# 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 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, 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].

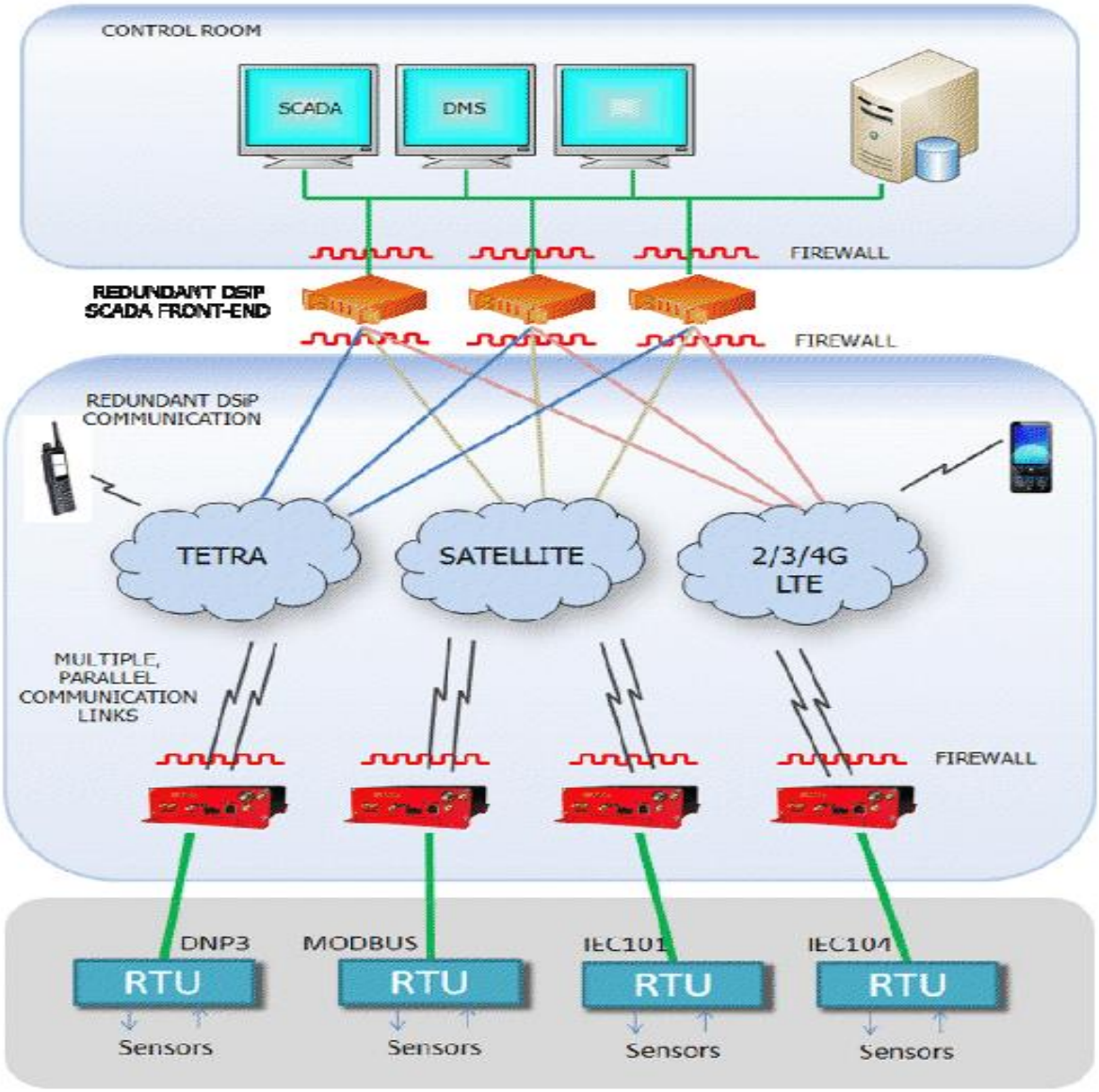


Fig. 1 Fully Redundant Multichannel SCADA Communication Network

### *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

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 CCTV and other surveillance and monitoring. 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.

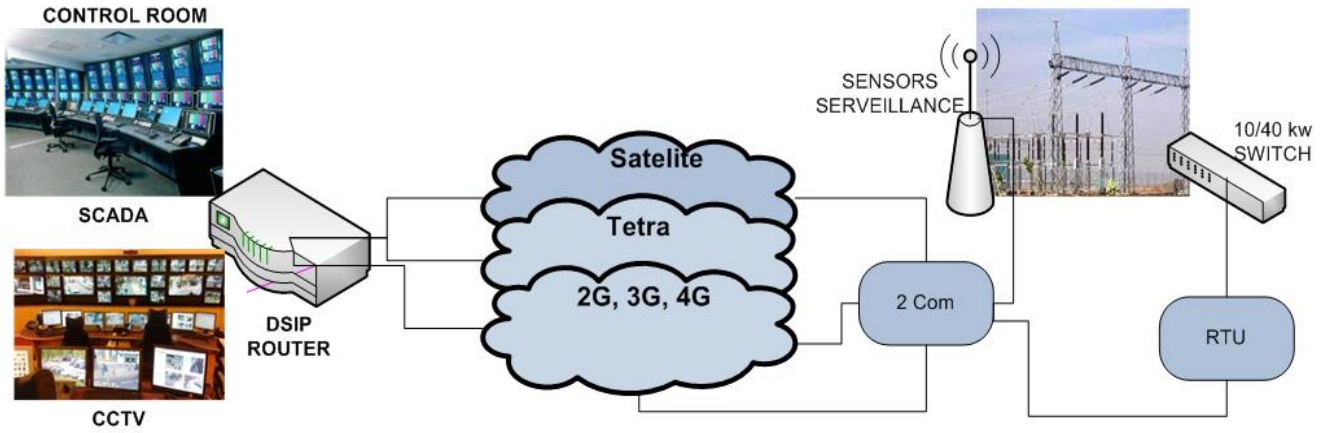


Fig. 2 Secure Communications for Multinational Electricity Supply Deployment

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.

### *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/