A redundant communications solution for critical infrastructure protection and SCADA systems

Jyri Rajamäki, Jari Ahokas and Paresh Rathod

***Abstract*— S**ecuring an electricity distribution network is equally crucial to securing other critical infrastructure (CI) components. Many critical infrastructure components are operating and controlling by Supervisory Control and Data Acquisition (SCADA) systems. Very SCADA system is also controlling the power network. In the modern infrastructure, these SCADA controlled systems are connecting to standard corporate networks for various reasons. Critical infrastructure and SCADA systems require higher resilient communication channels compared to the corporate network. This infrastructure and the system also demand equally high level of security along with a corporate network. Organizations must use standard base network as a part of solution in order to have resilient communications networks. These combined networks such as TETRA, 3G, LTE, ADSL and satellite have varied level of bandwidth and built-in security features. Recently the additional feature such as a live video stream transported on the critical infrastructure and SCADA networks. These data are transporting in the same logical communications channels without disturbing the SCADA command traffic. This paper aims to propose a new model to combine these networks to produce a highly resilient and secure communications network. The proposed communication system is built-on the Distributed Systems intercommunication Protocol (DSiP) that combines the contradicting requirements to a uniform and easily maintained system. The same requirements apply to 'Multi-Agency Cooperation in Cross-border Operations (MACICO)' project, part of an International Celtic Plus project. The proposed DSiP system is reusable for various needs and is adaptable to future network technologies.

***Keywords*—** SCADA, Critical Communications, Distributed Systems intercommunication Protocol, DSiP, MACICO, Multichannel networks.

I. Introduction

MULTI Agency Cooperation in Cross-Border Operations (MACICO) is an international Celtic-Plus research project. The project is aiming to develop a concept for interworking of critical infrastructure protection and public safety organizations in their daily activities. "MACICO's main purpose is addressing in a short-term stand needs for improved systems, tools and resources for radio broadcasting in cross-border operations as well as during operations taking place on the territory of other member states. Study shows high scale civil crisis operations or complex emergencies needing support of Public Safety Services from other Member States", [1]. On the other hand, MACICO also encompasses the interoperability issues European countries can experience in a long-term perspective, tackling the necessary conversion between currently deployed legacy system and future broadband networks [1].

Critical infrastructure comprises of electricity production, transmission and distribution with other key resources. It is particularly necessary to carry normal functioning of modern society and economy in general. Power distribution networks sprawl across several countries. Power stations are extremely significant components for the entire power distribution system. Data transfer between control centers and power stations is essential for controlling, monitoring and protecting power distribution. Earlier data transfer has only been restrained control signaling between control program Supervisory Control and Data Acquisition (SCADA) and power station components because of limited bandwidth and other technological limitations.

Recent research indicates the importance of video surveillance system in the Critical Infrastructure Protection (CPI). In addition, perimeter monitoring is enhancing security [2], [3]. Live video streaming from prime locations of power stations becoming more prominent because of security threats to the system. There are threats of terrorism, vandalism, natural disasters and phenomenon (like storms, wild animals and others). The threat vector is broader than said list.

Currently electricity distributing companies are using proprietary communication channels along with conventional public Internet connections. On the other hand, traditional radio communications carries substantial limitations including signal reliability and quality. It is clear that the current standard Internet connection, such as ADSL is struggling to provide Quality of Service (QoS). The research case is a power company in the Southern Finland region where experiments carried out. The company is using a standard commercial grade ADSL connection with VPN tunneling devices for SCADA communication and video surveillance

Manuscript received November 9, 2013. This work has been partly founded by the Finnish project as component of the Eureka project Celtic-Plus MACICO (Multi-Agency Cooperation In Cross-border Operations) with 9 partners from Finland, France and Spain.

Jyri Rajamäki is with the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: jyri.rajamaki@laurea.fi).

Jari Ahokas., was with the Master of Business Administration program at Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: jari@jariahokas.fi).

Paresh Rathod is with the Laurea University of Applied Sciences, Leppävaara, Espoo, Finland (e-mail: paresh.rathod@laurea.fi).

since last four years. This solution is working in normal operating conditions. However, it is lacking capabilities of QoS. In addition, it is also lacking any backup connection techniques. The study has demonstrated that the required technology exists, and it does function. However, the largest drawback was certain limitations regarding mission critical usage. Further, our study is showing that data transfer including the video stream from the power station requires secure and reliable connections to the command and control rooms.

This paper introduces a new way of approaching this problem by combining two previously separate data transfer systems. The more fault resistant system is achieved by connecting these independent channels together with enhanced control functionality without adding any complexity to the existing application layer.

II. Study Domain and Applicable Technologies

This section introduces detailed information on research domain and relevant technologies. Mainly, SCADA and surveillance systems and their requirements for data transfer systems.

A. SCADA Systems

SCADA refers to the industry control and monitoring systems including infrastructure, facility, productions or manufacturing processes. SCADA systems are used for supply, control and monitoring daily necessity for modern society. For example, physical processes like electricity, water, gas and oil transmission and transportation. SCADA is also used for areal heating power plant controlling systems. “SCADA protocols consist of Conitel, Profibus, Modbus RTU and RP-570. Standard protocols are mainly IEC 61850, DNP3 and IEC 60870-5-101 or 104” [4], [5]. These protocols are standardized and operated over Transmission Control Protocol / Internet Protocol (TCP/IP).

The SCADA system collects and transmits field data to master stations via Remote Terminal Units (RTU). The collected data allows performing remote tasks to operators. Hence, timely and accurate data are extremely critical to conduct efficient, reliable and secure operations. An RTU is a stand-alone computerized system with software. Broadly there are two types of SCADA software, proprietary and open. It is imperative that any of these software and hardware solutions must synchronously perform routine operation of SCADA systems [6].

A typical SCADA control setup is presented in Figure 1, and it also shows that most SCADA systems are now connected to the enterprise networks instead of being an isolated network [7]. Earlier implementations did not have such connectivity between different kinds of networks. Even nuclear power plants that are SCADA controlled can be connected to the Internet via corporate network. This is emphasizing the fact that both enterprise and SCADA networks need to be protected well. Overlooking the security in either of the networks could result to catastrophic results to the modern society.

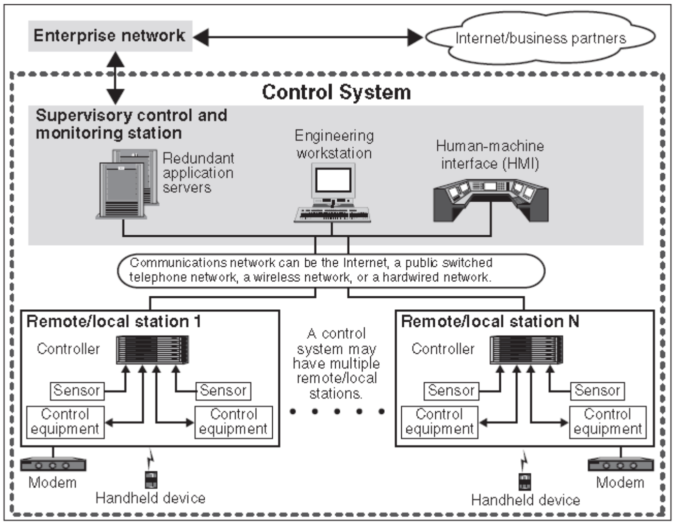

Enterprise network
Internet/business partners
Control System
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
Remote/local station 1
Controller
Sensor
Sensor
Control equipment
Control equipment
A control system may have multiple remote/local stations.
Remote/local station N
Controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
Handheld device
Modem

Fig. 1 Typical components of a control system

B. Access Control and Surveillance System

Access control and video surveillance are the most useful tools for various assets to protect against deliberate or accidental damage or theft. In addition, on various occasions existing vulnerabilities can be overcome by these tools.

There is a requirement of contactless access control implementation due to involved parties are not from individual soil, but also from cross-border countries. Contactless access control could be implemented, which enables the UHF RFID technology. RFID (Radio Frequency Identification) is a general term for technologies operating in the radio frequencies used for identification. Technology is relying on information storage, an RFID tag, and its wireless reading using radio waves. UHF RFID technology is latest, and radio frequency is higher (860-960 MHz) compare to RFID. That enables longer reading distance from tag. In practice, the use of RFID technology brings benefits and resolves current problem that a traveling movement of tag to be identified automatically [8].

C. Video Surveillance System

The largest usage segment for video surveillance is the retail branch, where video surveillance is used for theft and loss prevention. Other pertinent 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 also used in prevention of car thefts and vandalism such as graffiti. Nowadays, video surveillance systems are useful for purposes like space missions and border frontier guard. With the help of video surveillance system, it can be achieved monitoring, tracking and classified the needed target activities. Video surveillance is often a hideous task for an operator to monitor at the command and control center. This task is easier to execute with the application of technical solutions where less human interaction needed on the monitoring process [9].

The same surveillance systems can be used in various other locations and there are several alternative technological solutions available for implementing a video surveillance system. For remote surveillance an IP based system is the most flexible option because of IP traffic can be transported in various networks. A partial survey conducted in an earlier study shows that high quality digital camera systems are easily available and these are widely used in other purposes such as protecting public places in the city area to prevent act of vandalism. [10].

In areas where there are civilians constantly present in close proximity to secured premises, such as power stations in the city area, an automated threat detection system is a useful addition to other security measurements. INDECT research project is developing methods for "new type of monitoring, namely intelligent threat monitoring". [11] Intelligent information system for automatic detection of unlawful actions can be used as a part of a complete security schema for protecting the SCADA controlled CI systems.

D. Communication Systems Operating in Sparsely Populated Area

Normally power stations are sparsely located from resident area. In many cases, the telecommunication network coverage is poor. Various technologies and mechanisms are in use just to transfer information. Different data transfer network systems including leased line connections to commercial mobile networks, satellite and TETRA (Terrestrial Trunked Radio) networks are used to transfer data from sparsely populated areas.

Other technology like GSM was initially design as a pan-European mobile communication network. GSM systems were also deployed on other continents after successful commercial success in Europe. "General Package Radio Service (GPRS) is enabling an improved data transfer rate performance by allowing for more than one GSM timeslot to be used by a terminal for a service at a time [2]". The driving factor for new (and higher bandwidth) data service obviously is wireless access to the Internet [2], [12].

The Third-Generation (3G) mobile communication networks known as the Universal Mobile Telecommunications System (UMTS) in Europe and across the world [2]. The second-generation (2G) mobile system uses digital radio transmission for traffic. However, the 2G networks are close to their end of life cycle. 3G UTRA and GSM systems specifications developed by the Third-Generation Partnership Project (3GPP) consist of several Technical Specifications Groups (TSGs). The 3GPP Long-Term Evolution (LTE) is aiming to be a mobile communication system that can take the telecom industry in to the 2020s [13].

"TETRA is an open digital radio standard for professional mobile radio [13]". TETRA is more useful communicating with the mobile and remote work force along with commercial usage. Public safety and emergency service providers including police and fire departments are the most essential group of users of TETRA [14]. The TETRA system uses an end-to-end encryption, in addition, to the air interface encryption to provide enhanced security. The TETRA system also uses a synchronization technique known as frame stealing to providing synchronization to end-to-end encrypted data apart from the video coding synchronization mechanisms like MPEG-4 and H.263 [14].

Often, the satellite refers as an "orbit radio star" for reasons that can be easily appreciated. A communication satellite is a repeater station that receives signals from ground, processes them and then retransmits them back to the Earth [15].

Power Line Communications (PLC) is widely accepted and easily deployed method for communication with power stations. The live video streaming can be achieved depending on frequencies and modulation techniques within available speeds [16]. PLC is also suitable solution for SCADA communications. However, it may not be suitable as only communications channel for mission critical systems. PLC is not suitable in every situation for obvious reasons. For example, when the power line fails all communications will fail.

Telecommunications de-standardization is also affecting the communications network availability in the US. Telco service providers no longer have to offer legacy services, such as switched low-bandwidth low-yield services, at the same regulated tariff which is lower for rural areas than the actual cost of providing the service. Clients that wish to remain with legacy service could experience price increases once regulation is lifted. It is also a possible scenario that carriers choose no longer to offer the legacy services at all regardless of the actual cost. [17].

III. Research Problem and Methodology

Our research and experiment case is focusing on the power grid application and their infrastructure protection. The existing solutions and services are lacking some substantial feature to provide Quality of Service for Critical Infrastructure Protection (CIP) and SCADA systems. They are also struggling to address issues related to security and reliability of communications.

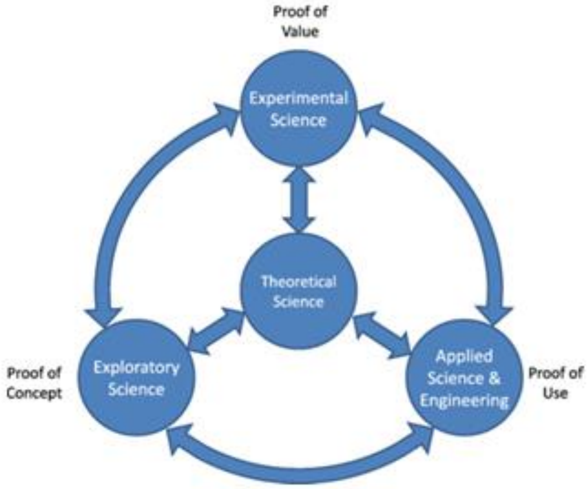


Fig. 2 Integrated multi-disciplinary and methodological development research

These challenges lead us to form research questions and find their solutions. Our research is focusing on following problems: How to provide secure and reliable communications to CIP and SCADA systems? How to implementing Quality of Service (QoS) mechanism to provide better services? We are also comparing and justifying proposed solution model.

Computer science technical solutions are facing challenges of current business problem. If we put innovative artifacts into the action and analyze how they are used and how they performed, we will see things that cannot be seen in the laboratory [18]. Management information systems (MIS) involve three primary resources: people, technology, and information. The MACICO project follows the basic development research in the MIS wheel diagram, first published in 1991 [19]. According to the "going the last mile" approach [18], the starting point of research should be a real problem for real people. In this project, real problem came from governmental SCADA systems and CIP in Finland who are experiencing challenges. This project integrated science both in the laboratory and the field (see Fig. 2), including the theory, prototype and validation by experiments or field studies.

Other studies have also noted the same problem with industrial control system (ICS) security. Preventing ICS contamination by viruses or other malicious software is also a matter of network level security. Reliability violated in case of denial of service (DoS) attack targeted against the network. However, while not all manufacturing systems hold a life-and-death consequence that cannot avoid from potential targets of a cyber-attack [17], [20].

IV. Proposed System

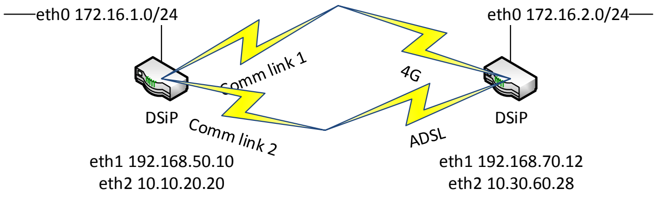
The communication solution should be flexible and adaptable to any changes caused by data transport layers. For example, management of services is based on available data channel bandwidth. Another significant characteristic and functionality requirement is maintaining the priority of message transport. Hence, site surveillance and SCADA-command and control should be carefully contemplated before implementation.

The proposed solution is utilizing multichannel communications resources spreading across the control room to the power station. It will perform SCADA-command and control messaging with the broad range of surveillance and monitoring systems including CCTV. The solution is aiming to provide consistent communication system considering requirements of smart-grid system, command and control of electrical substation; as well as site surveillance and perimeter monitoring.

A. *Multichannel Communication*

MACICO and related projects (for example, Mobile Object Bus Interaction - MOBI) are experimenting and studying multichannel communication. There are promising results, and some are noteworthy to mention here. A multichannel data communication method supplies a way to communicate over virtually any type of telecommunications media in such a way that parallel paths appear as a single robust, uninterruptable, secure and reliable communication link between communicating peers [21]. The solution is based on DSiP (Distributed Systems intercommunication Protocol). It is making possible to interoperate and flawless data transfers amongst various service providers, resulting in a true multichannel communication system. DSiP increases reliability, security and integrity in telecommunication and allows regular communication methods to be used in mission critical telemetry systems [21.] This is achieved by (1) splitting risks between operators and communication channels, (2) better routing and priority capabilities that takes security and intrusion risks into account and (3) adding modularity [3], [22].

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. Figure 3 demonstrates the multi-link connection between two sites in simplified form.



Application is unware of the eth1 & eth2 interfaces on both of the DSiP devices

Fig. 3 Secure communications for electricity supply deployment

Previous studies suggest that using only one network for communications can be considered a risky approach especially in public safety communications. The USA Office of Emergency Communications is aiming for Nationwide Public Safety Broadband Network, FirstNet, to be based on LTE network technology [23]. LTE networks are vulnerable to the wireless interface jamming using low cost relatively simple devices as described in Virginia Tech preliminary research [24]. If networks build on LTE technology were to be compromised, existing 2G and 3G networks would still operate without problems. However, those older networks are gradually being phased out. This very fact shows the need for uninterrupted and secured multichannel communications.

Combining different forms of communication networks is a challenging task. The DSiP solution meets this challenge. It integrates the quality of service definitions for a variety of traffic. Traffic priority levels can be based on the destination of the IP traffic flow in question or by analyzing the TCP headers. By using DSiP, it can be safer assumed that any User Datagram Protocol (UDP) traffic is neither time sensitive nor needing a highly reliable communications channel. It is also possible to divide, and direct traffic flows to a different channel based on the routing costs of each channel. All these features are combined in to a single device. DSiP solutions classify traffic flow and take routing decisions based on the priority of individual traffic channel and flow. Further, it is not causing unnecessary delays in high priority traffic. At the same time, cost control is maintained by routing traffic based on customer defined routing costs.

B. *Built in Security*

The requirement for secure communications in SCADA networks have been studied earlier and the proposed DSiP system fulfills identified reliability and security feature requirements [25]. As the earlier paper states, there are also other security and high availability features that have to be considered such as fault tolerant network switches or uninterrupted power supply for network appliances. Figure 4 shows an example of Closed-circuit television (CCTV) and SCADA communications combined it a single communications framework.

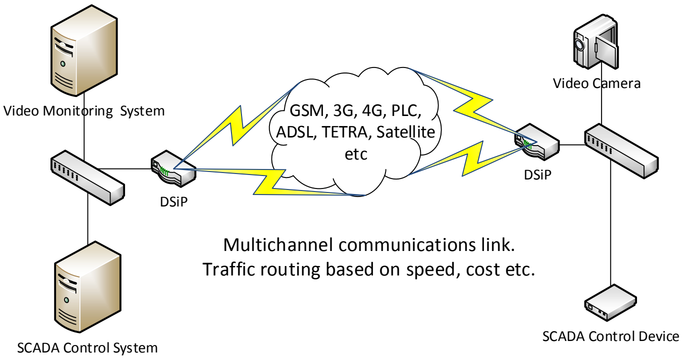

Video Monitoring System
GSM, 3G, 4G, PLC, ADSL, TETRA, Satellite etc
Video Camera
DSiP
DSiP
Multichannel communications link. Traffic routing based on speed, cost etc.
SCADA Control System
SCADA Control Device

Fig. 4 Secure communications for electricity supply deployment

DSiP infrastructure has powerful built in security measures for securing critical infrastructure communications, such as power stations. Several key factors for strong security are included in the DSiP. These elements are usage of IPsec protocol, encryption based on secure ciphers such as Advanced Encryption Standard AES-256, packet time stamping, sophisticated firewall and prevention of denial of service (DoS) attacks. All of these security features are required for constructing a high security communications network for SCADA operations. Deploying DSiP system can help in achieving North America Electric Reliability Corporation (NERC) standards, especially targeted for CIP. NERC CIP 002-009 documents set demanding reliability and security standards for protecting SCADA communications [26].

An earlier study on cyber-attacks targeted on SCADA systems indicate that the security issues should be treated the same way as with other standard IT operations. There are still a lot of old SCADA installations that do not have any built it security measures [27]. Thus the communications network should be able to provide the needed security features for SCADA communications and avoid the need to replace the vulnerable systems earlier than economically viable.

Combining two fundamentally different communications requirements can be achieved with the DSiP system. Video surveillance data requires high-bandwidth. It can survive network packet loss without functionality loss while SCADA commands require reliability and relatively sparse network delay. The DSiP system separates these requirements from each other and delivers the required functionality to both use cases.

C. *Test Setup*

DSiP-based systems have been in operative use in critical installations for several years, for example, the Finnish Coast Guard's coastal surveillance solution and SCADA control of Finland's main power grid [28]. However, simultaneous transmission of data for applications with so diverse requirements and characteristics than SCADA and CCTV needs testing. Different kind of DSiP nodes and router has been tested at Laurea University of Applied Sciences (LUAS). The required DSiP routers and communications devices, such as satellite and 3G modems, have been installed, also, in a police vehicle for testing purposes as a part of Mobile Object Bus Interaction (MOBI) project. There will be a proof of concept vehicle as an outcome of MOBI project. Among other things, similar data communications solutions are under testing for SCADA control.

The MOBI demo vehicle is equipped with multichannel router that is simultaneously connected to satellite, TETRA, and 3G data networks. Data communications solution is evaluated by field tests with the authentic police vehicle, which the Finnish Police Technical Centre has provided for LUAS for testing purposes. [21] A more advanced version of DSiP router with 4G/LTE functionality is about to be installed in the test vehicle.

For extended testing purposes Automatic License Plate Reader (ALPR) could be installed in the test vehicle. Uninterrupted access to the license plate database would be essential for the system to work in an efficient manner. As an example of the ALPR technology developed is a company Data911 in the US [29].

D. *Other Use Cases*

The proposed system can be used for various other purposes which are not considered as a critical infrastructure components. These applications are for example: A card payment system online verification for taxis. Continuous access to the payment system backend is required for efficient taxi vehicle usage. Other use case could be delivery trucks that require constant access to the backend systems for optimizing the delivery route and acquiring new work orders or closing existing work orders. All of these can be considered business critical use for private companies and the investment costs should be carefully evaluated to calculate ROI.

V. Discussion

The DSiP device and software package can hide the complexity of the network architecture from the applications and especially from the end users. However, a problem with TCP network convergence still exists and needs to be examined in more detail

A. TCP Protocol Challenges in Fluctuating Networks

TCP protocol has inherited problems with congestion protocols when switching to different network layers that use various techniques. Congestion protocol challenges are noticeable when delay or speed of the network link changes considerably in a situation like switching either from 2G to LTE network. The TCP protocol requires relatively long time to adjust to the new network environment after the vertical network handover

Normally this would not harm SCADA connections since communication with devices is not bandwidth incentive. Short delays caused by TCP protocol readjusting itself should not cause difficulties for SCADA control, since commands are usually small and can even be fitted into a single TCP/IP encapsulated packet. In relatively seldom instances where SCADA control communications is highly time critical requiring an instant response, jitter in network delay could cause issues. Long adjustment delay is a challenge for live video streaming or Voice over Internet Protocol (VoIP) traffic. The inefficacy of TCP protocol to adjust can be mitigated by implementing modifications to the TCP stack of the data sender operating system. There is no need to implement any new software or hardware to the routers and other network communications devices. Also, the receiver is not required of being aware of the changes to the TCP stack at the sender side.

General TCP algorithms for vertical network handoffs include Duplicate Selective Acknowledgement (DSACK) which is an extension of TCP SACK in that the receiver reports to the sender that duplicate segment has been received. TCP-Eifel detection algorithm uses TCP timestamps option to detect spuriously retransmissions. The Eifel detection provides a faster detection of Spurious Retransmission Timeouts (RTO) compared to DSACK. Forward RTO-Recovery is a TCP sender-only implemented algorithm that helps to detect Spurious RTOs. It does not require any additional TCP header 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 linkup or link quality is degrading.

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

Experiments conducted in Linux kernel version 2.6.18 shows 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 enhancement does not affect the normal behavior of the TCP algorithm [30]. A modified backpressure routing algorithm can separate the two time scales of Intermittently Connected Networks (ICN). 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 [31].

B. Alternatives for the SCADA Communications

There are other alternatives to the DSiP solution. One solution would be crossed crypto-scheme integration to the SCADA system in Smart Grid environment [32]. This solves the problem of securing the communication channels, but does not tackle the problem of managing several communications channels in an effective manner. However, using only the said solution does not answer the question of how to deliver several reliable communications channels seamlessly to the application layer, SCADA in this use case. The application itself should not be required to manage all possible communication channels combinations in the grid. Also managing security associations, that being pre shared keys or certificates, between multiple end points is unnecessary task.

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. There might be no 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 [33]. There are situations where all connections to the backbone network are entirely lost. In such situations, theoretically it would be possible to transfer data from the affected area. ICN is this kind of technique.

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 either practical for remote surveillance neither for remote control. In order to make ICN work, IP protocol modifications are required.

C. Quality of Service (QoS)

For communications to be successful, it is also essential to focus on network traffic prioritizes for different types of communication streams. A different technique required for assuring high-transport priorities while operating without DSiP systems. To solve this issue, a suitable QoS mechanism must be utilized. Using a suitable Differentiated Services (DiffServ) scheme is helping to solve prioritization problem.

The solution can be using a suitable QoS management module to control traffic prioritization. Centralized management for DiffServ schemes helps to manage all the possible QoS parameters. Since there are many services and several communications channels available, this cumulates to numerous combinations for QoS classes and service levels [34]. It is worth noting that many available commercial communications networks do not honor QoS tags in IP traffic. That makes difficult to deploy transportation priorities in multichannel environments. IPv6 protocol has enhancements over IPv4 with QoS. Datagrams include QoS features better support for multimedia and other applications.

D. *Optimizing the SCADA Infrastructure for Resiliency*

When implementing a secured communications for the SCADA remote control, the backend system must also be more faults tolerant. All of the components used for the CI SCADA systems must be considered equally important in order to have a secure and highly fault tolerant framework for continuous operation. For the backend infrastructure an Infrastructure as a Service (IaaS) concept can offer benefits in the form of lowered investment costs and higher level of usability. When IaaS or similar cloud computing scenarios are used with CI systems the security aspects are increasingly important. A recent study on securing could IaaS solutions suggest that most of the issues with data security in the cloud can be tackled. For example this requires ridged planning and use of carefully selected cryptographic solutions [35].

E. *Integrating Existing Systems to DSiP*

All communications should be carried over IP-protocol in order to DSiP solution to function. 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, replacing older RS-232 devices might not be economically viable solution since SCADA systems can have a pretty long life span. For older power stations, there is a minor additional cost building IP network inside the station premises, usually standard Ethernet based technology.

F. *Comparison of Available Solutions*

The proposed DSiP solution has several advantages compared to other technologies. Table I presents a comparison between the solutions introduced in this paper. The DSiP system does not require applications to be aware of any of the communications routes and/or the characteristics of the underlying networks.

However, further research work is recommended for a complete end-to-end solution. The most notable feature being that DSiP can combine many of the required functions into a single solution without application code rewriting.

Table I Comparison of Technical Solutions

	DSiP	**DiffServ**	**Crossed Crypto-Scheme**	**Ad hoc networks**	**ICN**
Multiple network routes	x	x	x	x (many point-to-point connections)	x
QoS	x	x			
Single device / hardware solution	x				
TCP enhancements in fluctuating networks					x
Built in security features	x		x	x (if network permits)	
Cost control based on network route	x		x (static)		

The table lists different technical solutions described in previous chapters. Features of the solutions are compared, and as a result, DSiP has the most beneficial feature set amongst them. There is one thing that not directly addressed by DSiP being TCP protocol issues in vertical network handovers. However, it must be noted that none of the compared technology offers a consolidated result for fluctuating TCP networks. Using TCP protocol enhancements in the operating system level can mitigate the problem.

VI. Conclusion

The Critical infrastructure is composing electricity generations, transmissions and distributions. That is essential for the functioning of a 21st century society and economy. SCADA systems are used for controlling the electric power stations. SCADA systems require high reliability and they may have very strict requirements on low latency. For added electrical power station security, a broad range of surveillance systems are needed, video surveillance being crucial. Current telecommunication networks used for SCADA systems do not support major volumes of information to be conveyed for real time video.

The MACICO (Multi-Agency Cooperation In Cross-border Operations) project is aiming to resolve this problem interconnecting different telecommunication networks and combining various communications ways in a single logical communications channel. An objective is to create a redundant, secure and fast single data transfer system for SCADA and video surveillance. The data transfer system should have the performance and capabilities needed to handle these diverse requirements and characteristics in an efficient way. The DSiP can solve many of the challenges with communications over different networks in a single solution.

A more fundamental problem with the TCP protocol itself needs to be address. This could be resolved with a help from the DSiP router in a form of providing information about the underlying network layer features. Some changes faster than TCP algorithms can discover in speed or reliability of the network connection. Further studies and research need to carry out on IPv6 networks with DSiP.

DSiP solution is likely to be more expensive compared to a single channel communications. The cost increases because of the need for specific communications networks, and more intelligent communications equipment and software. When calculating total cost of ownership and Return on investment for DSiP, it is necessary to consider how much one power outage cost. New and improved communications solution can diminish the power outage affecting thousands of users or even completely inhibit the outage from occurring in the first place. The cost savings would be enormous when compared to the initial investment costs.

One possible solution to develop critical infrastructure reliability is systems architecture based on cloud computing. This project also contributes producing a solution useable across borders in several countries. The international power companies operating in different countries are examples of cross border users for DSiP solution. Our future studies are going to focus on more field studies comparing available solutions.

REFERENCES

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

[2] J. Eberspächer, H. J. Vögel, C. Bettstetter and S. Hartmann, "GSM architecture protocol and services", Third Edition. John Wiley & Sons Ltd. Great Britain. 2011.

[3] 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.

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

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

[6] G. Clarke and D. Reynders, "Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems", Elsewier, Great Britain, pp. 15-16, 19, 163, 2004.

[7] United States General Accounting Office, "CRITICAL INFRASTRUCTURE PROTECTION Challenges and Efforts to Secure Control Systems", 2004. Available: http://www.gao.gov/new.items/

[8] UHF Wristband Sport. Available: http://www.rfidtag.cz/

[9] D. Kieran, J. Weir & W. Yan, "A Framework For An Event Driven Video Surveillance System", *Journal of Multimedia*, Volume 6, Number 1, February, pp. 3-13, 2011.

[10] M. Adámek, Z. Tvrdý, M. Matýsek and P. Neumann, "The Use of Camera Systems in Municipalities", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 160-166, 2013.

[11] A. Dziech, J. Derkacz and M. Leszczuk "INDECT and TAPAS projects – research objectives and chosen solutions", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 119-124, 2013.

[12] J. Korhonen, "Introduction to 3G Mobile Communications", Second Edition. Artech House. Norwood, MA. 3, 14, 2003.

[13] E. Dahlman, S. Parkval, J. Sköld and P. Beming, "3G Evolution: HSP and LTE for mobile Broadband", Second Edition. Academic Press. Burlington, MA, pp. 9, 22, 2008.

[14] P. Stavroulakis, "Signals and communication technology, Terrestrial Trunked Radio- TETRA, A Global Security Tool", Springer, Heidelberg, pp. 2, 27, 51, 170, 2007.

[15] A. Maini and V. Agrawal, Satellite Technology: "Principles and Applications", John Willey & Sons Ltd, Noida, India, p. 4, 2011.

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

[17] T. Macaulay and B. Singer, "Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS", CRC Press, USA, 2012.

[18] R. Winter, "Interview with Jay F. Nunamaker, Jr. on "Toward a Broader Vision of IS Research"", Business & Information Systems Engineering, Vol. 2: Iss. pp. 5, 321-329, 2010.

[19] J. F. Nunamaker, Jr., M. Chen and T. D. M. Purdin, "Systems development in information systems research", J. Manage. Inf. Syst. pp. 7, 3, 89-106, 1990.

[20] E. Knapp, "Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems", Elsevier Inc, USA, 2011.

[21] J. Ahokas, J. Rajamäki and I. Tikanmäki, "Secure and Redundant Public Safety Communication Network for Public Protection and Disaster Relief (PPDR) Organizations", *International Journal of Communications*, Issue 1, Volume 6, 2012, pp. 120-127.

[22] 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 Law Enforcement Authorities", *Proc. of the 17th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, Nov 24-25, 2010.

[23] Office of Emergency Communications, "Nationwide Public Safety Broadband Network", USA, 2012, The U.S. Department of Homeland Security (DHS), Available: http://www.dhs.gov/

[24] Wireless @ Virginia Tech, A brief response to the FirstNet NOI regarding the conceptual network architecture, USA, 2012, Available: http://www.ntia.doc.gov/files/ntia/va_tech_response.pdf

[25] M. Zafirovic-Vukotic, R. Moore, M. Leslie, R. Midence and M. Pozzuoli, "Securing SCADA Communications following NERC CIP Requirements", Asia Energy Week 2008, Kuala Lumpur, Malaysia, May, 2008.

[26] NERC Standard CIP-002-3 through -009-4, Cyber Security, 2009-2012 Retrieved November 10, 2012, North American Electric Reliability Council (NERC), Critical Infrastructure

[27] B. Zhu, A. Joseph and S. Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems", *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, 19-22 Oct,. pp. 380-388, 2011.

[28] J. Rajamäki, "The MOBI project: Designing the future emergency service vehicle", *IEEE Vehicular Technology Magazine*, June 2013 [In Press].

[29] *Data911's License Plate Reader (LPR).* Available: http://www.data911.com/images/pdf/data911_lpr.pdf

[30] 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.

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

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

[33] 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.

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

[35] A. Delfosse, J. Fanton, T. Floriani, V. Malguy, N. Marine and C. Tavernier, Cloud Data security and privacy in IAAS model", 2nd International Conference on Information Technology and Computer Networks (ITCN '13), Antalya, Turkey, pp 54-67, 2013.

Jyri Rajamäki received his M.Sc. (Tech.) degree in electrical engineering from Helsinki University of Technology, Finland in 1991, and Lic.Sc. (Tech.) and D.Sc. (Tech.) degrees in electrical and communications engineering from Helsinki University of Technology in 2000 and 2002, respectively.

From 1986 to 1996 he works for Telecom Finland being Development Manager since 1995. From 1996 to 2006 he acted as Senior Safety Engineer and Chief Engineer for the Safety Technology Authority of Finland where his main assignment was to make the Finnish market ready for the European EMC Directive. Since 2006 he has been a Principal Lecturer at Laurea University of Applied Sciences, Espoo, Finland, where he also serves as a Head of Laurea’s Data Networks Laboratory ´SIDLabs Networks´. His research interests are electromagnetic compatibility (EMC) as well as ICT systems for private and public safety and security services. He has authored about 90 scientific publications.

Dr. Rajamäki has been an active actor in the field of electro technical standardization. He was 17 years the secretary or a member of Finnish national committee NC 77 on EMC, ten years a member of NC CISPR and he represented 15 years Finland at IEC, CISPR, CENELEC and ETSI EMC meetings. He was also the Chairman of Finnish Advisory Committee on EMC from 1996 to 2006. Dr. Rajamäki has been the scientist in charge for several research projects funded by Tekes – the Finnish Funding Agency for Technology and Innovation, industry and EURESCOM. He is currently the scientific supervisor and director of one ITEA2 and one Tekes project.

Paresh Rathod is born in India and settled in Finland. He has received his Masters of Computer Application (MCA) from Bhavnagar University, India in year 2000. Paresh is also holding Post Graduates in Advanced Computer Systems Development (ACSD) from University of The West of Scotland, UK in year 2006. Paresh has also achieved his NSA sanctioned CNSS information security professional certification from MIS Department of University of Arizona, USA in year 2010. Paresh is also an Oracle Certified Professional since year 2004.

He is a technocrat, educator and researcher. He has many years’ experience in an International business and ICT fields, as a consultant, project leader, database administrator, application programmer, quality assurance professional and researcher. Currently, he is working as a Senior Lecture and Degree Programme Coordinator (BIT) at Laurea University of Applied Science, Espoo city, Finland. His current research interests in the area of information assurance and cyber security, service innovation and service-oriented architecture (SOA), cloud computing and cutting-edge technologies. He has published scientific articles in refereed international conferences and journals.

Mr. Rathod is a professional member of many professional bodies including ACM, IEEE, IEEE Computer Society, ISACA, ASIS and Finnish Information Security Association (FISA). Mr. Rathod also a member of Special Interest Group on Security, Audit and Control (SIGSAC) and Special Interest Group on Information Technology Education (SIGITE). He is a member of scientific committees of international conferences and organizations. Mr. Rathod is active reviewer in international journals, publications and conferences. He is also volunteering in many causes.

Jari Ahokas was born in Vihti, Finland, in 1972. He received the BBA and MBA degrees in computer and information sciences from the Laurea University of Applied Sciences, Espoo, Finland in 2002 and 2013 respectively. He is also carrying professional certifications in VMware and Microsoft Certified Technology Specialist.

He is currently working in the private sector at a financial institution as a Senior Systems Specialist in Helsinki, Finland. He has worked many years as systems engineer and specialist. Mr. Ahokas has been active researcher during his studies and published four research papers focusing on SCADA and critical infrastructure security. His research interests include communications systems, infrastructure control systems and cyber security.