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.

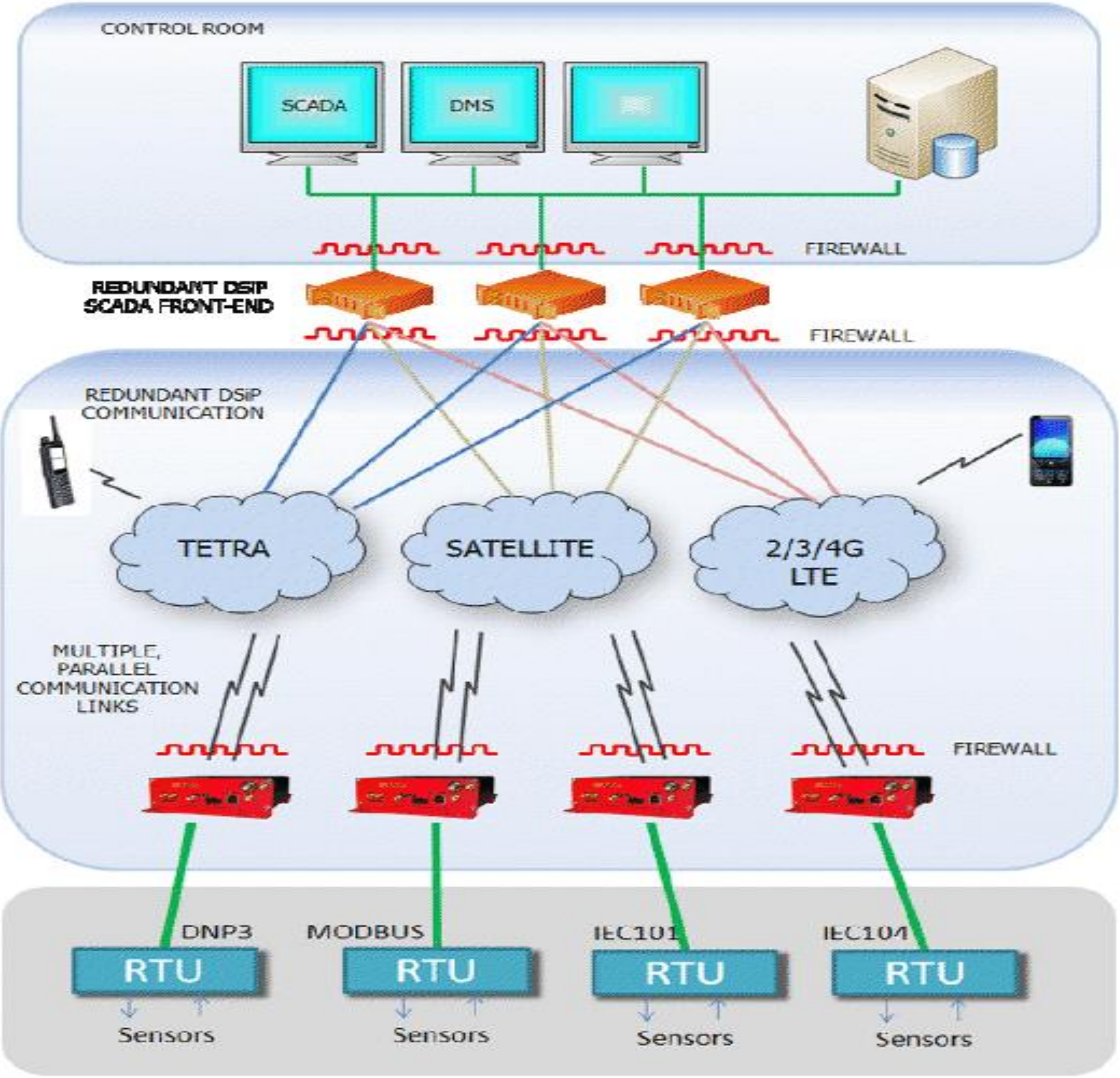

Fig. 1 Fully Redundant Multichannel SCADA Communication Network

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.

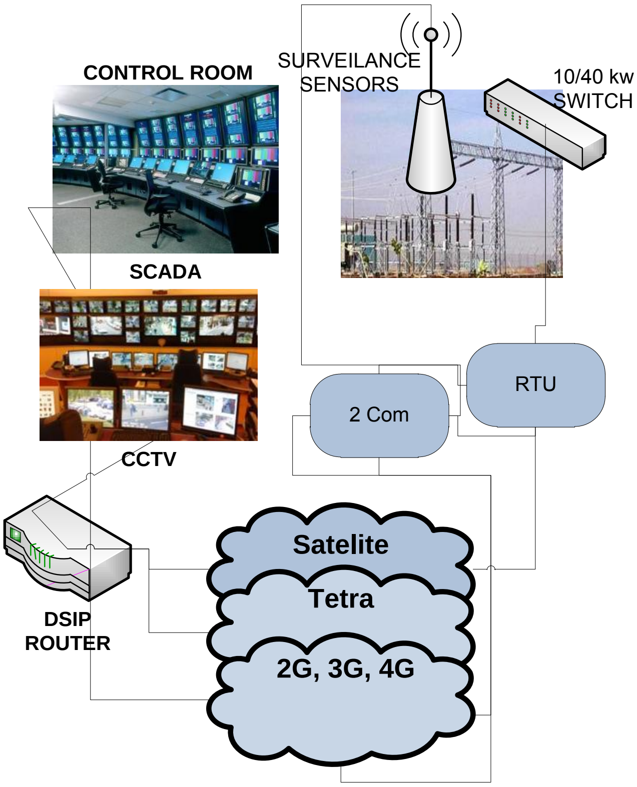

Fig. 2 Secure Communications for Multinational Electricity Supply Deployment

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/