 2013).

In the future, a common cyber secure voice and data network for MIL, PPDR and CIP brings synergy and enables interoperability; separate networks are waste of resources (Ahokas at al 2012a). This can be extended to cross border level of operation when officials from different countries can use unified communication devices for all use cases regardless of their physical location.

4.1.1 Use Case

The particular problem studied in publications [P1, P2] was securing the power station communications. The aim was to provide reliable communications for SCADA control regardless of used communications channels. And at the same to provide faster communications channels for video surveillance if permitted by high priority, defined by QoS, SCADA communications traffic. Figure 4 shows a principal diagram of video surveillance and SCADA control combined with all communications channels handled by a DSiP router.

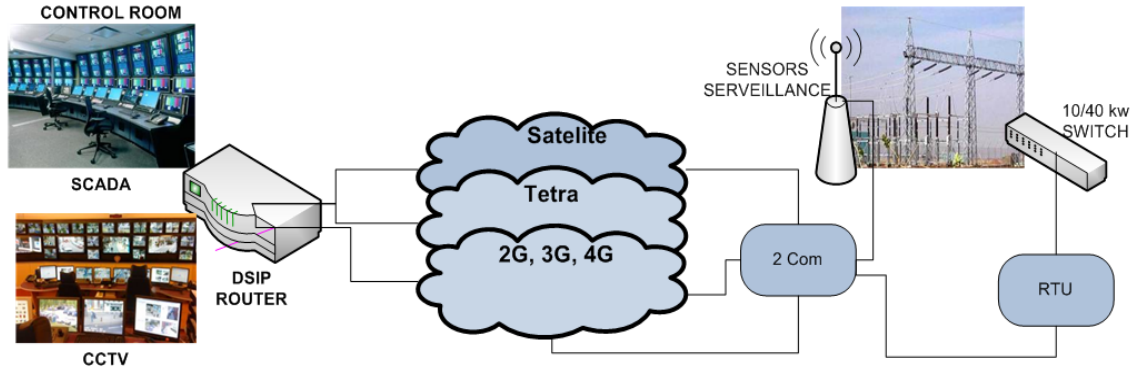

Figure 4 SCADA communications and video surveillance network with DSiP (Ahokas at al 2012b)

This use case aims to creating a multichannel communication resource from a control room to an electric power station. The communication solution will implement SCADA-command and control messaging in parallel with of a CCTV monitoring and other surveillance and monitoring systems. The aim of this use case is to provide an easily implementable uniform communication solution that will take into account the needs of a smart-grid system, command and control of an electrical substation and site surveillance and perimeter monitoring. (Ahokas at al 2012b.)

4.2 Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations

The same communications networks can be used with PPDR as with SCADA. Publication [P3] addresses these challenges from a different perspective than SCADA publications [P1, P2]. Security and reliability is of an essence for PPDR use. Cross border functionality is also required for example in border control operations that might span to neighboring countries. Mobility creates additional requirements to the system when compared to the SCADA use case. For PPDR this is hand held devices which must be reasonable sized & weight and must also have long battery life. For vehicle usage limited power capabilities must be considered, when the engine of the vehicle is not running vehicle battery life is an issue as additional batteries might not be possible to install.

PPDR has an additional challenge with situations where no traditional communications networks are available for use. In these cases intermittently connected networks are viable solution. In this research, ICNs were discussed in publication P3, it was not a primary research target so ICNs were not analyzed with greater detail.

These devices carrying data from communications blackout areas can be data collecting and transmitting unmanned flying objects. Critical infrastructure organizations could benefit from such technology. Mainly because organizations could collect data, such as pictures or other data describing the situation at hand, from the disaster area and transfer it to the control room easily. Other possible solution is to transfer data with an external memory device manually from the area affected by a communications failure to a location with functioning network connection. This solution is not practical for remote surveillance nor remote control. In order to make this kind of ICN to work IP protocol modifications are required. A modified backpressure routing algorithm can separate the two time scales of ICNs. It is presented in Jung Ryu's research, this algorithm improves performance. On top of this, algorithm is a rate control protocol implemented on TCP protocol (Ryu 2011).

In emergency situations, it is possible to utilize ad hoc networks for communications when communication network fails because of infrastructure destruction. In case of power stations, usages for ad hoc communications methods are few. Since there might not be any other (communications) nodes available within the communications range. One solution for managing communication paths using ad hoc networks is the Ad hoc On-Demand Distance Vector (AODV) algorithm. (Park at al 2010.)

The two main challenges in European PPDR field operations are the lack of interoperability and the lack of broadband connectivity (Baldini 2010). Lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, and gaps in procurement or research. Lack of broadband connectivity of wireless communications limits especially the work of the commander of the mobile rescue team at the scene of events.

4.2.1 Use Case II

At LUAS there is an actual police vehicle equipped with DSiP router & satellite and 3G network connectivity for field testing purposes. With this test unit it is possible to test different usage scenarios and functionality in mobility situations. Also power consumption of the equipment, that is an important with factor in vehicle use, can be tested in actual usage scenario. Figure 5 demonstrates the proposed and to be tested communications schema for the onboard vehicle usage.

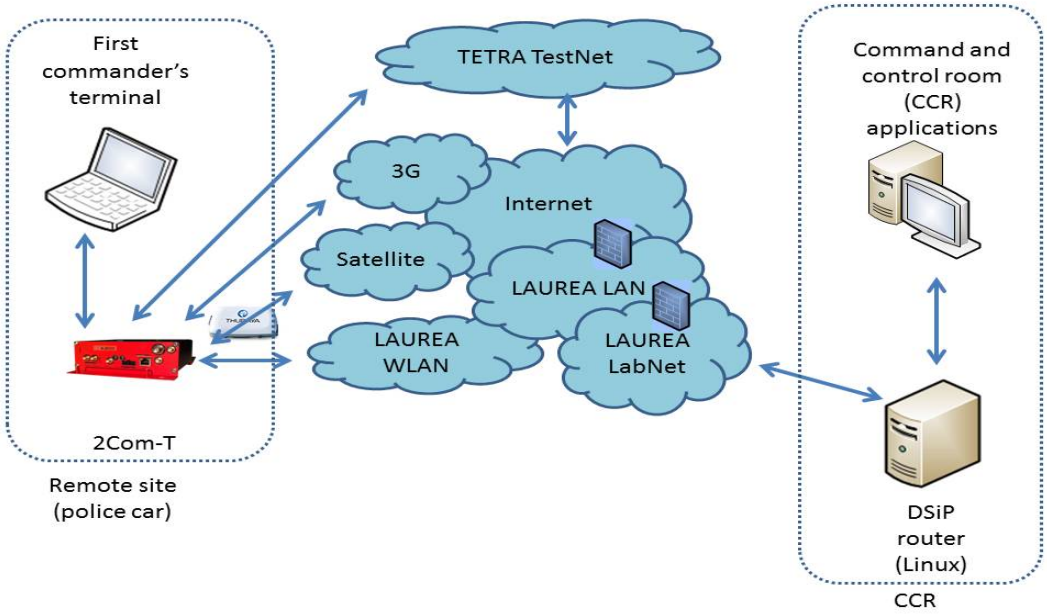

Figure 5 A Communications network for PPDR use (Ahokas, Rajamäki & Tikanmäki 2012)

Laurea University of applied sciences (LUAS) has ongoing project called Mobile Object Bus Interaction (MOBI), funded by the Finnish Funding Agency for Technology and Innovation (Tekes). Project's aims are to create a basis for export-striving emergency vehicle concept and to initiate standardization development with like-minded-countries and possible with EUROPOL. There are also three corporate projects exploiting data which are launched alongside with the project. Project has eight work packages; 1) Coordination, 2) User needs, 3) Vehicle infrastructure and power generation, 4) Data communication, 5) Software infrastructure, 6)

Applications, 7) Demonstration on police vehicle and 8) Business model development. (Hult & Rajamäki 2011.)

4.3 Solution: DSiP

As a solution to the problem a DSiP device is offered in the publications P [1,2,3]. It combines multichannel multinetwork system with reliability, security without any application recoding. The DSiP has QoS features and has an easy-to-use control and monitoring framework.

Distributed Systems intercommunication Protocol (DSiP) system allows for combining all kinds of telecommunication resources into a single, uniform and maintainable system (Holmström at al 2011). The DSiP solution makes communication reliable and unbreakable. DSiP uses several physical communication methods in parallel. Applications, equipment and devices operate as these were communicating over a single unbreakable data channel. Satellite, TETRA, 2G, 3G, 4G/LTE, VHF-radios etc. can be used simultaneously in parallel. DSiP is suitable for a vast range of applications (Rajamäki at al 2010; Holmström, Rajamäki & Hult 2011). Power Grid Control, SCADA and Public Safety communication are given as examples of use cases.

The DSiP solution brings several benefits to communications. For example better data security, integrity & priority. Immunity towards virus infusion and DoS network attacks with intrusion detection. For communications there are data-flow handshaking and flow-control systems implemented with automatic re-routing. Early detection of communication problems helps minimizing communication disruptions because the change of the communication channel can occur earlier. (Ahokas at al 2012b.)

The DSiP system establishes several IP communications channels between the client and command and control center. All of these connections have different IP addresses for each end point and have unique security associations between them. Complexity of this communications network mesh is hidden behind the DSiP system by showing only one logical connection to the application, such as SCADA, using the mesh network. This can be referred also as a Multi-Link VPN connection. In a Multi-Link configuration, the VPN traffic flow can use one of multiple alternative VPN tunnels to reach the same destination device. This ensures that even if one or more tunnels should fail, the VPN service continues to function as long as there is at least one tunnel available. Some of the defined tunnels and network links can be configured in standby mode. (Rajamäki at al 2013.)

Other benefits include: authentication- and management tools, controllable data casting and compression, interfacing capabilities to equipment and software. For communications DSiP

offers: transparent tunneling of any data, cost-efficient network topology, insulation from Internet-system flaws and routing according to lowest cost and/or shortest hops. Critical networks and communication solutions require efficient management and monitoring tools. The DSiP solution contains several modules for support, maintenance and configuration. Authentication Server Software: The DSiP features centralized and mirrorable Authentication Server software. This software allows for editing passwords for DSiP nodes. The nodes may have passwords that expire after a specific time for security reasons. Nodes may be allowed in the DSiP routing system and they may be excluded from it at any given time. (Ahokas at al 2012b.)

The DSiP device and software solution can hide the complexity of the network architecture from the applications and especially from the end users. But a problem with TCP network convergence still exists. When the characteristics of the undelaying physical network change rapidly, often and/or considerably, the currently used TCP congestion protocols are unable to follow the change in a timely manner. To mitigate this problem various solutions are available such as TCP ACK algorithm enhancements. (Ahokas, Rajamäki & Tikanmäki 2012.)

Table 2 shows comparison between different kind of solutions used for securing (security and reliability) communications channels and how this effects currently used systems. The comparison table shows that DSiP fulfills the requirements except in the fluctuating network situation.

	Multiple routes	**QoS**	**Single Device / Software / Firmware**	**Application rewriting**	**TCP in fluctuating networks**	**Security**	**Cost control per route**
DSiP	X	X	X			X	X
Diff-Serv		X		X			
Crossed Crypto-Scheme	X			X		X	X (static)
Ad Hoc networks	X (point to point)					X (if provided by the network)	
ICN	X				X		

Table 2 Comparison of different solutions for secure and reliable communications (Rajamäki at al 2013)

In figure 6 there is a principal operating chart introduced. It demonstrates a SCADA use case with control room and remote terminals (RTUs) using alternative networks combined with the DSiP routers. Traditional connection would involve radio communications and custom hardware for connecting RTUs to the control center. The DSiP devices are able to select from multiple communications links the most suitable for each use case depending on required speed, cost etc. variables.

Deploying DSiP system can help in achieving NERC (North America Electric Reliability Corporation) standards, especially targeted for CIP (Critical Infrastructure Protection). NERC CIP 002-009 documents set demanding reliability and security standards for protecting SCADA communications (NERC Standards 2012; Rajamäki at al 2013).

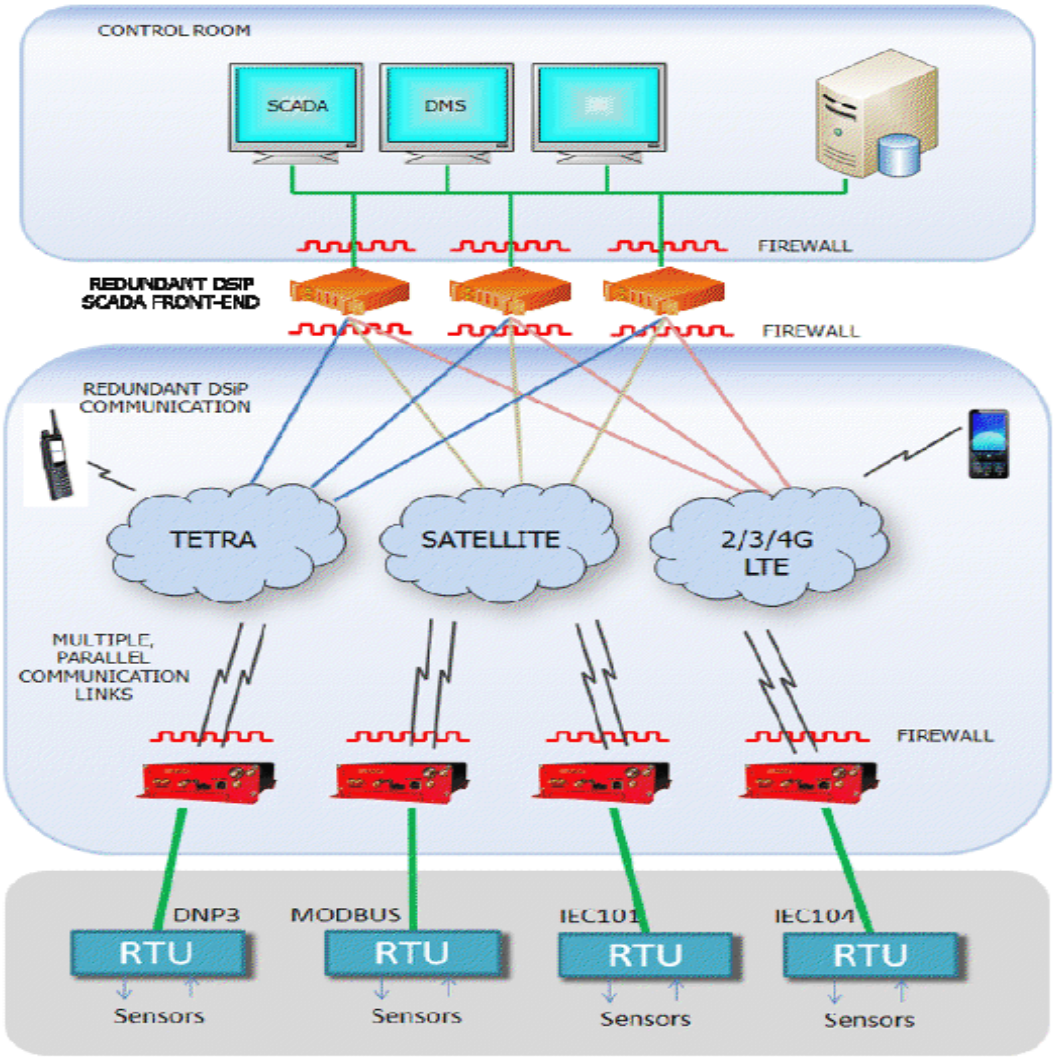

Figure 6 DSiP network principal (Ahokas at al 2012a)

For communications to be successful at the first place, it is also essential to focus on network traffic prioritizes for various communication streams. Operating without DSiP system requires

an alternative method for assuring transport priorities. To solve this issue, a suitable QoS mechanism must be implemented. Using a suitable Differentiated Services (DiffServ) scheme makes solving prioritization problem easier. The solution could be a suitable QoS management module to control traffic prioritization. Centralized management for DiffServ schemes helps managing QoS parameters. Since there are numerous services and alternative communications channels available, this cumulates to large amount of combinations for QoS classes and service levels (Orefice at al 2010). It must be noted that many of the commercial communications networks available do not honor QoS tags in IP traffic thus making it difficult to use QoS in multichannel environments. IPv6 protocol has enhancements over IPv4 with QoS features. Datagrams include QoS features, allowing better support for multimedia and other applications requiring quality of service definition.

4.4 Contribution of the Author

The first paper was written as a three students' team with almost equal shares, the author of this paper had the largest role with the deliverable. The first publication [P1] was presented by the author at a WSEAS conference at Rovaniemi in April 2012. Dr. Rajamäki inspired the team by helping in selecting the subject in the first place and he had also a contribution to the paper.

The second publication [P2] is an extend version, published in a journal, of the first publication [P1]. The author of this thesis had somewhat larger contribution to writing the paper than with the first paper. Dr. Rajamäki did not contribute any new material to this publication. The subject matter is explored in more detail and alternative solutions for securing SCADA communications are presented in the second paper. Also new issues with communications with fluctuating networks is raised compared to publication [P1].

The third publication [P3] is and extended version, also published in a journal, of Dr. Rajamäki's paper presented in Rovaniemi 2012. Valuable contribution from Dr. Tikanmäki was received in writing of this document. Dr. Rajamäki did not produce any additional material for this publication, his contribution in the extended version being from the original publication. The author of this thesis added new material to the publication thus giving the author the largest contribution of the publication.

The fourth publication [P4] is currently under review. The paper is continuing research work from the earlier papers and the authors contribution is not at the same level as with publications [P1, P2, P3].

5 Conclusions and Discussions

The main focus in this research was to find a suitable communications solution for SCADA and PPDR usage. Main results of this research was that DSiP is the most suitable for securing reliable multi-channel communications in PPDR and SCADA use cases. After comparing to other solutions and evaluating between them and DSiP the results show that DSiP can achieve the required features with minimum effort and changes to the current infrastructure. There is no need to modify existing program code and there is a possibility to use any IP based network as they exist nowadays.

All of the publications [P1, P2, P3] investigate challenges with communications in mission critical infrastructure systems. Mission critical systems are a tempting target for various attacks like DoS thus preventing monitoring and adjustment of the system or actually gaining control of a power station / power grid. Even nuclear power plants have been reported to be connected to the internet and other infrastructure systems are using default passwords with SCADA systems (INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM 2012; Thread post 2013).

During the research work we found out that some of the networks have inherited security issues, such as disturbing LTE networks relatively easily with low cost equipment. This is an important lesson to learn and shows that more than one communications network should be available all the time for critical usage scenarios.

DSiP solution is more than likely to be more expensive than a traditional single channel communications solution. The need for several communications networks and more intelligent communications hardware and software increases costs. When calculating TCO and ROI for DSiP in SCADA usage it is essential to consider how much does a one power outage cost. New and improved communications solution can shorten the power outage affecting thousands of users or even completely prevent the outage from occurring in first place. The cost savings would be considerable when compared to the initial investment costs and higher operating costs.

5.1 Discussion of the Results

Evaluation of different solutions indicated that DSiP has certain advantages compared to other solutions. It combines several advantages such as built-in network selection based on user defined parameters and QoS functionalities. Existing applications do not need to be aware of the complexity of network infrastructure connecting remote sites to the command

and control center. Also a major advantage for DSiP is the fact that applications do not need to be aware of the different network characteristics.

The publications provide a useable technological solution that is also an acceptable from business point of view. Business needs are created by people, organizations and technology (Hevner at al 2004). It can be stated that business needs are fulfilled when the system is designed to fulfill the needs of the technical requirements and usability requirements as defined by the end users.

5.2 Discussion of the Research Process

The objective of this research was to find a solution for securing SCADA and PPDR communications and increasing reliability at the same time. For this research the main focus was on analyzing and evaluating technical solutions. Actual development work was not done during the research process.

The research process was analyzed and compared to the IS research guidelines. As Hevner at al indicate the research must solve a real problem, provide contribution in the research area in question, use rigorous methods and the results must be communicated properly (Hevner at al 2004). Definition of the problem space was retrieved from the MOBI project. There was a real problem requiring study and there was previous studies covering the subject area from different angles. The research produced practical and theoretical contributions; a description of SCADA and PPDR communications, a list of acceptable solutions, comparison between solutions, the proposed DSiP solution description and discussion of further research questions. The contributions of publication P1 was presented for scientific audience at an international seminar. Publications [P2, P3] were published in a journal for the scientific audience.

5.3 Limitations

An end-to-end testing was not done during this research project. All findings are based on theoretical evaluation and comparison of the features of various solutions. A real world end-to-end testing might show some unexpected features in the DSiP solution. These might be issues with network handovers in challenging physical locations where low grade networks are the only ones available.

TCP protocol in fluctuating network situations can still cause problems with data transfer. Video surveillance applications might not react fast enough to changes in the network environment. The DSiP solution cannot by itself handle these fluctuation problems but it can help to mitigate the problem. Applications and underlying operating systems should be part of the

solution by using more advanced ACK mechanisms. Also routers, modems and such devices the communications path can provide information to the application layer regarding changes in the communications path features.

5.4 Further Research Topics

As for continuing the work in this research area a study of end to end communications testing using proposed solution should be done. A part of the required testing is currently underway at Laurea UAS using a real police vehicle with DSiP communications. Theoretical strengths and weaknesses with DSiP should be verified with extensive field testing.

TCP/IP protocol has weakness with fluctuating network characteristics, protocol and possibly applications need to be further developed. DSiP device might need some additional features for handling jitter and similar network situations. Communications with DSiP in fluctuating network should be tested and correcting actions suggested in the publications [P2, P3] should be tested and documented.

The importance of approaching IPv6 global adaption for general usage in all core IP networks should be studied more. Considering the improvements in mobility, IPSEC and QoS features with IPv6 more testing and research work is needed both for DSiP and mobility in PPDR usage in general. Some of the features new to IPv6 could change the DSiP system implementation since native IPv6 features might satisfy some of the communications requirements set for secured and reliable communication.

References

Ahokas, J., Guday, T., Lyytinen, T. & Rajamäki, J. 2012a. Secure Data Communications for Controlling Electric Power Stations and Distribution Systems. Rovaniemi: Mathematical Modelling and Simulation in Applied Sciences.

Ahokas, J., Guday, T., Lyytinen, T. & Rajamäki, J. 2012b. Secure and Reliable Communications for SCADA Systems. INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, p ISSN: 2074-1294, p. 167-174.

Ahokas, J. Rajamäki, J. & Tikanmäki I. 2012. Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations. INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, ISSN: 2074-1294, p. 120-127.

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

Dahlman, E., Parkval, S., Sköld, J. & Beming, P. 2008. 3G Evolution: HSP and LTE for mobile Broadband.

Daneels, A. & Salter, W. 1999. What is SCADA?. International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy.

Ferreira, H. C., Lampe, L., Newbury, J. & Swart, T.G. 2010. Power Line Communications: Theory and Applications for Narrowband and Broadband Communications over Power Lines. United Kingdom. John Wiley & Sons.

Hevner, A., March, S., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. MIS Quarterly. Volume. 28 Issue.1.

Holmström, J., Rajamäki, J. & Hult, T. 2011. DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication. In Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canary, Canary Islands Spain, March.

Holmström, J., Rajamäki, J. & Hult T. 2011. The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication. International Journal of Communications, Issue 3, Volume 5.

Hult, T. & Rajamäki, J. 2011. ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project. 10th WSEAS International Conference on Applications of Computer Engineering, Playa Meloneras, Gran Canary, Spain, March 22-26.

Korhonen, J. 2003. Introduction to 3G Mobile Communications. Arctech House Publishers.

Lee, A. 1999. Inaugural Editor's Comments. MIS Quarterly (23:1), March

Maini, A. & Agrawal, V. 2011. Satellite Technology: Principles and Applications.

Nunamaker, J., Minder, C. & Purdin, T. 1991. Systems Development in Information System Research.

Orefice, J. P., Paura, L. & Scarpiello, A. 2010. Inter-vehicle communication QoS management for disaster recovery. The Internet of Things, 20th Tyrrhenian Workshop on Digital Communications, Springer, New York.

Park, H. G., Shin, B., Park, H. K., Park, J., Yoon, C., Rho, S., Lee, C., Jang, J., Jung H. & Lee, Y. 2010. Development of Ad hoc Network for Emergency Communication Service in Disaster Areas. Proceedings of the 9th WSEAS International Conference on APPLICATIONS of COMPUTER ENGINEERING.

Rajamäki, J., Ahokas, J., Rathod P. 2013. Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System. 2nd International Conference on INFORMATION TECHNOLOGY and COMPUTER NETWORKS (ITCN '13). Antalya, Turkey October 8-10, 2013. Under review.

Rajamäki, J., Holmström, J. & Knuuttila, J. 2010. Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT).

Ryu, J. 2011. Congestion Control and Routing over Challenged Networks. The University of Texas at Austin.

Stavroulakis, P. 2007. Signals and communication technology, Terrestrial Trunked Radio-TETRA, A Global Security Tool. Springer.

Electronic References

ETSI Project MESA: Services and Applications SoR - TS 170.001 V3.3.1. Referred on 26.02.2013. http://www.etsi.org/about/our-global-role/mesa

ICS-CERT Monitor October-December. Referred on 12.05.2013. http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf

MACICO project information. Referred on 11.09.2012. http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

NERC Standard CIP-002-3 through -009-4, Cyber Security, 2009-2012 Retrieved November 10, 2012, from North American Electric Reliability Council (NERC), Critical Infrastructure Protection Committee. Referred on 16.01.2013. http://www.nerc.com/page.php?cid=2|20

Office of Emergency Communications, "Nationwide Public Safety Broadband Network", USA, 2012 The U.S. Department of Homeland Security (DHS). Referred on 16.05.2013. http://www.dhs.gov/sites/default/files/publications/Fact%20Sheet_Nationwide%20Public%20Safety%20Broadband%20Network.pdf

SCADA information. Referred on 16.12.2012.: http://www.scadasystems.net , http://www.controlmicrosystems.com/resources-2/faqs/scada11/

Thread Post. Referred on 10.05.2013. http://threatpost.com/shodan-search-engine-project-enumerates-internet-facing-critical-infrastructure-devices-010913/

Wireless @ Virginia Tech, "A brief response to the FirstNet NOI regarding the conceptual network architecture. ", USA, 2012 Wireless@ Virginia Tech. Referred on 16.05.2013. http://www.ntia.doc.gov/files/ntia/va_tech_response.pdf

Appendices

Appendix 1: Publication [P1], Secure Data Communications for Controlling Electric Power Stations and Distribution Systems
Appendix 2: Publication [P2], Secure and Reliable Communications for SCADA Systems
Appendix 3: Publication [P3], Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations
Appendix 4: Publication [P4], Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System

Publication P[1]

P[1] J. Ahokas, T. Guday, T. Lyytinen, J. Rajamäki, Secure Data Communications for Controlling Electric Power Stations and Distribution Systems, 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12), Proceedings Title: Mathematical Modelling and Simulation in Applied Sciences, Series Title: Mathematics and Computers in Science and Engineering Series | 1, Rovaniemi, Finland, Apr 18-20, 2012, ISSN: 2227-4588, ISBN: 978-1-61804-086-2, pp. 108-113, Paper URL: http://www.wseas.us/e-library/confernces/2012/Rovaniemi/INEE/INEE-00.pdf, Publisher: WSEAS Press

Secure Data Communications for Controlling Electric Power Stations and Distribution Systems

JARI AHOKAS, TEWODROS GUDAY, TEEMU LYYTINEN & JYRI RAJAMÄKI
LaureaSID
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 ESPOO
FINLAND
{jari.ahokas, tewodros.guday, teemu.lyytinen, jyri.rajamaki} @laurea.fi http://laureasid.com

Abstract: - Uninterrupted electric power distribution is vital for modern society. One of the key components is electric power stations and distribution systems. SCADA systems are used for controlling the power stations. SCADA systems have traditionally used propriety communication networks. For added electrical power station security, a video surveillance is required. Current telecommunication networks used for SCADA systems don't support speeds required for real time video. A standard Internet connection does not offer required reliability and security for SCADA communications. Multi-Agency Cooperation In Cross-border Operations (MACICO) project aims to produce a new way of combining multiple telecommunication channels, such as TETRA, satellite and 2G/3G/4G networks. A certain target is to create a single redundant secure and faster data transfer path for SCADA and video surveillance systems. In Finland there is a project starting utilizing new technologies for data transfer thus demonstrating usability and reliability of this new communication method.

Key-Words: - Data communications, Critical infrastructure protection, Electrical power station, ICT, Professional mobile radio, Public safety, SCADA

1 Introduction

Electricity generation, transmission and distribution compose a critical infrastructure, which is essential for the functioning of a society and economy. Power stations are very important components for the whole power distribution network. Data transfer between control centers and power stations is critical for controlling and protecting power distribution. Earlier data transfer has only been control signaling between control program (Supervisory Control and Data Acquisition, SCADA) and power station components.

For security reasons a surveillance video system is required. Also perimeter monitoring adds to enhanced security. Live video stream from power stations is coming more and more important because of several security threats against the system. These threats include, but are not limited to: terrorism, vandalism, natural phenomenon (like storms), wild animals etc.

Also video stream needs a secure and reliable connection to command and control rooms. This paper introduces a new way of approaching this problem by combining two previously separate data transfer systems. By connecting these separate channels together, a more fault resistant system is achieved.

This paper presents the Multi-Agency Cooperation In Cross-border Operations (MACICO) project. One of MACICO's targets is to provide a solution for communications problem between power stations and control rooms.

1.1 Current Situation

Currently electric companies use propriety communication channels together with standard public use Internet connections. Traditional radio communications has limitations regarding signal quality, distance and reliability. Standard Internet connections, such as ADSL, do not offer Quality of Service (QoS) capabilities.

An electric company from Southern Finland has used a normal ADSL connection with VPN tunneling devices for SCADA communication and video surveillance for four years. This solution did work but it lacked QoS capabilities and did not offer any backup connection possibilities. It showed that the required technology exists and it works but there were still major limitations for mission critical usage.

2 Applicable Technologies

In order to provide reliable data transfer with a secure communication system, a proper applicable technologies need to be available.

In the following part we will see SCADA and surveillance video systems and their needs for data transfer systems.

2.1 SCADA- Systems

Supervisory Control and Data Acquisition (SCADA) generally refers to the control system of the industry, where SCADA is a computer system that controls and monitors a process. This process can be infrastructure, facility or industrial based. [1], [2]

SCADA systems are also used for monitoring and controlling physical processes like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society. [1], [2]

SCADA protocols consist of Conitel, Profibus, Modbus RTU and RP-570. Standard protocols mainly are IEC 61850, DNP3 and IEC 60870-5-101 or 104. These protocols of communication can be recognized, standardized and most of these protocols contain extensions for operating over the TCP/IP. [1], [2]

SCADA networks provide great efficiency and are widely used. However, they also present a security risk. SCADA networks were initially designed to maximize functionality with only little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak. This makes some SCADA networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure. Action is required by all organizations, government or commercial, to secure their SCADA networks as part of the effort to adequately protect the nation's critical infrastructure. The two major categories to improve the security of its SCADA network are specific actions to improve implementation and actions to establish essential underlying management processes and policies. Further information how to improve the security of its SCADA network is available from the US President's Critical Infrastructure Protection Board, and the Department of Energy. [3]

2.2 Video Surveillance System

Video surveillance is probably the most common tool used for protection of various types of assets against intentional or unintentional damage or theft. The largest usage segment is the retailing business, where video cameras are used for loss prevention. Other important segments are corporate offices, public buildings such as museums and all other places where valuable goods can be seized or harmed. Outdoors, video surveillance is used for example in prevention of car thefts and vandalism such as graffiti. Nowadays, video surveillance systems are used also for such purposes like space missions and boarder frontier guard [5]. With the help of video surveillance system, it can be achieved monitoring, tracking and classified the needed target activities.

2.3 Communication Systems Operating in Sparsely Populated Area

Many electric power stations are located in sparsely populated areas, where the coverage of telecommunication networks could be poor. In order to send information from a rural area to post processing, there are many different data transfer network systems. From fixed connections to commercial Mobile Networks, satellite communication and TETRA Networks are used to transfer data from sparsely populated areas.

The Global System for Mobile communications (GSM) is a wireless telecommunications standard for digital cellular services that can be used for a communication system in sparsely populated areas. The original standard was optimized for voice communications and provided only circuit-switched data connections at a bit rate of 9.6 kbps and a short messages service (SMS). Later enhancements made higher bit rates and packet switched data possible. GSM is based on TDMA technology. Although the roots of GSM are European, GSM is nowadays the biggest standard used for the 2nd generation of mobile communications. The success of GSM made roaming in big parts of the world possible. [5]

The General Packet Radio Service (GPRS) is a technology for the support of packet switching traffic in a GSM network. GPRS enables high-speed wireless Internet and other data communications in GSM. The data speed of GPRS is more than four times greater speed than conventional GSM systems. Using a packet data service, subscribers are always connected and always on line so services will be easy and quick to access. In GSM the maximum data rate is 9.6 kbps per time slot. In GPRS the data is packetized which gives in principle an even lower data rate of 9.05 kbps of

which 8 kbps is available for the user. However, in GPRS there are two technologies introduced to increase this data rate. Firstly, the error correction that is used can be adapted to the quality of the radio channel. Secondly, it is possible to use more than one time slot. In theory all 8 time slots can be used. [5]

3G is an abbreviation for the 3rd Generation system for mobile communications. 3G consists of a family of standards under the framework of International Mobile Telecommunications for the year 2000 (IMT-2000). Under this framework, a number of standards are developed. The European version is known as The Universal Mobile Telecommunications System (UMTS). The main other standards are CDMA2000 and Mobile WiMax. The third generation is typified by the convergence of voice and data with mobile Internet access, multimedia applications and high data transmission rates. The 3rd generation must make worldwide roaming possible. [5]

3GPP LTE or 3G LTE (Long Term Evolution) is the 3GPP work item on the long term evolution (LTE) of the air interface of UMTS (evolved UTRA) and its associated radio access network (evolved UTRAN). LTE will offer even higher peak data rates with a reduced latency. LTE will be a completely packet-optimized radio-access technology. 3GPP LTE improves spectral efficiency, allowing for a large increase in system capacity and reduced cost per gigabyte. This will lead to the ability to offer more services with better user experience. [5]

Terrestrial Trunked Radio (TETRA) is an open digital radio standard for professional mobile radio. TETRA can be used by a company for the communication with the mobile work forces (Private Mobile Radio; PMR) as well as by an operator to offer the same services on a commercial basis (Public Access Mobile Radio; PAMR). A third group of users are the Emergency Services (such as police and fire departments). The TETRA radio standard is defined by ETSI European Telecommunications Standards Institute. TETRA is based on radio channels with a bandwidth of 25 kHz. Each channel is subdivided in 4 traffic channels using Time Division Multiple Access TDMA. The traffic channels can be used for both voice and data. The maximum bit rate is 28.8 kbps if all 4 traffic channels are joined together for one data connection. Mainly the frequency band 410-430 MHz is used for civil systems in Europe. TETRA is used in the 380-385/390-395 MHz band for emergency services. In some countries civil systems use the whole or parts of the 380-400 MHz band. [5], [6]

C-band (Comprise) is a portion of the microwave band ranging from 4-8 GHz, and a wavelength of around 5 cm. The C-band is commonly used by communications satellites. Downlink frequencies (space to earth) are around 4 GHz and uplink frequencies (earth tot space) around 6 GHz. The band is also used for radar, including weather radar, and Radio LAN in the 5 GHz range. [5]

Broadband Global Area Network (BGAN) is a new satellite network from The International Mobile Satellite Organization. BGAN will offer transmission speeds of theoretically up to 492 kbps. Actual data rates will be lower, depending on the satellite terminal used. BGAN will offer both voice and data services. BGAN supports both packet switched services based on IP as well as traditional circuit switched services. BGAN uses the new series of Inmarsat-4 satellites. BGAN offers coverage around the whole globe with the exception of the Polar Regions and parts of the Pacific Ocean. Services will be offered to land-based, airborne and maritime users. [5]

2.4 Distributed Systems intercommunication Protocol (DSiP)

Distributed Systems intercommunication Protocol (DSiP) system allows for combining all kinds of telecommunication resources into a single, uniform and maintainable system. [7]

The DSiP solution makes communication reliable and unbreakable. DSiP uses several physical communication methods in parallel. Applications, equipment and devices believe they communicate over a single unbreakable data channel. Satellite, TETRA, 2G, 3G, 4G/LTE, VHF-radios etc. can be used simultaneously in parallel. DSiP is suitable for a vast range of applications. [8], [9] Power Grid Control, SCADA and Public Safety communication are only a few examples.

3 MACICO Research Project

In recent years, the capabilities of Critical Infrastructure Protection (CIP) and Public Safety (PS) organizations across Europe have been considerably improved with the deployment of new technologies including dedicated TETRA and TETRAPOL networks. CIP and PS organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe to empower joint responses to

threats and crisis in an increasingly interconnected network, but also security organizations have to benefit from interoperability functionality in their day-to-day work.

An international research project 'Multi-Agency Cooperation In Cross-Border Operations (MACICO)' aims at developing a concept for interworking of critical infrastructure protection and public safety organizations in their daily activity. MACICO's main goal is addressing in a short-term perspective the needs for improved systems, tools and equipment for radio communication in cross-border operations as well as during operations taking place on the territory of other member states (high scale civil crisis operations or complex emergencies needing support of Public Safety Services from other Member States). On the other hand, MACICO encompasses the interoperability issues European countries will be faced to in a long-term perspective, tackling the necessary transition between currently deployed legacy network and future broadband networks. [10]

3.1 Contribution to the Celtic

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new "Smart Connected World" paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the inter-governmental EUREKA network. [11]

EUREKA 'Clusters' are long-term, strategically significant industrial initiatives. They usually have a large number of participants, and aim to develop generic technologies of key importance for European competitiveness. Celtic is a EUREKA cluster project that carries out projects in the domain of integrated telecommunications systems. [11]

MACICO project aims to develop the interoperability between Professional Mobile Radio communication systems. Through this new feature required by end users, the ultimate goal is to integrate all the current deployed PMR systems within an integrated and secured network.

MACICO will build on existing and promote a standardization of the interface between TETRA and TETRAPOL networks, interface that will be reused for the connection and the migration to future broadband networks. MACICO facilitates the vertical integration of the telecommunications systems dedicated to public safety within an end-to-end architecture and the horizontal integration between themselves via standardized interfaces, which is completely in line with the Celtic Integrated Telecommunications System approach as defined in the Celtic Purple Book.

MACICO focuses on the development of integrated system to enhance public safety communication, the work will include the open interface for interoperability that could be considered as a part of Pan European Lab concept promoted by Celtic (but in the Public Safety frame); The project will look at the new system concept of heterogeneous PMR network and will facilitate the introduction of new services for public safety; All these concepts are at the core of the Celtic Pan-European Laboratory and will enable the trial and evaluation of service concepts, technologies and system solutions.

3.2 Work Packages

MACICO research project contains six Work Packages (WPs). The project starts by collecting end-user requirements (WP2). Architecture and Standard operating procedures design and definition outcomes (WP3) will feed the work packages dealing with Implementation for multi-agency interoperability (WP4) and architectural design for the Demonstration (WP5) of use cases. WP6 includes Dissemination of the project achievements and findings outside the consortium to the larger public audience. The whole project coordination and management is taken care by WP1.

3.3 The Finnish Contribution

The impact of the Finnish partners of the MACICO project will produce services that enhance the international competitiveness of companies, society and other customers at all stages of their innovation process.

The Finnish partners will promote the realization of innovative solutions and new businesses by foreseeing already in the strategic research stage the future needs of their customers. The Finnish partners will creatively combine their multidisciplinary expertise with the knowledge of the partners.

The Finnish partners will develop a use case called Interoperability of TETRA and 4G/LTE. The use case is driven by Cassidian Finland Ltd. and other main contributors are Ajeco Ltd. and Laurea University of Applied Sciences. Electric power stations will be an area, where the interoperability will be demonstrated. Additional to the main goal, also interoperability between other networks will be tested, as shown in Fig. 1. In addition to this, the use case will include new data communication needs for video surveillance of electric power stations.

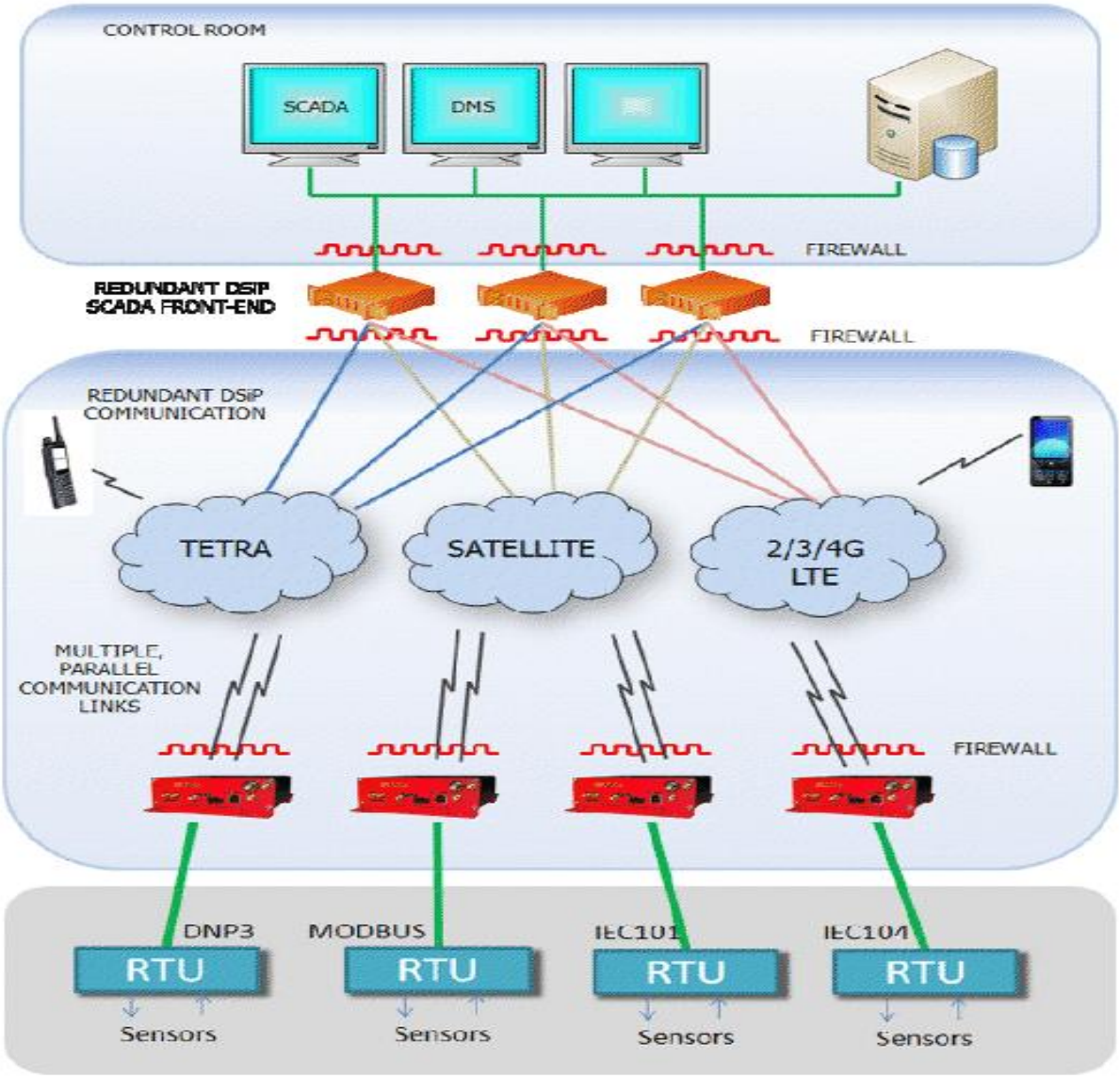

Fig. 1 Fully Redundant Multichannel SCADA Communication Network

This use case addresses secure and reliable telecommunication power grid applications. The need for secure and reliable communication among power utility customers is divided; on one hand the communication from the control system (SCADA) to the remote terminal units (RTU's) on the field, must be reliable and on the other hand, there is a need for performing site monitoring for detecting physical intrusion for example. In this use case will be implemented a communication system capable of sharing the available communication resource between SCADA-command and control messaging and site surveillance as shown in Fig. 2.

The communication solution must be able to vividly adopt itself to changes in the underlying data transport layers e.g. services of the communication solution must be controllable according to available bandwidth of a communication channel. Another very important task is to control the priorities of the transported messages; Site surveillance and SCADA-command & control must be thoroughly contemplated before implementation.

This use case aims at creating a multichannel communication resource from a control room to an electrical power substation. The communication solution will implement SCADA-command and control messaging in parallel with CCTV and other surveillance and monitoring. The aim of this use case is to provide an easily implementable uniform communication solution which will take into account the needs of a smart-grid system, command and control of an electrical substation and site surveillance and perimeter monitoring.

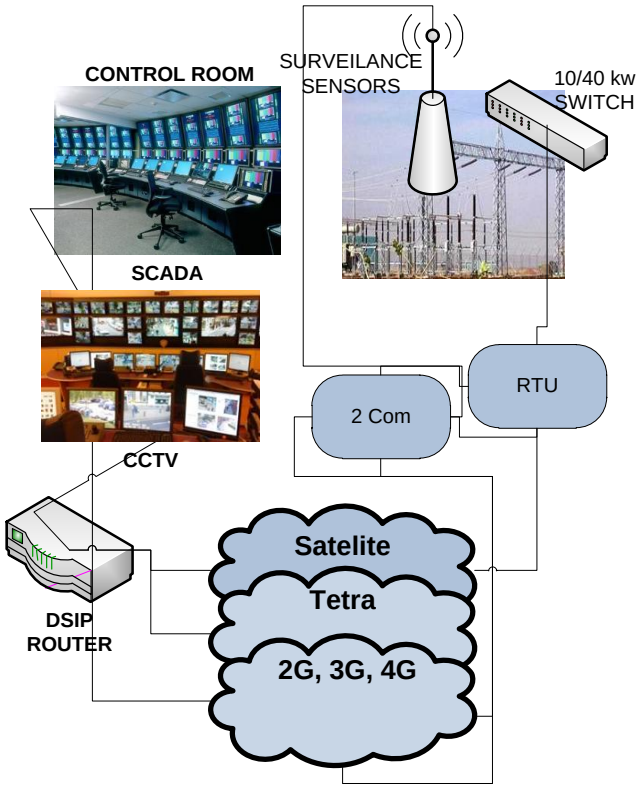

Fig. 2 Secure Communications for Multinational Electricity Supply Deployment

3.4 Current Situation

MACICO is a large project with many participants all over Europe. This causes many requirements for project management and funding requires arrangements in several countries. This project is expected to be completed by the year 2014. The current situations of the MACICO project is that Switzerland has dropped out form the project, whereas Finland, France and Spain have arranged national funding. The kick-off meeting of the project is held in December 2011.

4 Conclusions

The military (MIL), public protection and disaster relief (PPDR) as well as critical infrastructure protection (CIP) actors have multiple similar needs. Electricity generation, transmission and distribution compose a critical infrastructure, which is essential for the functioning of a society and economy. SCADA systems are used for controlling the electric power stations. For added electrical power station security, a video surveillance is required. Current telecommunication networks used for SCADA systems don't support speeds required for real time video. The Multi-Agency Cooperation In Cross-border Operations (MACICO) project aims to produce a new way of combining multiple telecommunication channels, such as TETRA, satellite and 2G/3G/4G networks. A certain target is to create a single redundant secure and faster data transfer path for SCADA and video surveillance systems.

In the future, a common cyber secure voice and data network for MIL, PPDR and CIP brings synergy and enables interoperability; separate networks are wasting of resources.

References:

[1] SCADA, http://www.scadasystems.net/, http://www.controlmicrosystems.com/resources-2/faqs/scada11/

[2] A. Daneels and W. Salter, "What is SCADA?" International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy, 1999.

[3] 21 Steps to Improve Cyber Security of SCADA Networks. http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf

[4] Intelligent Distributed Video Surveillance System. Edited by S.A Velastin and P.Remaginio. Institution of Electrical Engineers, London 2006.

[5] Telecommunications and internet directory http://www.telecomabc.com/

[6] TETRA: http://www.etiworld.com/tetra.pdf

[7] J. Holmstrom, J. Rajamaki and T. Hult, "The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication", International Journal of Communications, Issue 3, Volume 5, 2011.

[8] J. Rajamäki, J. Holmström and J. Knuuttila, "Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities", Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT) 2010, IEEE Xplore,

[9] J. Holmstrom, J. Rajamaki & T. Hult, "DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication" in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 2011

[10] MACICO project information, http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp

[11] Celtic-Plus http://www.celticplus.eu/

Publication P[2]

P[2] J. Ahokas, T. Guday, T. Lyytinen, J. Rajamäki, Secure and Reliable Communications for SCADA Systems, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, p ISSN: 2074-1294, p. 167-174, Paper URL: http://naun.org/multimedia/UPress/cc/16-296.pdf, Publisher: NAUN Press

Secure and Reliable Communications for SCADA Systems

Jari Ahokas, Tewodros Guday, Teemu Lyytinen and Jyri Rajamäki

***Abstract*—**Uninterrupted electric power distribution is vital for modern society. Secure data transfer between control center and power stations is critical for controlling and protecting power distribution. Supervisory Control and Data Acquisition (SCADA) systems are used for controlling the power stations. SCADA systems have traditionally used a limited propriety communication networks to transfer only control signals between centralized control systems and power stations. To improve security and reliability of an electrical power distribution, a video surveillance is required at power stations and distribution centers. Current telecommunication networks used for the SCADA system does not provide required capacity for real time video streaming. A standard Internet connection does not offer required reliability and security for SCADA communications. Multi-Agency Cooperation In Cross-border Operations (MACICO) project aims to produce a new way of combining multiple telecommunication channels, such as TETRA, satellite and 2G/3G/4G networks to create a single redundant secure and faster data transfer path for SCADA and video surveillance systems. The project relies on the Distributed Systems intercommunication Protocol (DSiP) that allows combining all kinds of telecommunication resources into a single, uniform and maintainable system. In Finland there is a project starting utilizing new technologies for data transfer thus demonstrating usability and reliability of this new communication method.

***Keywords*—**Data communications, Critical infrastructure protection, Professional mobile radio, Public safety, SCADA, Distributed Systems intercommunication Protocol, DSiP

I. Introduction

Electricity production, transmission and distribution compose a critical infrastructure, which is essential for the functioning of a society and economy. Power stations are very important components for the whole power distribution network. Data transfer between control centers and power stations is critical for controlling and protecting power distribution. Earlier data transfer has only been control signaling between control program Supervisory Control and Data Acquisition (SCADA) and power station components.

For security reasons a surveillance video system is required. Also perimeter monitoring adds to enhanced security. Live video stream from power stations is coming more and more important because of several security threats against the system. These threats include, but are not limited to: terrorism, vandalism, natural phenomenon (like storms), wild animals etc.

Also the video stream from the power stations requires a secure and reliable connection to the command and control rooms. This paper introduces a new way of approaching this problem by combining two previously separate data transfer systems. By connecting these separate channels together, a more fault resistant system is achieved.

This paper presents the Multi-Agency Cooperation In Cross-border Operations (MACICO) project. One of MACICO's targets is to provide a solution for communications problems between power stations and control rooms.

Other possibilities for delivering secure are reliable communications solution are presented in this paper but these solutions do not offer the same level of functionality in a single solution as in the DSiP solution presented in this paper. Some of the possible problems and issues to be considered are introduced such as TCP vertical handoff challenges to applications. TCP protocol has challenges with fluctuating networks and applications must be aware of this and TCP protocol enhancements are also available to tackle the problem.

A. Current situation

Currently electric companies use propriety communication channels together with standard public use Internet connections. Traditional radio communications has some limitations regarding signal quality, distance and reliability. Standard Internet connections, such as ADSL, do not offer Quality of Service (QoS) capabilities.

An electric company from Southern Finland has used a normal ADSL connection with VPN tunneling devices for SCADA communication and video surveillance for four years. This solution did work but it lacked QoS capabilities and did not offer any backup connection possibilities. It showed that the required technology exists and it does work but there were still major limitations for mission critical usage.

The power station used with communications testing is located in densely populated area and can be easily accessed by the power company employees if there are problems connecting the power station. New communications methods could be tested because an alternative method of monitoring and controlling the power station were easily available if the experiment failed.

Manuscript received May 20, 2012. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Ahokas, T. Guday, T. Lyytinen and J. Rajamäki are with Laurea University of Applied Sciences, Vanha Maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail: jari.ahokas@laurea.fi, tewodros.guday@laurea.fi, teemu.lyytinen@laurea.fi and jyri.rajamaki@laurea.fi.

II. Applicable Technologies

In order to provide reliable data transfer with a secure communications system, a proper applicable technologies need to be available for deployment.

In the following part we will see more detail information on SCADA and surveillance video systems and their requirements for data transfer systems.

A. SCADA-Systems

Supervisory Control and Data Acquisition (SCADA) generally refers to the control system of the industry, where SCADA is a computer system that controls and monitors a process. This process can be infrastructure, facility or industrial based [1], [2].

SCADA systems are also used for monitoring and controlling physical processes like distribution of water, traffic lights, electricity transmissions, gas transportation and oil pipelines and other systems used in the modern society [1], [2].

SCADA protocols consist of Conitel, Profibus, Modbus RTU and RP-570. Standard protocols mainly are IEC 61850, DNP3 and IEC 60870-5-101 or 104. These protocols of communication can be recognized, standardized and most of these protocols contain extensions for operating over the TCP/IP [1], [2].

A SCADA system consists of a number of Remote Terminal Units (RTUs) collecting field data and sending data back to a master station via a communications system. The master station displays the scquired data and also allows the operator to perform remote control tasks. The accurate and timely data allows for optimixation of the plant operation and process. A further benefits is more efficient, reliable and most importantly, safer operation [3].

An RTU is a stand-alone data acquisition and control unit, generally microprocessor based, that monitors and controls equipment at a remote location. Its primary task is to control and acuire data from process equipment at the remote locationa and to transfer this data back to a central station. It generally also has the facility for having its configuration and control programs dynamically downloaded from some central station [3].

SCADA software can be divided into two types, properietary or open. Companies developed proprietary software to communicate to their hardware. These systems are sold as “turn key” solutions. Open software systems have gained popularity because of the interoperability they bring to the system. Interoperability in this case is the ability to mix different manufacturers’ equipment on the same system [3].

Communications in a SCADA system will generally have a structure where some stations may be identified as master stations, and others as slave stations, sub-master stations, or outstations. In a hierarchical structure, there may be some devices that can act both as slave stations and master stations [3].

One of the important SCADA features of DNP3 is that it provides time-stamping of events. Time stamping DNP3 provides resolution of events to one-millisecond. For events to match up correctly across the system, it is essential that clocks at all out-stations are synchronized with the master station clock [3].

B. Video Surveillance System

Video surveillance is probably the most common tool used for protection of various types of assets against intentional or unintentional damage or theft. The largest usage segment is the retailing business, where video cameras are used for loss prevention. Other important segments are corporate offices, public buildings such as museums and all other places where valuable goods can be seized or harmed. Outdoors, video surveillance is used for example in prevention of car thefts and vandalism such as graffiti. Nowadays, video surveillance systems are used also for such purposes like space missions and boarder frontier guard. With the help of video surveillance system, it can be achieved monitoring, tracking and classified the needed target activities.

Video surveillance can be quite hideous task for an operator to monitor at the command and control center. This task is easier if there is a technical solution in use for controlling how much data or live video stream is shown to the operator in general. An event driven video surveillance system can help dealing with this problem of too much information on the video monitors. Event driven video monitoring is a system that shows an alert only when an interesting event has occurred in the video stream from any of the cameras covering the monitored area [4].

Video coding specification was developed by the Motion Picture Experts Group (MPEG) as a standard for coding image sequences to a bit of about 1.5 Mbit/s for MPEG-1 and 2 to 8 Mbit/s for MPEG-2. MPEG-1 applies to non-interlaced video while MPEG-2 was ratfied in 1995 for broadcast (interlaced) TV transmissions. The lower rate was developed, initially, for 352 x 288 pixl images because it is compatiable with digital storage devices. The algorithm is delibertely flexibile in operation, allowing different image resolution, compression rations and bit rates to be achieved [5].

MPEG-4 is a standard for interactive multimedia applications. Key objectives of MPEG-4 video coding are to be tolerant of or robust to transmission network errors, to have high interactive functionality (e.g. for audio and video manipulation) to allow accessing or addressing of the stored data by content. Thus it is able to accept both natural (pixl based) and synthetic data and, at the same time, archieve a high compression effeciency. It aslo facilitates transmission over mobile telephone networks and the Internate at rates of 20 kbt/s to 1 Mbit/s.

MPEG-4 uses contents based coding where the video images are separated or partitioned into objects such as background, moving person, text overlay, etc. Video data representing each of these video objects (Vos) in then separeted out and encoded as a separate layer or video object plane (VOP) bit stream which includes shape, transparency, spatial coordinates, i.e. location data, etc. relevant to the video object. Objects are selected from video sequence using, for example, edge detection techniques [5].

In video data transfer UDP protocol is more efficient than TCP because virtually no handshaking and transmission control is in use compared to TCP protocol. Other advantage

is that if packet loss occurs, video stream is not affected severely and UDP protocol does not use retransmissions.

C. Communication Systems Operating in Sparsely Populated Area

Many electric power stations are located in sparsely populated areas, where the coverage of telecommunication networks could be poor. In order to send information from a rural area to post processing, there are many different data transfer network systems. From fixed connections to commercial Mobile Networks, satellite communication and Terrestrial Trunked Radio (TETRA) Networks are used to transfer data from sparsely populated areas.

GSM intially designed as a pan-European mobile communication network, not shortly after the successful start of the first commercial networks in Europe, GSM systems were also deployed on other continents. In addition to GSM networks that operate in the 900 MHz frequency band, others so-called Personal Communications Networks (PCNs) and Personal Communication Systems (PCSs) are in operation. They use frequencies around 1800 Mhz, or around 1900 MHz in North America [6].

General Package Radio Service (GPRS) is enabling improved data rate performance by allowing for more that one GSM timeslot to be used by a terminal for a service at a time. The driving factor for new (and higher brandwidth) data service obviously is wirless access to the Internet [7].

The third-Generation (3G) mobile communication networks known as the Universal Mobile Telecommuniaction System (UMTS) in Europe and as the international Mobile Telecommunication System 2000 (IMT2000) worldwide, have already been introduced [7].

The second-generation (2G) mobile system uses digital radio transmission for traffic. The 2G networks have much higher capacity than the first-generation systems. There are four main standards for 2G systems: Global Systems for Mobile (GSM) communication and itse derivateives; digital AMPS (D-AMPS); code-division multiple access (CDMA) IS-95; and personal digital cellular (PDC) [6]. The 2G networks are close to their end of life cycle.

The Third-Generation Partnership Project (3GPP) is the standard-developing body that sepecfies the 3G UTRA and GSM systems. 3GPP is a partnership project formed by the standard bodies ETSI, ARIB, TTC, TTA, CCSA and ATIS. 3GPP consists of several Technical Specifications Groups (TSGs).

The 3GPP Long-Term Evolution is intended to be a mobile-communication system that can take the telecom industry in to the 2020s. The philosophy behind LTE standardaization is that the competence of 3GPP in specifying mobilecommunication systems in general and radio interfaces in particular shall be used, but the result shall not be restricted by previous work in 3GPP. Thus, LTE technology does not need to backward compatible with older WCDMA and HSPA technologies [8].

TETRA is an open digital radio standard for professional mobile radio. TETRA can be used by a company for the communication with the mobile work forces (Private Mobile Radio; PMR) as well as by an operator to offer the same services on a commercial basis (Public Access Mobile Radio; PAMR). A third group of users are the Emergency Services (such as police and fire departments).

The TETRA radio standard is defined by ETSI European Telecommunications Standards Institute. TETRA is based on radio channels with a bandwidth of 25 kHz. Each channel is subdivided in 4 traffic channels using Time Division Multiple Access TDMA. The traffic channels can be used for both voice and data. The maximum bit rate is 28.8 kbps if all 4 traffic channels are joined together for one data connection [6].

Identifying the elements on which a comparison of the requirements with its special features of the evolving standards and the improvement that are possible for TETRA, that TETRA can play a major role in the next generations of Private Wirless System PMR systems. TETRA system can be improved to become a unique tool for security [9]. Private Wireless System can extend to cover mobile video, voice and data transmission simultaneous as low as 640 kpps data [9].

Average TETRA cells are remarkably larger than GSM cells. Firstly, TETRA uses typically a frequency of 400MHz, while GSM uses 900 or 1800MHz. The propagation losses are theoretically proportional to the square of the frequency. Secondly, commercial networks are typically capacity driven and PSS networks with less users are coverage driven. This means that population density usually determines cell size in GSM [9].

The TETRA system uses end-to-end encryption in addition to the air interface encryption to provide enhanced security. End-to-end encrypted continuous data, such as video, requires synchronization of the key streem at the reciever to the incoming encrypted data streem from the transmitter. Apart from the video coding synchronisation mechanisms (e.g. MPEG-4, H.263), the TETRA system uses a synchronization technique known as frame stealing to providing synchronization to end-to-end encrypted data [9].

A satellite is often reffered to as an “orbit radio star” for reasons that can be easily apprciated. These so-called orbiting radio stars assist ships and aircraft to navigate safely in all weather conditions. The sitellite-based global positioning system (GPS) is used as an aid to navigate safely and securely in unknown territories [10].

A satellite in general is any natural or artificial body moving around a celestial body such as planets and stars. In the present context, reference is made only to artificial satellites orbiting the planet Earth. These sattlites are put into the desired orbit and have payloads depending upon the intended application [10].

A satellite while in the orbit performs its designated role throughout its lifetime. A communication satellite is a kind of repeater station that recieves signals from ground, processes them and then retransmits them back to Earth. An Earth observation satellite is a photographer that takes pictures of regions of interest during its periodic motion [10].

D. Distributed Systems intercommunication Protocol (DSiP)

Distributed Systems intercommunication Protocol (DSiP) system allows for combining all kinds of telecommunication resources into a single, uniform and maintainable system [11].

The Next Generation Network (NGN) enables users seamlessly access heterogeneous networks (including ad hoc

networks) for reaching a common IP-based core network. Some critical issues are to be faced in order to allow data sharing among different networks, related to items such as Access Control and Command and Control. Intense research activity on this topic has been promoted in recent years [12], [13] and network level solutions have been suggested [14].

The DSiP solution makes communication reliable and unbreakable. DSiP uses several physical communication methods in parallel. Applications, equipment and devices think that they communicate over a single unbreakable data channel. Satellite, TETRA, 2G, 3G, 4G/LTE, VHF-radios etc. can be used simultaneously in parallel. DSiP is suitable for a vast range of applications [15], [16]. Power Grid Control, SCADA and Public Safety communication are examples.

The DSiP solution brings several benefits to communications. For example better data security, integrity & priority. Immunity towards virus infusion and DoS network attacks with intrusion detection. For communications there are data-flow handshaking and flow-control systems implemented with automatic re-routing. Early detection of communication problems helps minimizing communication disruptions because the change of the communication channel can occur earlier.

Other benefits include: authentication- and management tools, controllable data casting and compression, interfacing capabilities to equipment and software. For communications DSiP offers: transparent tunneling of any data, cost-efficient network topology, insulation from Internet-system flaws and routing according to lowest cost and/or shortest hops.

Critical networks and communication solutions require efficient management and monitoring tools. The DSiP solution contains several modules for support, maintenance and configuration.

Authentication Server Software: The DSiP features centralized and mirrorable Authentication Server software. This software allows for editing passwords for DSiPnodes. The nodes may have passwords that expire after a specific time for security reasons. Nodes may be allowed in the DSiP routing system and they may be excluded from it at any given time.

Configuration Server Software: The Configuration Server software is an entity for providing routing instructions and firmware updates to nodes. Nodes may be instructed to contact the Configuration Server at any time.

Network Management Server Software: The Network Management Server software constantly monitors the connections in the DSiP system. A graphical tool called DSiPView enables the user to get a visual feedback over the current network function. Nodes marked green are OK, yellow indicates anomalies in the functionality and red errors. Users may select a node and query its status. DSiP-Graph is a browser tool presenting graphs over node latencies, transferred data mounts etc. [17].

E. TCP Protocol Challenges in Fluctuating Networks

TCP protocol has problems with congestion protocol when switching to different network using other techinques at the network layer. When delay or speed of the network link changes in a situation like switching from 2G to LTE network, the TCP protocol requires relatively long time to adjust to the new network environment.

Normally this would not harm SCADA connections but live video stream might suffer from this. The inefficacy of TCP protocol to adjust can be mitigated by implementing changes to the TCP stack of the sender. There is no need to implement any new software or hardware to the routers and other network communications devices. Also the receiver does not require being aware of the changes to the TCP sender side.

General TCP algorithms for vertical handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in which the receiver reports to the sender that duplicate segment has been received. TCP-Eifel detection algorithm uses TCP timestamps option to detect spurious retransmissions. The Eifel detection provides a faster detection of spurious Retransmission Timers (RTO) compared to DSACK. Forward RTO-Recovery is a TCP sender-only algorithm that helps to detect spurious RTOs. It doesn't require any TCP options to operate.

TCP congestion control algorithms have been designed to enable TCP to adapt to the fluctuating bandwidth available on its end-to-end path. TCP connection remains fairly stable over the lifetime of a connection. Mobile node can easily obtain information regarding the occurrence of a vertical handoff and the status of the wireless link: IEEE 802.21 standard can provide event notifications such as link-up or link quality is degrading.

Proposed enhancements are implemented in the TCP SACK algorithm and they are invoked when a cross-layer notification arrives from the mobile node to the TCP sender. This information contains occurrence of a handoff and rough estimate of the bandwidth and delay of the old and the new access links. Algorithms are incremental in nature and are also conservative it the sense that they are designed not be counter-productive in any situation.

Experiments conducted in Linux kernel version 2.6.18 show that performance of the proposed algorithms is quite close to the results obtained in the simulation experiments. In the absence of the cross-layer information, the proposed enhancements don't affect the normal behavior of the TCP algorithm [18].

Intermittently Connected Networks (ICN) introduces a new problem. How to control TCP traffic flow with networks that are connected to each other only intermittently? Delays can be extremely long and when the connection is made, transfer rate could be high. This creates a challenge for currently used TCP congestion protocols.

Communication protocols for intermittently connected networks must start with an algorithm with very few assumptions about the underlying network structure. The traditional back-pressure algorithm is impractical in intermittently connected networks, even though it is throughput optimal. The back-pressure algorithm is reasonable starting point for developing new protocols for intermittently connected networks.

A modified back-pressure routing algorithm that can separate the two time scales of ICNs is presented in Jung Ryu's study, this algorithm improves performance. On top of this algorithm is a rate control protocol implemented on TCP protocol [19].

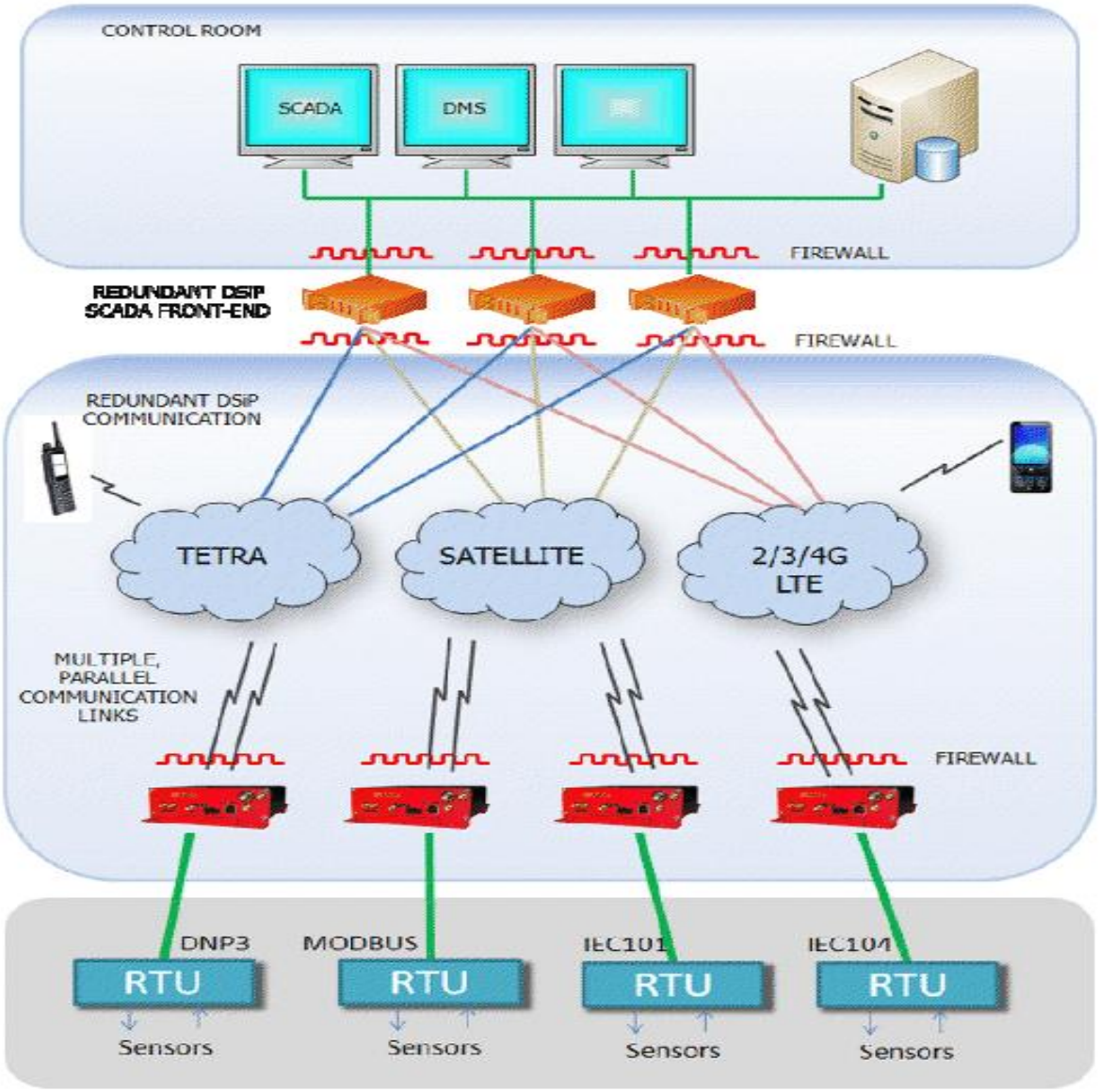

Fig. 1 Fully Redundant Multichannel SCADA Communication Network

F. Other Possibilities for Communications in a Case of Disaster

It is possible to utilize ad hoc networks for communications in special circumcises. If communication networks fail because of destruction of infrastructure it would be possible to use ad hoc communications. In case of power stations usage for this kind of communications is limited since there might not be any other (communications) nodes available within communications range. One solution when using ad-hoc networks is the Ad hoc On-Demand Distance Vector (AODV) algorithm [20].

G. Other Possibilities for the SCADA communications

DSiP is not the only possibility to solve secure and reliable network requirement. One solution would be the integration of the Crossed crypto-scheme to the SCADA system in Smart Grid environment [21]. It solves the problem of securing communication channels but does not handle the problem of managing several communications channels.

However using only this solution does not answer the question of how to deliver several reliable communications channels seamless to the application, SCADA in this use case. The application should not be required to manage all possible communication channels.

III. MACICO Research Project

In recent years, the capabilities of Critical Infrastructure Protection (CIP) and Public Safety (PS) organizations across Europe have been considerably improved with the deployment of new technologies including dedicated TETRA and

TETRAPOL networks. CIP and PS organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe to empower joint responses to threats and crisis in an increasingly interconnected network, but also security organizations have to benefit from interoperability functionality in their day-to-day work.

An international research project 'Multi-Agency Cooperation in Cross-Border Operations (MACICO)' aims at developing a concept for interworking of critical infrastructure protection and public safety organizations in their daily activity. MACICO's main goal is addressing in a short-term perspective the needs for improved systems, tools and equipment for radio communication in cross-border operations as well as during operations taking place on the territory of other member states (high scale civil crisis operations or complex emergencies needing support of Public Safety Services from other Member States).

On the other hand, MACICO encompasses the interoperability issues European countries will be faced to in a long-term perspective, tackling the necessary transition between currently deployed legacy network and future broadband networks [22].

A. Contribution to the Celtic

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new "Smart Connected World" paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the inter-governmental EUREKA network [23].

EUREKA 'Clusters' are long-term, strategically significant industrial initiatives. They usually have a large number of participants, and aim to develop generic technologies of key importance for European competitiveness. Celtic is a EUREKA cluster project that carries out projects in the domain of integrated telecommunications systems [23].

MACICO project aims to develop the interoperability between Professional Mobile Radio communication systems. Through this new feature required by end users, the ultimate goal is to integrate all the current deployed PMR systems within an integrated and secured network.

MACICO will build on existing and promote a standardization of the interface between TETRA and TETRAPOL networks. Interface will be reused for connecting and migrating to future broadband networks. MACICO facilitates the vertical integration of the telecommunications systems dedicated to public safety within an end-to-end architecture and the horizontal integration between themselves via standardized interfaces, which is completely in line with the Celtic Integrated Telecommunications System approach as defined in the Celtic Purple Book.

MACICO focuses on the development of integrated system to enhance public safety communication, the work will include the open interface for interoperability that could be considered as a part of Pan European Lab concept promoted by Celtic (but in the Public Safety frame); The project will look at the new system concept of heterogeneous PMR network and will facilitate the introduction of new services for public safety; All these concepts are at the core of the Celtic Pan-European Laboratory and enables the trial and evaluation of service concepts, technologies and system solutions.

B. Work Packages

MACICO research project contains six Work Packages (WPs). The project starts by collecting end-user requirements (WP2). Architecture and Standard operating procedures design and definition outcomes (WP3) will feed the work packages dealing with Implementation for multi-agency interoperability (WP4) and architectural design for the Demonstration (WP5) of use cases. WP6 includes Dissemination of the project achievements and findings outside the consortium to the larger public audience. The whole project coordination and management is done in WP1.

C. The Finnish Contribution

The impact of the Finnish partners of the MACICO project will produce services that enhance the international competitiveness of companies, society and other customers at all stages of their innovation process.

The Finnish partners will promote the realization of innovative solutions and new businesses by foreseeing already in the strategic research stage the future needs of their customers. The Finnish partners will creatively combine their multidisciplinary expertise with the knowledge of the partners.

The Finnish partners will develop a use case called Interoperability of TETRA and 4G/LTE. The use case is driven by Cassidian Finland Ltd. and other main contributors are Ajeco Ltd. and Laurea University of Applied Sciences. Electric power stations will be an area, where the interoperability will be demonstrated. Additional to the main goal, also interoperability between other networks will be tested, as shown in Fig. 1. In addition, the use case includes requirements for video surveillance of electric power stations

This use case addresses secure and reliable telecommunication power grid applications. The need for secure and reliable communication among power utility customers is divided; on one hand the communication from the control system (SCADA) to the remote terminal units (RTU's) on the field, must be reliable and on the other hand, there is a need for performing site monitoring for detecting physical intrusion for example. In this use case will be implemented a communication system capable of sharing the available communication resource between SCADA-command and control messaging and site surveillance as shown in Fig. 2.

The communication solution must be able to vividly adopt itself to changes in the underlying data transport layers e.g. services of the communication solution must be controllable according to available bandwidth of a communication channel. Another very important task is to control the priorities of the transported messages; Site surveillance and SCADA-command & control must be thoroughly contemplated before implementation.

This use case aims at creating a multichannel communication resource from a control room to an electric power station. The communication solution will implement SCADA-command and control messaging in parallel with of a

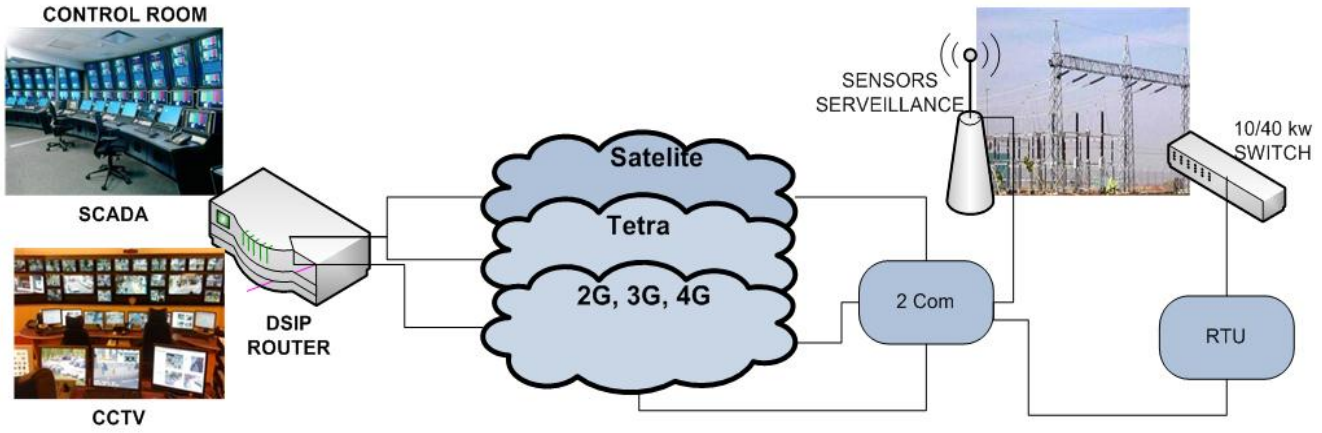

Fig. 2 Secure Communications for Multinational Electricity Supply Deployment

CCTV monitoring and other surveillance and monitoring systems. The aim of this use case is to provide an easily implementable uniform communication solution that will take into account the needs of a smart-grid system, command and control of an electrical substation and site surveillance and perimeter monitoring.

D. Current Situation

MACICO is a large project with many participants all over Europe. This causes many requirements for project management and funding requires arrangements in several countries. This project is expected to be completed by the year 2014. The current situation of the MACICO project is that Switzerland has dropped out form the project, whereas Finland, France and Spain have arranged national funding. The kick-off meeting of the project was held in December 2011.

IV. Conclusions

The military (MIL), public protection and disaster relief (PPDR) as well as critical infrastructure protection (CIP) actors have multiple similar needs. Electricity generation, transmission and distribution compose a critical infrastructure, which is essential for the functioning of a society and economy. SCADA systems are used for controlling the electric power stations.

For added electrical power station security, a video surveillance is required. Current telecommunication networks used for SCADA systems don't support speeds required for real time video. The Multi-Agency Cooperation In Cross-border Operations (MACICO) project aims to produce a new way of combining multiple telecommunication channels, such as TETRA, satellite and 2G/3G/4G networks. A certain target is to create a single redundant secure and faster data transfer path for SCADA and video surveillance systems.

In the future, a common cyber secure voice and data network for MIL, PPDR and CIP brings synergy and enables interoperability; separate networks for the actors are wasting of resources. The benefits expand cross borders for all involved parties.

The cost of the proposed solution should not be evaluated only by the cost of the new solution or the development costs. DSiP is likely to be more expensive than a single channel solution because of the need for several communications networks and more intelligent communications hardware and software.

When calculating TCO and ROI it is essential to consider how much does a one power outage cost. If this new communications solution can shorten a power outage affecting thousands of users even for 5 minutes or prevent it completely then calculated savings can be huge compared to investment costs.

This project also contributes producing a solution useable across borders in several countries. For example cross border users for DSiP solution are international power companies operating in several countries and also border control authorities.

References

[1] SCADA information. Available: http://www.scadasystems.net/, http://www.controlmicrosystems.com/resources-2/faqs/scada11/
[2] A. Daneels and W. Salter, "What is SCADA?" International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy, 1999.
[3] G. Clarke and D. Reynders,"Practical Modern SCADA Protocols", 2004.
[4] D. Kieran, J. Weir & W. Yan, "A Framework For An Event Driven Video Surveillance System", Journal of Multimedia, Volume 6, Number 1, February 2011
[5] I. Glover and P. Grant, "Digital communication", 2004.
[6] J. Korhonen, "Introduction to 3G Mobile Communications", 2003.
[7] J. Eberspächer, H. J. Vögel, C. Bettstetter and S. Hartmann, "GSM-architecture protocol and services", 2011.
[8] E. Dahlman, S. Parkval, J. Sköld and P. Beming, "3G Evolution: HSP and LTE for mobile Broadband", 2008.
[9] P. Stavroulakis, "Signals and communication technology, Terrestrial Trunked Radio- TETRA, A Global Security Tool", 2007.

[10] A. Maini and V. Agrawal, “Satellite Technology: Principles and Applications”, 2011.
[11] J. Holmstrom, J. Rajamaki and T. Hult, “The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication”, International Journal of Communications, Issue 3, Volume 5, 2011.
[12] Project MESA information Available: www.projectmesa.org/
[13] A. Boukalov, “Cross Standard System for Future Public Safety and Emergency Communications”, Vehicular Technology Conference IEEE 60th, 2004.
[14] A. Durantini, “Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications”, Fourth International Conference on Networking and Services ICNS, 2008.
[15] J. Rajamäki, J. Holmström and J. Knuuttila, “Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities”, Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT) 2010.
[16] J. Holmstrom, J. Rajamaki & T. Hult, “DSiP Distributed Systems intercommunication Protocol - A Traffic Engineering Solution for Secure Multichannel Communication” in Proc. 9th WSEAS International Conference on Applied Electromagnetics, Wireless and Optical Communications (ELECTROSCIENCE '11), Meloneras, Gran Canaria, Canary Islands Spain, March 2011.
[17] DSiP information sheet, Ajeco Ltd, 2011.
[18] L. Daniela, “Cross-layer Assisted TCP Algorithms for Vertical Handoff”, Department of Computer Science Series of Publications Report A-2010-6, University of Helsinki Finland, 2010.
[19] J. Ryu, “Congestion Control and Routing over Challenged Networks”, The University of Texas at Austin, 2011.
[20] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung and Y. Lee, “Development of Ad hoc Network for Emergency Communication Service in Disaster Areas”, Proceedings of the 9th WSEAS International Conference on APPLICATIONS of COMPUTER ENGINEERING, 2010.
[21] R. Robles & T. Kim, “Communication Security for SCADA in Smart Grid Environment”, WSEAS Conference in ADVANCES in DATA NETWORKS, COMMUNICATIONS, COMPUTERS, 2010.
[22] MACICO project information. Available: http://www.celticplus.eu/Projects/Celtic-projects/Call8/MACICO/macico-default.asp
[23] Celtic-Plus. Available: http://www.celticplus.eu/

Publication P[3]

P[3] J. Ahokas, J. Rajamäki, I. Tikanmäki, Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 3, Volume 6, 2012, E-ISSN: 1998-4480, p. 120-127, Paper URL: http://naun.org/multimedia/UPress/cc/16-295.pdf, Publisher: NAUN Press

Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations

Jari Ahokas, Jyri Rajamäki and Ilkka Tikanmäki

***Abstract*—** European Public Protection and Disaster Relief (PPDR) organizations have similar needs for communications. A common network for PPDR creates synergy and makes interoperability possible. This paper presents a new highly redundant and secure data communications network solution for Public Safety Communications (PCS). The solution is decentralized and communications paths are redundant. Even if the network layer is shared with different users or different use purposes all communications remains secured and access controlled. Distributed Systems intercommunication Protocol (DSiP) offers all of these features in a single solution. This enables building cyber-secure data network for PPDR organizations. Even though the communications channels are reliable and secured, there are still some issues to be considered. This paper introduces these issues and offers solutions for these challenges.

***Keywords*—**Cyber security, Disaster relief, Distributed Systems intercommunication Protocol, Multi organizational environment, Public safety communications.

I. Introduction

IN recent years, the capabilities of Public Protection and Disaster Relief (PPDR) organizations across Europe have been considerably improved with the deployment of new technologies including dedicated Terrestrial Trunked Radio (TETRA) and digital professional mobile radio (TETRAPOL) networks. Nevertheless, a number of events like the London bombing of 7th July 2005, the Schiphol airport disaster and the flooding disasters in 2010 and 2011 have highlighted a number of challenges that PPDR organizations face in their day-to-day work.

Secure and reliable wireless communication between first responders and between first responders and their Emergency Control Center is vital for the successful handling of any emergency situation, whichever service (Police, Fire, Medical or Civil Protection) is involved.

Security organizations increasingly face interoperability issues at all levels (technical, operational and human) as they interact with other national, regional or international organizations. Not only assets and standards must be shared across Europe to empower joint responses to threats and crisis in an increasingly interconnected network, but also security organizations have to benefit from interoperability functionality in their day-to-day work.

On the one hand Europe is a patchwork of languages, laws, diverse cultures and habits that can change abruptly across borders. On the other hand, even in a same country, each security organization develops its own operational procedures even using incompatible technical solutions within the same country. For efficient operations, many significant challenges need to be addressed, including public safety communication systems (not compatible even when they use the same technology), differing procedures (legal issues) as well as inadequate language skills in cross-border cooperation.

This paper addresses not only the technical security and interoperability issue, but also the complete procedure to build a cyber-secure Public Safety Communication (PSC) system for a multi organizational environment enabling foreign users to cooperate keeping the intrinsic and vital cyber security mechanisms of such networks. Information of other requirements to communications networks and applications such as managing TCP vertical handoff challenges is also included. This paper also presents some of the other available technical solutions for partly producing the same functionality as with DSiP system.

II. Requirements for Public Safety Communication

This chapter identifies the generic requirements for Public Safety Communication (PSC). It addressed specifically the communication requirements that impact first responders.

PPDR field operations are increasingly dependent on ICT systems, especially on wireless and mobile communications. The generic PSC requirements are essentially the need for secure, bi-directional wireless voice communication, but with certain special features not available from the commercial mobile telecommunication network, such as the flexible formation of talk groups, broadcasting, fast call setup, the capability for team leaders to interrupt conversations, and direct-mode communication for cases where network service is either unavailable or disturbed due to the nature of the disaster [1].

Manuscript received May 19, 2012. This work was supported in part by Tekes – the Finnish Funding Agency for Technology and Innovation – as a part of the research project 40350/10 Mobile Object Bus Interaction (MOBI).

J. Ahokas, J. Rajamäki and I. Tikanmäki are with Laurea SID Leppävaara, Laurea University of Applied Sciences, Vanha maantie 9, FI-02650 Espoo, Finland (phone: +358-9-8868 7400; e-mail:jari.ahokas@laurea.fi, jyri.rajamaki@laurea.fi, ilkka.tikanmaki@laurea.fi).

The TETRA system satisfies a large extent of these requirements, as evidenced by its popularity for PSC in Europe and Asia and recent large sales to police forces in the UK and Germany. The equivalent system in the US is Project 25. Details of the TETRA services can be summarized as [2]:

Secure communications: not only to protect any personal data, but also to prevent eavesdropping or malicious intervention. The TETRA radio standard is defined by European Telecommunications Standards Institute (ETSI). TETRA is based on radio channels with a bandwidth of 25 kHz. Each channel is subdivided in 4 traffic channels using Time Division Multiple Access (TDMA).

The traffic channels can be used for both voice and data. The maximum bit rate is 28.8 kbps if all 4 traffic channels are joined together for one data connection. Average TETRA cells are remarkably larger than GSM cells. TETRA uses typically a frequency of 400 MHz, while GSM uses 900 or 1800MHz which provides much greater range for a single base station. Security is provided through the use of private frequencies and end-to-end encryption. Other features of the TETRA standard:

- Creation of teams (group call) and control hierarchy
- Prioritization (emergency call)
- Broadcasting (e.g. evacuation signal)
- Fast call setup (Push-To-Talk)
- Direct mode communication (no base station)
- Open channel
- Listen-in
- Access to the public network
- Short Data Service

However, today's immediate missing requirement is interoperability, not only between different services, but also within the same service if different systems are in operation between regions. This situation has arisen due to the fact that the different emergency services in each region, in each country had historically much autonomy in the way they developed their networks and the terminal devices they purchased [2].

A solution covering all regions regardless of the available communication technologies would be useful. For example if frontier guard is in the middle of a mission and the target moves to another country. Currently communications problems would make it technically impossible to continue following the target when the officials have entered the other country's territory only a few kilometers since communications to command and control center would be lost because most likely roaming would not work at a foreign territory.

Regarding the next generation of services for first responders, the ETSI MESA project [3] has examined what would be possible if wireless broadband capacity was available; i.e. if some of the technologies that have revolutionized the commercial transport of information (both wired and wireless) in recent years were applied in the PSC market. Fig 1 shows project MESA generic core network architecture picture for public services networks.

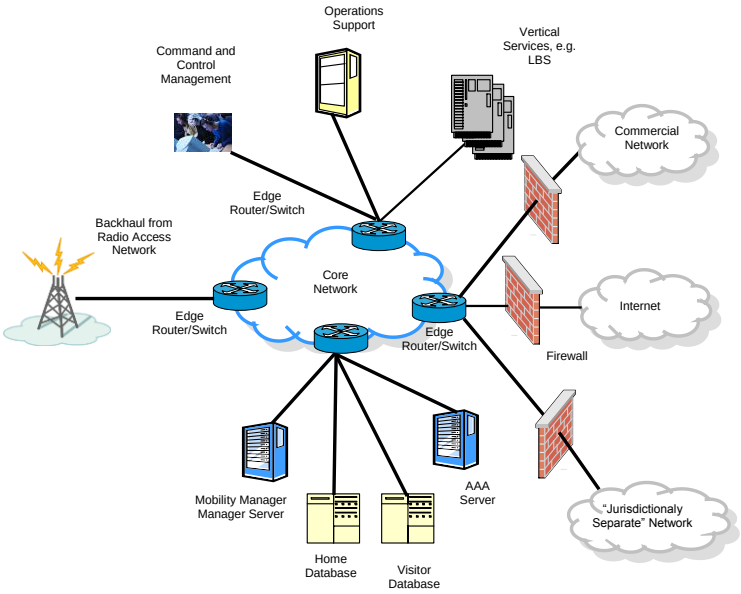

Fig. 1 Project MESA network architecture [3]

From the full list from [3], the ones selected below are considered as being common to all PPDR services:

- Interoperability
- Communication inside buildings
- Improvement in spectrum efficiencies (e.g. reducing channel spacing, using Software Defined Radio, or Cognitive Radio)
- Migration path from existing systems (TETRA, Project 25)
- The ability to remotely partition the network system or bandwidth at a particular site
- Simultaneous access to multiple networks or host computers by a single device, and simultaneous access from multiple user devices to a single host
- Pre-emption: the prioritization of access and routing and the ability to pre-empt non PPDR users (which implies the use of public or open (non-licensed) networks)
- A transaction and audit trail of the use of the network resources
- High-speed, error free transmission: at least 1.5 -> 2Mbps, end-to-end transmit time for data <400ms, end-to-end transmit time for voice <150ms (duplex), <250ms (half duplex) and <400ms if over satellite
- Seamless transparent transfer of devices across networks
- Inherent redundancy
- Typical data to be transported is identified as being:
  - o Voice
  - o Text
  - o Detailed graphical information (e.g. maps)
  - o Images
  - o Video
- Connectivity to local, national and international PPDR databases, and the dynamic updating of database entries from in-vehicle equipment and personal handheld devices
- Remote control of robotic devices
- Geographical position-locating capability

Lack of broadband connectivity of wireless communications for existing and future PPDR applications is a real problem [4]. The rationale behind many of the new services for PPDR actors is that having access to more information at the scene of the emergency, rather than having to request and retrieve it from the Emergency Control Centers, will improve the decision-making process at the scene of a crisis. Every first responder does not need a broadband terminal, but the commander of the mobile rescue team at the scene should have the broadband capability inside a fire engine, police car or ambulance [2].

Some new features can be deployed using the narrowband capabilities of the existing Private Mobile Radio (PMR) spectrum allocated for PSC. Examples are [2]: exploiting the use of sensors in tunnels (or sent into tunnels) to detect temperature, air quality, traffic flow, or built into the clothing of firemen (e.g. location detection, health monitoring), and the electronic tagging of accident victims at the scene and informing the hospital of his/her condition during the ambulance journey.

However, such solutions as the visualization of current traffic congestion on the route to an incident, or enabling remote access to critical information resources such as building plans, satellite photographs, crime databases, etc., depend upon the incorporation of multimedia services that are not feasible over today's PSC networks [2]. For example, descriptions of potential new services from the ETSI MESA group assume bandwidths of at least 1.5 -> 2 Mbps, which would require network infrastructure such as 2.5/3G (EDGE, WCDMA), IEEE802.x (WLAN, WiMAX, 4G/LTE) or satellite [3].

A Finnish study [5] notes that all PPDR actors have the same basic needs for the system, voice and data communication but they also have own distinct requirements. For finding mutual solutions and operation models, system integration is needed. This also enables coherent system design including improved activities, cost savings and improved multi-authority co-operation at the scene.

The roles of complementary technologies in the future are as follow [5]:

• GSM was initially designed as a pan-European mobile communication network. Shortly after the successful start of the first commercial networks in Europe, GSM systems were also deployed on other continents. In addition to GSM networks that operate in the 900 MHz frequency band, others so-called Personal Communications Networks (PCNs) and Personal Communication Systems (PCSs) are in operation. They use frequencies around 1800 MHz, or around 1900 MHz in North America. There are four main standards for 2G systems: Global Systems for Mobile (GSM) communication and its derivatives; digital AMPS (D-AMPS); code-division multiple access (CDMA) IS-95; and personal digital cellular (PDC). 2G/GPRS technologies are reaching the end of their life cycle.

• 3G technology has good coverage with 900 MHz band (better than 2G). However, there are problems on the availability/capacity of commercial networks during major accidents in crowded areas. The 3GPP Long-Term Evolution (LTE) is intended to be a mobile-communication system that is usable in the 2020s. The philosophy behind LTE standardization is that the competence of 3GPP in specifying mobile communication systems in general and radio interfaces in particular shall be used. The result shall not be restricted by previous work in 3GPP. Thus, LTE does not need to backward compatible with WCDMA and HSPA. The first 4G/LTE networks will be at 2.6 GHz, which is not suitable for rural coverage. In future, 800MHz LTE systems are anticipated.

• Wireless local area network (WLAN) technology has three use cases for data transfer: 1) from a vehicle to command and control room at the garage, 2) a local wireless network around the PPDR vehicle at the scene, and 3) from a vehicle to the Internet via a public WLAN; "WLAN fire plug". WLAN has limited range compared to other wireless technologies but bandwidth is generally good and network delay is lower than 3G networks are capable of. A future solution might be WiMAX which provides much larger coverage than WLAN networks are able to provide. Currently WiMAX availability is somewhat limited in Finland.

• Satellite technology has a complementary role when there is no terrestrial communications system coverage. This includes long term usage when no other systems are available and communication need for temporary sites. The telecommunication operator TeliaSonera has announced a start of EutelSat KA-SAT services in June 2011. The service may however be of limited use in PPDR communication applications due to the requirement of a relatively large-size satellite dish antenna, limiting the usability of the service in moving vehicles. A limiting factor is also the requirement of a clear view to a satellite, making it impossible to use satellite communications in an area where a clear view to the sky is unavailable such; as in tunnels or areas with dense forest. Also weather conditions affect satellite communications, heavy rain or snow can weaken the signal considerably. The cost of satellite communications fees (monthly and usage) can be considered an issue.

III. MULTI ORGANIZATIONAL ENVIRONMENT

According to [6] in major disasters no PPRD organization can work alone, but co-operation is needed between different actors. The operational parties should not merely trust on their own resources. Besides, a few organizations possess all the needed areas of expertise in a large-scale event, not to mention a large-scale disaster. Information sharing and training at organizational levels is required in order to achieve a working relationship between the actors. This means the actual and operational interoperability between the first responding organizations; also in reality and in the field – not only on "a paper level" in the form of an official agreement [6].

The military (MIL), public protection and disaster relief (PPDR) as well as critical infrastructure protection (CIP) actors have multiple similar needs. Similarities in disaster relief mission scenarios include 1) serious disruptions in expected functionalities of critical infrastructures, e.g. transport, supplies, infrastructures, 2) operations in remote

areas without communication infrastructures, 3) cross border operations and multi-national teams, 4) high demand for interoperability, 5) no remaining communications infrastructure after a serious disaster, 6) congestion or otherwise not usable commercial networks, and 7) utilizing both AdHoc networks and permanent infrastructures [7]. Similarities in command and control communications involve 1) need to receive information on the operational environment, 2) need for the decision maker to watch operation (live video feed), 3) need to decide and emanate orders, and 4) need to assess the evolution of the operational situation after decision [7].

One possible use case for higher bandwidth and multichannel communications is use of an aircraft patrolling over a disaster area transmitting collected information to the command and control center or the rescue units already at the scene.

IV. CYBER SECURE PUBLIC SAFETY COMMUNICATIONS

Fig. 2 presents a new cyber secure data communications network structure for a multi organizational PPDR environment.

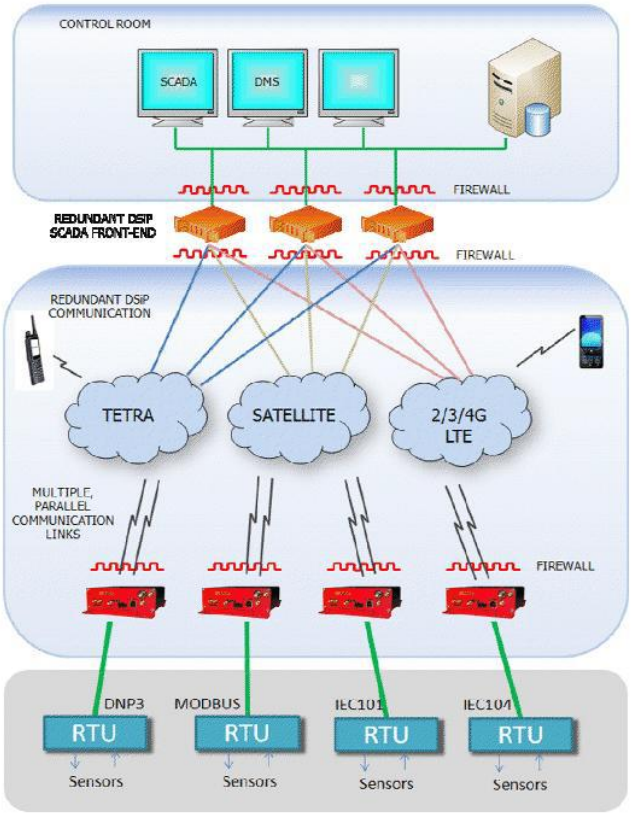

Fig. 2 Cyber secure data communications network structure [8]

The architecture is fully decentralized and all critical communication paths have redundancy. Although having common physical connections, all network actors and elements (multichannel routers, nodes) are identified as well as every organization's all user levels and their rights to different data sources are known.

The decentralized architecture based on the Distributed Systems intercommunication Protocol – DSiP (see e.g. [7], [9]-[10]) is highly fault-tolerant in normal conditions as well as in crises. The software-based approach is independent from different data transmission technologies, from IP core networks as well as from services of telecommunication operators. The solution enables to build a practical and timeless cyber secure data network for multi organizational environment, which being fully decentralized is hard to injure. The networks of different organizations are virtually fully separated, but if wanted they can exchange messages and other information which makes them interoperable.

The DSiP solution is able to offer several benefits:

- Better data security, integrity & priority
- Immunity towards virus infusion
- Immunity towards DoS network attacks
- Intrusion detection
- Authentication- and management tools
- Data-flow handshaking and flow-control
- Controllable data casting and compression
- Interfacing capabilities to equipment and software
- Transparent tunneling of any data
- Early detection of communication problems
- Automatic re-routing
- Cost-efficient network topology
- Insulation from Internet-system flaws
- Routing according to lowest cost and/or shortest hops
- LAN/WAN, TETRA, 2/3/4G, LTE(4G), WLAN, VHF, Satellite etc. communications channels can all be used simultaneously in parallel.

Critical networks and communication solutions require reliable and efficient management and monitoring tools which are easy to operate by command and control center employees. The DSiP solution contains several modules for support, maintenance and configuration of the system.

Authentication Server Software: The DSiP features centralized and mirrorable Authentication Server software. This software allows for maintaining passwords for DSiPnodes. The nodes may have passwords that expire after a specific time for security reasons. Nodes may be allowed in the DSiP routing system and they may be excluded from it at any given time.

Configuration Server Software: The Configuration Server software is an entity for providing routing instructions and firmware updates to nodes. Nodes may be instructed to contact the Configuration Server at any time.

Network Management Server Software: The Network Management Server software constantly monitors the connections in the DSiP system. A graphical tool called DSiPView enables the user to get a visual feedback over the current network function. Nodes marked green are working as normal, yellow indicates anomalies in the functionality and red fatal errors. Users may select a node and query its status. DSiP-Graph is a browser tool presenting various graphs over node latencies, volume of transferred data in a given time etc. [8].

A. *MOBI -Project*

Laurea University of applied sciences (LUAS) has ongoing project called Mobile Object Bus Interaction (MOBI), funded by the Finnish Funding Agency for Technology and Innovation (Tekes). Project's aims are to create a basis for export-striving emergency vehicle concept and to initiate standardization development with like-minded-countries and possible with EUROPOL. There are also three corporate projects exploiting data which are launched alongside with the project. Project has eight work packages; 1) Coordination, 2) User needs, 3) Vehicle infrastructure and power generation, 4) Data communication, 5) Software infrastructure, 6) Applications, 7) Demonstration on police vehicle and 8) Business model development [11].

In MOBI project will be tested a demo vehicle, where among other things is tested similar data communications solution that Fig. 3 illustrates. Demo vehicle is equipped with multi-channel router which is connected satellite-, TETRA, and 3G data networks. Data Communications solution is tested by field tests with the authentic police vehicle, which the Finnish Police Technical Centre has provided for LUAS to enable tests. Fig 3 shows a concept used in demo vehicle.

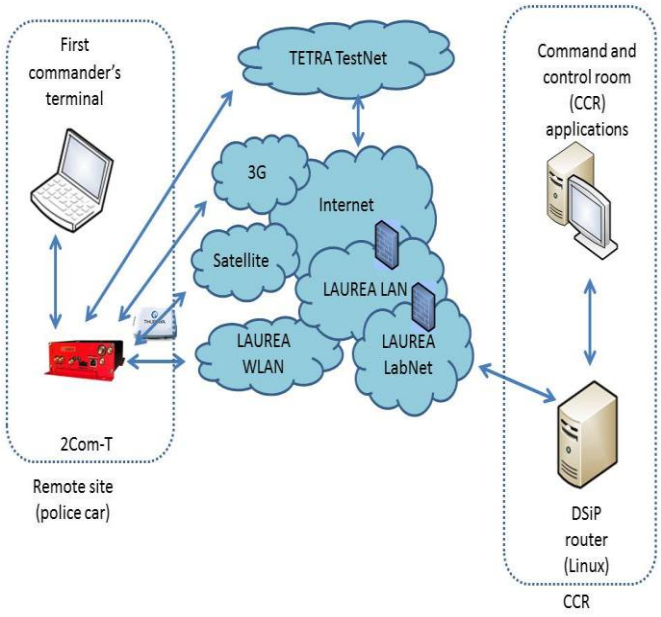

Fig. 3 data communication network structure: case demo vehicle

As shown in Fig. 2, TETRA communication is done by a TETRA test network, which is suitable for this kind of demonstration. There are multiple 3G operators normally used in police cars because of their different coverage in different locations. In this demo we use only one operator's 3G networks. For a satellite communication in this demo is used Spacecom Vehicle Antenna for ThurayaIP and ThurayaIP satellite modem.

Although the TETRA radio network is available, the signal quality may be poor, and system is in practice inoperable. Even if TETRA network is not available, it is not intended to exclude other networks to be used [12].

A multichannel router gives a solution for a problem where is needed duplicated, more than one functional data communication channel for data transmission. The router has opportunities to use several parallel communication paths instead of particular one [8]. In this demonstration is used Ajeco Inc's manufactured 2Com-T Multichannel Router with 3G, TETRA, and Satellite communication channels to vehicle's external communications.

All connection methods do not work in all areas, so several connection methods improve access in the public authorities' information systems (IS) availability. If one of the communication channels, such as 3G network is not available, multichannel router changes the connection automatically for an available network. Multi-Channel Router's Quality of Service (QoS) option sets the desired order of the network access by desired Cost of Service (CoS) value. Therefore, when operating in areas where the network availability and signal strength vary widely, the network exchange should proceed without user noticing it and without breaking the connection.

The user organization will choose in advance whether to use neither the strongest signal nor the cheapest cost network. This selection is done by setting the value of the CoS.

B. *Related Other Public Safety Projects*

There is also another project currently going on which is relying on the same techniques as used in this project. This other project is about securing Supervisory Control and Data Acquisition (SCADA) program communication to power stations and providing enough bandwidth for delivering live video stream from the power stations to the control room. The communications solution is also based on DSiP system using same communications channels and techniques as in PPDR, see Fig 4. Power station control and surveillance communications do not have the same need for mobility as with PPDR units but many of the power stations are located in remote locations thus requiring communications methods like satellite communications. Securing the power distribution network has similar requirements as PPDR and uninterrupted power distribution is equally important to the modern society [13].

DSiP is not the only possibility to solve secure and reliable network requirement. One solution would be the integration of the Crossed crypto-scheme to the SCADA system in Smart Grid environment [14]. It solves the problem of securing communications channels but does not handle the problem of managing several communications channels.

However using only this solution does not answer the question of how to deliver several reliable communications channels seamless to the application. That is; communications without requiring that the application, SCADA in this use case, has complete knowledge of all possible communications channels.

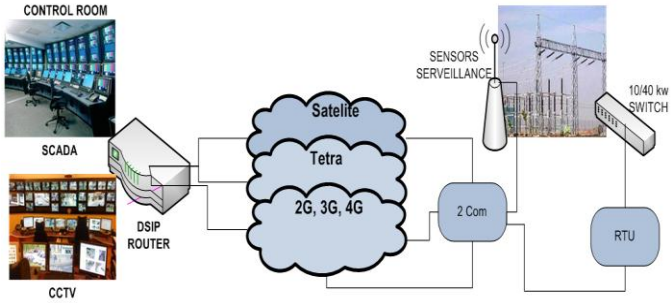

Fig. 4 secure communications for multinational electricity supply deployment [14]

Also tracking of the sea traffic can benefit from the same communications solution as PPDR does. Several sensor nodes collect information of vessels at the sea and transmit this information to the command and control center. This information, such as pictures of the vessel and tracking of the voyage of vessel, is processed at the command and control center and a threat assessment can be made from the collected information. All of these nodes require communications channels and some of the nodes require faster and more reliable connection than the others. DSiP technology is suitable also for this use case when reliability and security is required [15].

C. Other Communications Solutions

As an example it is possible to communicate between communications nodes without supporting infrastructure as ad-hoc basis. This is required when the supporting infrastructure has failed completely because of a natural phenomenon or an act of terrorism or similar event. One solution when using ad-hoc networks is the Ad hoc On-Demand Distance Vector (AODV) algorithm [16]. The AODV algorithm makes communications more efficient by enhancing the routing protocol and guaranteeing level of QoS. In this case DSiP solution security measures and seamless roaming from network to network would be temporarily unavailable until connectivity is restored.

In theory it would be possible to transfer data in such a situation where all network communications to the backbone network are completely lost. This technique is called Intermittently Connected Networks (ICN). In practice a data collecting device can collect data and travel to another location where network connectivity is again available and connect to the backbone network and transfer the data the device carried from other cells to the backbone network. Such a device could be data collecting and transmitting unmanned airplane. PPDR organizations could benefit from this kind of technology because of PPDRs could collect data from the disaster area and transfer it to the control room relatively easily compared to other possible solutions such as transferring data with an external memory device manually from the disaster area to a location with functioning network connection.

A more common usage example would involve communications between military groups in a hostile area where normal communications networks are unavailable, unreliable or unsecure for transferring data. Continuous network connection is not required for exchanging situation information and receiving orders from unit commanders.

A modified back-pressure routing algorithm that can separate the two time scales of ICNs is presented in study of [16] ICN. These algorithms are required to make ICNs usable with TCP protocol. This algorithm improves communications performance in demanding environments. On top of this algorithm a rate control protocol implemented for transmissions in order to control the speed of the data transfer when connectivity is available [17].

D. TCP Protocol Challenges with DSiP

The DSiP device and software solution can hide the complexity of the network architecture from the applications and especially form the end users. But a problem with TCP network convergence still exists. When the charcteristics of the unrelaying physical network change rapidly, often and/or considerably, the currently used TCP congestion protocols are unable to follow the change in a timely manner. To mitigate this problem various solutions are available. One possible solution is to modify the senders TCP/IP stack to make it adjust itself faster when the network changes by using techniques improving vertical handoff. The ability to quickly adapt to network changes is essential to VOIP communications and also streaming technologies like live video feed could have issues with rapidly changing network characteristics.

General TCP algorithms for vertical handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in which the receiver reports to the sender that duplicate segment has been received. TCP-Eifel detection algorithm uses TCP timestamps option to detect spurious retransmissions. The Eifel detection provides a faster detection of spurious retransmission timeouts (RTO) compared to DSACK algorithm. Forward RTO-Recovery is a TCP sender-only implemented algorithm that helps detecting spurious RTOs. This doesn't require any TCP options to operate.

The TCP protocol congestion control algorithms have been designed to enable TCP protocol to adapt to the fluctuating bandwidth available on its end-to-end path. TCP connection itself remains fairly stable over the lifetime of the connection. A mobile node can quite easily obtain detailed information regarding the occurrence of a vertical handoff and the status of the wireless link: IEEE 802.21 standard can provide event notifications such as link-up or link quality is degrading.

Proposed enhancements are implemented in the TCP SACK algorithm and they are invoked when a cross-layer notification arrives from the mobile node to the TCP sender. This information contains occurrence of a handoff and rough estimate of the bandwidth and delay for the old and the new access links. Algorithms are incremental in nature and are also conservative it the sense that they are designed not be counter-productive in any situation. Experiments conducted in Linux kernel version 2.6.18 show that performance of the proposed algorithms is quite close to the results obtained in the

simulation experiments. In the absence of the cross-layer information, the proposed enhancements don't affect the normal behavior of the TCP algorithm [18].

E. Quality of Service (QoS)

For communication to be successful it is also important to focus on network traffic prioritizes for different types of communication streams. When Voice Over IP (VOIP) traffic does not have the highest possible priority in the network it would quite easily become impossible to use any IP based network for reliable voice communications. VOIP traffic is unable to handle jitter, delay or packet loss in a decent manner. To solve this issue a suitable QoS mechanism must be utilized. Using a suitable Differentiated Services (DiffServ) scheme helps solving this prioritization problem. This can be achieved by using a suitable QoS management module for controlling traffic prioritization. Centralized management for DiffServ schemes helps managing all the possible QoS parameters since there are many services and several communications channels available and this cumulates to numerous combinations for QoS classes and service levels [19].

V. DISCUSSION

The public safety communication and information management services market is relatively small (in the year 2008 approximately 2 million users in the US, and similar amounts in Europe and Asia) compared with the 3.4 billion mobile phone users in the commercial telephone network [2]. The PSC and information management systems have different needs (reliability, robustness, security and simplicity) from the regular consumer ITC business. Furthermore, different PPDR services in each region had much autonomy, how they developed their networks. This has caused inadequate interoperability. PSC systems (networks, devices, services) also have a long lifespan; the systems being sold today have changed little over the past 25 years [2]. The aforementioned matters present the need for different business models than in the regular consumer ITC services which have a lifecycle of couple of years for support and maintenance.

The two main challenges in European PPDR field operations are the lack of interoperability and the lack of broadband connectivity [4]. Lack of interoperability limits the effectiveness of PPDR practitioners in actual operations, and an evident lack of understanding as to whether these limitations arose from technology, operational procedures, and gaps in procurement or research. Lack of broadband connectivity of wireless communications limits especially the work of the commander of the mobile rescue team at the scene. At least every fire engine, police car and ambulance should have the broadband capability.

Fault tolerant and highly secure network with seamless roaming capabilities alone does not provide a complete solution for authorities in Europe. Even in Finland there is a lack of communication between different authorities like the police and the border guard. Legislation might permit accessing data cross authorities but there is no technical solution to enable access across authorities automatically. Authorities must have a common framework for transferring data between systems and accessing data in all databases available for different actors. One possible solution to improve data sharing between authorities is systems architecture based on cloud computing [20]. This could also increase availability of the systems since it enables faster capacity additions and provides possibilities to host the services at many different locations for disaster recovery purposes. If cloud computing is designed and deployed thoroughly it can help lowering the TCO of IT systems required by PPDR organizations. This also increases the need for reliable and fast communications system such presented in this paper.

DSiP solution is likely to be more expensive than a regular single channel solution. The reason for this is the required more sophisticated hardware & software than earlier and use of several simultaneous communications channels. But this cost can be considered insignificant if it can save human lives in a disaster scenario. Or even preventing illegal activity in the border zone justifies the cost of the DSiP solution.

If other users also implement the DSiP solution, like power station controlling and monitoring, the cost of the system will be lower per organization when implementing the solution.

Today, all new cars have dual brake systems; if one fails, the brakes can still be used for stopping the car in a safe way. Commercial passenger aircraft have two or more engines; if one engine fails, the plane is still able to fly safely. How it is possible that critical communication systems are based only on a single communication channel? Distributed Systems intercommunication Protocol (DSiP) offers multichannel communication software forming multiple parallel communication paths between the remote end and the command and control room. All this is achieved in a safe manner from network security point of view. Should one of the communication channels be unavailable for use, the other channels can still continue transmitting data without interruption to applications or end users.

REFERENCES

[1] ETSI EMTEL Technical Reports TS 102 181: Requirements for communication between authorities/ organisations during emergencies.

[2] Public Safety Communication Europe, WP1: Users requirements, Report on the definition of the generic users requirements, D1.2, 2009.

[3] ETSI Project MESA: Services and Applications SoR - TS 170.001 V3.3.1.

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

[5] M. Rantama, Pelastustoimen langattoman tiedonsiirron tarpeet ja toteutusmahdollisuudet tulevaisuudessa, Pelastusopiston julkaisu, B-sarja. Tutkimusraportit 2/2011.

[6] Investigation Commission of Jokela School Shootings, Ministry of Justice Publications 2009:2, Helsinki. G. Lapierre, "Synergies and challenges between Defence and Security (PPDR) applications. What implication for the EU?", PSC Europe Conference, 7-8 June 2011, Brussels.

[7] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt and P. Hämäläinen, "A TCP/IP communication architecture for distribution network operation and control", in Proc. of the 17th Internal Conference on Electricity Distribution, Barcelona, Spain, May 12-15, 2003.

[8] Ajeco Oy. Available: http://www.ajeco.fi/

[9] J. Rajamäki, J. Holmström and J. Knuuttila, Robust Mobile Multichannel Data Communication for Rescue and Law Enforcement Authorities, Proc. of the 17th Symposium on Communications and Vehicular Technology in the Benelux, Twente, The Netherlands, 2010. IEEE Xplore.

[10] J. Holmstrom, J. Rajamaki and T. Hult, "The Future Solutions and Technologies of Public Safety Communications - DSiP Traffic Engineering Solution for Secure Multichannel Communication", International Journal of Communications, Issue 3, Volume 5, 2011, pp.115-122.

[11] T. Hult and J. Rajamäki. "ICT Integration of Public Protection and Disaster Relief (PPDR): Mobile Object Bus Interaction (MOBI) Research and Development Project", 10th WSEAS International Conference on Applications of Computer Engineering, Playa Meloneras, Gran Canaria, Spain, March 22-26, 2011.

[12] A. Durantini, M. Petracca, F. Vatalaro, A. Civardi, and F. Ananasso, "Integration of Broadband Wireless Technologies and PMR Systems for Professional Communications", Fourth International Conference on Networking and Services, ICNS 2008, Gosier, Guadeloupe, March 16-21, 2008.

[13] J. Ahokas, T. Guday, T. Lyytinen and J. Rajamäki, "Secure Data Communications for Controlling Electric Power Stations and Distribution Systems", Proceedings of the 3rd International Conference on Energy, Environment, Devices, Systems, Communications, Computers (INEEE '12), Rovaniemi, Finland, April 18-20, 2012.

[14] R. Robles & T. Kim, "Communication Security for SCADA in Smart Grid Environment", WSEAS Conference in Advances in Data Networks, Communications, Computers, 2010.

[15] M. Morel and S. Claisse, "Integrated System for Interoperable sensors & Information sources for Common abnormal vessel behavior detection, & Collaborative Identification of threat (I2C)", IEEE Conference publishing, 2010

[16] H. G. Park, B. Shin, H. K. Park, J. Park, C. Yoon, S. Rho, C. Lee, J. Jang, H. Jung & Y. Lee, "Development of Ad hoc Network for Emergency Communication Service in Disaster Areas", Proceedings of the 9th WSEAS International Conference on Applications of Computer Engineering, 2010.

[17] J. Ryu,"Congestion Control and Routing over Challenged Networks", The University of Texas at Austin, USA, 2011.

[18] L. Daniel, "Cross-layer Assisted TCP Algorithms for Vertical Handoff", University of Helsinki, Finland, 2010.

[19] J P. Orefice, L. Paura & A. Scarpiello, "Inter-vehicle communication QoS management for disaster recovery", The Internet of Things, 20th Tyrrhenian Workshop on Digital Communications, Springer New York 2010.

[20] J. Lehto, J. Rajamäki and P. Rathod," Conceptualised View on: Can Cloud Computing Improve the Rescue Services in Finland?", 11th WSEAS International Conference on Applied Computer and Applied Computational Science, Rovaniemi, Finland, April 18-20, 2012.

Publication P[4]

J. Rajamäki, J. Ahokas, P. Rathod Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System. 2013. 2nd International Conference on INFORMATION TECHNOLOGY and COMPUTER NETWORKS (ITCN '13). Antalya, Turkey October 8-10, 2013. Under review.

Proposing a Redundant Communications Model for Critical Infrastructure Protection and Supervisory Control and Data Acquisition (SCADA) System

JYRI RAJAMÄKI, JARI AHOKAS & PARESH RATHOD
LaureaSID
Laurea University of Applied Sciences
Vanha maantie 9, FI-02650 ESPOO
FINLAND
{jyri.rajamaki, jari.ahokas, paresh.rathod} @laurea.fi http://laureasid.com

Abstract: - Uninterrupted electric power supply and delivery is a part of Critical Infrastructure (CI) for modern society. Secure data transfer between the control center and power station is an essential requirement for controlling and protecting a power distribution system. Supervisory Control and Data Acquisition (SCADA) systems are at the core of power stations control infrastructure. Traditionally, SCADA systems use a proprietary communication network to transfer control signals. These signals are critical between central control systems and power stations. Current telecommunication networks used for the SCADA system do not provide the required capacity for modern Critical Infrastructure Protection (CIP) systems, such as real-time video streaming. In addition, present communication networks or internetworks do not give the required reliability and security for SCADA system. 'Multi-Agency Cooperation in Cross-border Operations (MACICO)' is an International Celtic Plus project to create an innovative communication model. The proposed model will combine multiple telecommunication networks including satellite, TETRA and 4G LTE. This innovative system will also support legacy and future communication technology like 2G, 3G. The MACICO project also includes subprojects. One is to create a secure, redundant and broadband data transfer channel for SCADA and video surveillance systems. This paper aims to propose a new model to address related problems. A proposed communication model relies on the Distributed Systems intercommunication Protocol (DSiP). DSiP allows the combining of various telecommunication resources into a uniform and easy maintain system. The paper is also comparing available solutions of the research problem.

Key-Words: - SCADA, Critical Communications, Secure Communications, Distributed Systems intercommunication Protocol, DSiP, MACICO, Cross-Border Operations, Multichannel networks