C. Alcaraz, J. Lopez, J. Zhou, and R. Roman, "Secure SCADA Framework for the Protection of Energy Control Systems", *Concurrency and Computation Practice & Experience*, vol. 23, pp. 1414-1430, 2011.
http://doi.org/10.1002/cpe.1679
NICS Lab. Publications: https://www.nics.uma.es/publications

Secure SCADA Framework for the Protection of Energy Control Systems

C. Alcaraz[1], J. Lopez[1], J. Zhou[2], and R. Roman[1]

[1]Computer Science Department, University of Malaga,

Campus de Teatinos s/n, 29071, Malaga, Spain

[2]Institute for Infocomm Research, 1 Fusionopolis Way,

Singapore, 138632, Singapore

November 3, 2015

Abstract

Energy distribution systems are becoming increasingly widespread in today's society. One of the elements that is used to monitor and control these systems are the SCADA (Supervisory Control and Data Acquisition) systems. In particular, these control systems and their complexities, together with the emerging use of the Internet and wireless technologies, bring new challenges that must be carefully considered. Examples of such challenges are the particular benefits of the integration of those new technologies, and also the effects they may have on the overall SCADA security. The main task of this paper is to provide a framework that shows how the integration of different state-of-the-art technologies in an energy control system, such as Wireless Sensor Networks (WSNs), Mobile Ad-Hoc Networks (MANETs), and the Internet, can bring some interesting benefits such as status management and anomaly prevention, while maintaining the security of the whole system.

Keywords: Energy distribution and control systems,,SCADA systems, ICT systems, Wireless sensor networks, Mobile Ad-Hoc Networks, the Internet

1 Introduction

Our society comprises a set of critical infrastructures, which provide certain essential services that are especially the input to other critical infrastructures. Energy distribution systems are a type of critical infrastructures that today's society heavily relies on. Every day millions of watts of electricity are being channeled from power suppliers to power consumers. A disruption of such services could involve serious consequences in the performance of other critical

infrastructures, such as transport systems, water treatment systems or communication systems, consequently affecting the social and economic being-well of a city, a region or even a country [**?**]. For this reason, specialized control systems, known as SCADA systems, are used together with a set of state-of-the-art ICT systems for supervising and monitoring in real-time.

At present, two of the most demanded ICT systems for control systems are the Internet and wireless technologies. The Internet provides remote monitoring and management, whereas wireless technology offers monitoring services as a wired infrastructure to a low installation and maintenance cost. Taking advantages of this situation, this paper analyzes the coexistence of WSNs, MANETs and the Internet in a same context to provide an approach which complements specific properties of each of them. For example, WSNs could offer system control, detection and alert of anomalous situations, whereas MANETs could provide mobility, management and collaboration among operators, and obviously the Internet could offer control from anywhere at any time, other critical systems.

Thus operators in field may know in real-time the actual state of the system or subsystems with the possibility of collaboratively interacting with other (close or distant) operators, and in the worst case to have the capability for attending an anomalous situation before this happens, i.e. to prevent it. These anomalous situations generally are associated to a failure or a (logical or physical) threat detected in field. To detect such anomalies is necessary to deploy nodes sensors with capability for alerting, for instance, to nearest operators with MANETs devices on hand or a central system through the Internet. As a result, a new framework is proposed for the literature, where WSNs, MANETs and the Internet play an important role in monitoring processes, offering continuity and reliability of services. Likewise, a security analyze for this framework is provided to guarantee a secure applicability in a real context.

The remainder of this paper is organized as follows. In the Section **??**, we present the architecture and functionality of current energy control systems, analyzing their state-of-the-art control technologies and infrastructures, as well as the security problems associated to these critical energy systems. These security problems will help introduce in the Section **??** our framework, which is based on technologies described in the Section **??**. The integration and security challenges are posteriorly analyzed in the Section **??** whose application in a real case is described in the Section **??**. Finally, the Section **??** concludes the paper.

2 Energy Distribution and Control Systems

Electric energy systems began to be developed in the 20th century when electricity production plants were only associated with local loads. These loads consisted of lighting and electricity transportation, and system failures resulted in complete energy outage in the region. The increased reliance on electrical energy created a need to improve reliability. Energy stations were linked together via substations, points where the energy lines connected. The increase in labor

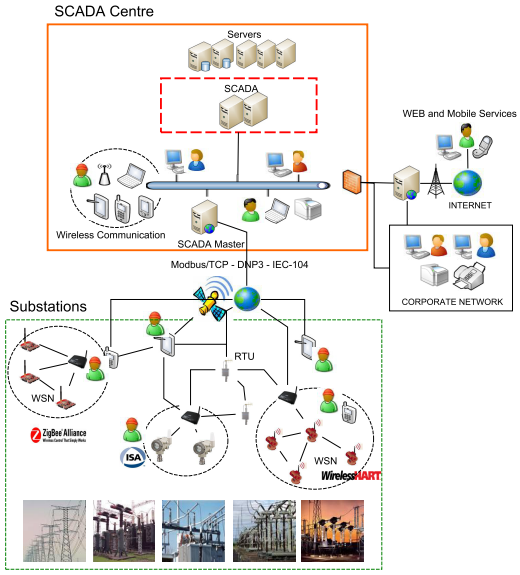

Figure 1: A Current SCADA Network Architecture

costs and number of substations brought about a need for a more sophisticated technology, the SCADA systems, in order to provide real-time remote monitoring, reducing the need for operationally ready personnel. This infrastructure, which is based on a set of ICT systems for the control, is also considered a critical infrastructure since a disruption, a failure or a (logical or physical) threat could affect the performance of the controlled systems [**?**].

Due to the criticality of the controlled system, a SCADA system must guarantee some essential properties to achieve the maximum functionality, such as performance, availability, interoperability, scalability, adaptability, reliability and security. In other words, (hardware and software) components of a SCADA system must always operate and respond in real-time. Also, new components have to be interoperable with existing industrial devices to ensure extensibility, adaptability and the economic saving. Likewise, the system has to provide reliability and security of both the offered services and the exchanged information through strict security policies, access control policies, automatic and intelligent control mechanisms, maintenance and audit processes, and the use of recommended practices [**?**].

2.1 SCADA network architecture

The corporate network is a business network based on local area networks connected to the SCADA network to gain accesses to critical data streams on SCADA servers, which are generally protected by firewalls, demilitarized zones

(DMZ) and Intrusion Detection Systems (IDSs). Thus, the organization can supervise the whole system from a global point of view. In contrast, the control center is in charge of constantly monitoring the controlled infrastructures through a SCADA master, which establishes connections to the respective remote substations under a distributed network architecture. The advantage of having a distributed system over a centralized one is that the data stream processing is shared across the network making even easier the security and configuration of the system. In addition, these control systems can support open architectures and interfaces to interact with other third parts' components [**?**].

SCADA Centre. The SCADA center is practically a data acquisition and basic processing system, where each SCADA subsystem is mainly used for both real-time operational process control and control of data processing. For example, the database subsystems are the support for the historical database and Human Machine Interfaces (HMIs) are the graphical interfaces for visualization of processes, control operations and critical data streams received from devices deployed in field. Such visualization is presented through a map-board where an overview of the entire energy distribution system, including the network architecture, is shown. This preserves as much detail as necessary for the most purposes, as well as the orientation of the energy distribution network.

Remote Substations. Remote substations are composed of Remote Terminal Units (RTUs) in charge of representing the communication interface between the remote substation and the SCADA master using, for example, either a serial line or a TCP/IP line. In particular, these RTUs retransmit to the control centre information received from their sensors close to the controlled infrastructure. If the communication is under TCP/IP, RTUs are able to open multiple sessions, use TCP/IP security services and be hierarchically configured to establish multiple communication networks. Thus the load work and functionality of the system is distributed. RTUs are also able to carry out multiple tasks for the data acquisition, management and protection. Specially, they can establish local inter-RTU communications to federate all communicating devices to a centralized point, such as for example a HMI.

RTUs can act as a data concentrator or a remote access controller as well. A data concentrator is in charge of collecting the required data from field devices and providing data exchange among systems or subsystems. In contrast, a remote access controller is responsible for the remote configuration, data retrieval and remote accesses to other field devices. It is possible to reconfigure the system architecture such that the RTU, the HMI and the data concentrator are all in a single device, or the remote access controller can work as a data concentrator. Furthermore, the RTUs guarantee data stream redundancy through the store and forward protocol. This protocol assures that information is replicated in other field devices, not only to protect critical information in anomalous situations but also to provide real-time monitoring.

Both substations and SCADA centre can also include in their network configurations different types of state-of-the-art ICTs to improve the processes of supervision and monitoring in real-time [**?**]. Such technological conglomeration includes both wired and wireless communication infrastructures, such as:

fiber optical, Power Line Carrier (PLC), microwave signal, Bluetooth, WiMAX, WiFI, TETRA, GPS, Satellite, WSNs, MANETs, and so on. Particularly, it is important to highlight that one of the most demanded technologies nowadays by the Industria is precisely WSNs. The reason is this technology is to able to provide the same functionalities as an RTU but with a low installation and maintenance cost. In fact, it is considered as an optional control technology for substations where a set of specific communication standards are available for its use, such as ZigBee PRO [**?**], WirelessHART [**?**] and ISA100.11a [**?**]. Moreover, this new alternative together with MANETs and the Internet will constitute a main part of the focus of this paper and will be developed in the remainder of sections.

Finally, the automation processes between substations and SCADA centre, and among substations, are carried out through specific SCADA protocols, which include commands (e.g. step up input voltage). These SCADA protocols contemplate both serial communication (e.g. IEC-101 [**?**]) and TCP/IP communication (e.g. Modbus/TCP [**?**], DNP3 [**?**] or IEC-104 [**?**] - both DNP3 and Modbus/TCP are the most used automation protocols by United States, whereas IEC-104/101 are the most used in Europe -). Equally, a SCADA system can establish connection with other SCADA systems using for instance the protocol ICCP (Inter-Control Center Communications Protocol)/TASE.2 (Telecontrol Application Service Element) [**?**].

The main problem associated with these SCADA communication protocols is that they lack of authentication and encryption mechanisms. Nonetheless, there are some security advances. For example, the IEC-62351 standard [**?**] offers security mechanisms to guarantee authentication and integrity, as well as confidentiality with SSL/TLS. Furthermore, a new DNP Secure Authentication (SA) specification has been recently proposed by DNP Users Group. This offers message authentication with HMAC and challenge-response to prevent replay attacks based upon NIST and ISO recommendations [**?**]. This covers both serial and TCP/IP communication, and it was considered by ISO within the DRI project to be implemented in Smart Grids [**?**]. A Smart Grid is an intelligent electric energy network that controls any operation developed in the system in order to efficiently deliver sustainable, economic and secure electricity supplies. The core of this network is precisely a SCADA system [**?**].

2.2 SCADA security challenges

As was already seen in the previous subsection, the vast majority of highly-critical control systems are composed of numerous ICTs for the monitoring and automation. These ICTs have done that the critical systems have a strong reliance on them, increasing their hardware and software capabilities. This type of complexity together with the use of TCP/IP connections and open software components have involved a notable increase in weaknesses, vulnerabilities and failures in the system [**?**]. In fact, over the last decade, a number of logical threats have been registered in public databases (e.g. BCIT [**?**], CERT [**?**]), the most of which ones carried out by malicious insiders (e.g. discontent or

malicious members of an organization) [**?**]. Obviously, the consequences can be devastating since a failure or attack could trigger massive deficiencies in essential services which may affect to a city, a region, or even a country.

It is important to comment that some registers indicate that most attacks are aimed to energy systems or SCADA systems. For instance, in 2003, a slammer worm took over a private computer network, disabling a monitoring system for nearly five hours at the nuclear energy plant Daves-Basse in Ohio [**?**]. In that same year, numerous blackouts occurred in United States and Canada, and even in Europe (Italy) because of diverse failures found in the ICT systems [**?**]. Furthermore, most of these threats are published in Internet. In February of 2000, an adversary documented and announced how to break into energy company networks and shut down power grids of utility companies in the United States [**?**]. The Department of Homeland Security (DHS) also presented a video documenting a theoretical cyber-attack on an energy station. The video showed a green diesel generator shaking violently before going into total meltdown. The DHS did not reveal the details of the attack, except that it was an over-the-Internet, man-in-the-middle attack. According to this study, the DHS tried to show that many of our critical infrastructures are subject almost to the same vulnerabilities. In fact, some other studies showed that using wireless technology, an energy system can be not only just shut down, but also caused to overload. If this attack had been carried out on a real energy plant, especially at an electrical or nuclear plant, the results could have been catastrophic.

Other of the main security problems related to these threats is the high number of misconceptions in SCADA systems [**?**]. More specifically, a SCADA system is still considered *an isolated and standalone network* due to SCADA systems were built before the advent of the Internet. Thus when the need for the Internet in a SCADA system came about, many system engineers simply integrated the Internet components into the SCADA system without any regard for how expanding the network or adding an Internet-connected node could affect the security of the system. Also, most of members of the SCADA organization believe that *connections between SCADA systems and corporate networks are secure*. The integration of SCADA systems, which is a decades-old technology, with modern corporate communication networks, poses the problem of compatibility. Thus, access controls that are designed to prevent unauthorized access from outside networks are very minimal, and often inadequate.

It is also assumed that *an extensive knowledge of the SCADA system is required to perform an attack*. In other words, the SCADA systems have special safeguards that regular computers do not have, it is a gross overstatement. In fact, any individual with moderate computer programming knowledge and a computer with network access has the means to break into a SCADA system. Moreover, due to the primitive nature of SCADA systems, it is likely that an average SCADA system is in fact more vulnerable than a state-of-the-art personal computer. Moreover, companies that employ SCADA technologies are also likely targets for cyber terrorists, who are more organized, more motivated and better than a random individual with a computer trying to test out his/her

skills as a hacker.

Another security problem is the inherent weaknesses associated to the SCADA network architecture. For instance, SCADA systems and corporate networks of a utility company are often linked. This means that a security failure in the corporate network may lead to significant security failures in the whole system, even if the strongest firewalls and IDSs exist. Furthermore, deregulation has led to the rise of open access capabilities, which have led to an equally rapid rise in the potential vulnerabilities in corporate networks [**?**]. Also, information about the corporate network of a utility company is too easily available on the web, which may be used to initiate a more focused attack on the system [**?**].

Likewise, members of an organization take access to unauthorized areas and email servers, and they use insecure web services and protocols for the remote control. Even worse, the file transfer protocols sometimes provide unnecessary internal corporate network accesses and network connections between corporate partners are often not secured by firewalls and IDSs. There is also no real-time monitoring of network data, which leads to the oversight of organized attacks over a period of time [**?**]. Finally, multitude attacks may arise (e.g. eavesdropping or Denial of Service attacks), since most of SCADA protocols are lack of security up to date (see Section **??**).

All these vulnerabilities were also detected by the U.S. Government Accountability Office (GAO) in a study done on the Tennessee Valley Authority's (TVA) energy systems [**?**]. TVA is the biggest public energy company in United States, operates 51 energy plants (including 3 nuclear plants), and provides energy for over 8.7 million people. With this case study, GAO showed that critical systems can easily be hacked into. The TVA's corporate network was loosely linked to the critical systems that control energy production, thus an adversary could exploit the security weaknesses of the corporate network to easily gain access to the energy production systems. Every firewall and IDS between the two systems were found to be easily bypassed. As a result, GAO's analysts believe a major cause for the lack of security has been the attempts to link SCADA systems to the Internet without any type of protection to this type of public infrastructure. The same analysts had reportedly launched a successful attack on an energy plant outside United States, causing an energy outage in multiple cities. A major issue in the implementation of security systems has been that there are no federal guidelines regarding such measures, and it would thus not be cost-effective to actually implement them.

Therefore, a special attention must be paid in the protection of energy control systems, where it is necessary to rigorously define security and access control policies, properly configure traditional security mechanisms, frequently carry out auditing and maintenance processes, and provide training. However, there are other security mechanisms that must be considered, such as status management and anomaly prevention. A SCADA system should have proactive tools that are capable of preventing anomalous situations, such as failures (e.g. a circuit break), threats (e.g. environment changes, bird nails, strong fluctuations/high voltage in a power line) and vulnerabilities (e.g. stresses). These preventive mechanisms help to manage the system and to detect irregular or drastic

changes in the voltage generation and distribution, thus allowing operators to react to anomalous events. The core of these mechanism can be composed of specialized sensors whose main task is to provide an accurate diagnosis of a certain critical context, detecting irregular events and reacting accurately against them by feeding determined systems known as Early Warning Systems (EWSs). In fact, if these mechanisms were able to connect to the Internet or another secondary communication link to warn of a possible change in an isolated subsystem of the real world, it would be possible to reduce significant risks and prevent the spread of the phenomenon to the whole system and other critical infrastructures. Given the importance of these prevention mechanisms for the protection of highly-critical systems, we will focus on them on the remainder of the paper.

3 A Framework for the Protection of Energy Control Systems

In order to improve the energy control processes from anywhere at any time, a new framework is presented in this section where sensors nodes, MANETs and the Internet play an important role. Furthermore, the integration of sensor nodes in the Internet and the use of the MANETs as an alternative link for the control will be the essential pieces to obtain a preventive mechanism for the protection of energy distribution and control systems.

3.1 WSNs, MANETs and the Internet

WSNs have evolved considerably in the last few years turning from a promising research field into an efficient and profitable technology. As a result, WSN has the potential to become a key technology not only to substitute traditional RTUs to a low maintenance and installation cost, but also to constantly provide protection to highly-critical systems [**?**]. Their low-powered and resource-constraint sensor nodes are autonomous devices capable of sensing information from their surroundings to measure, for example, tension in an electrical supply or a power energy wire. Such information is processed and transmitted over a wireless channel to a powerful base station, which retransmits it to a SCADA center or to the nearest operators.

The functionality of sensor nodes goes well beyond the simple retrieval of information: they can provide alerting services by checking the state of specific conditions and triggering alarms under anomalous circumstances (e.g. drastic tension changes), and they can also activate external systems in response to particular situations. Other features of WSNs are worth noting and are contributing to their adoption in industrial applications is the self-configurability. This property allows the network to adapt its topology, reacting against mobility or failure of nodes, thus providing self-healing capabilities in the case of unexpected network events. Given its relevance in the industrial and scientific field, several communication standards were recently specified, such as ZigBee

PRO, WirelessHART and ISA100.11a. All of them sharing several goals in common, such as communication reliability, security and coexistence with other communication systems, like for example mobile ad-hoc networks.

MANETs are also become increasingly important for the protection of critical infrastructure, since these can provide an alternative communication link between operators and the remote substations. Thus operators localized close to the substation can locally and directly manage the information sensed from sensors without requiring to go through the SCADA centre while offering mobility in the area. On the other hand, this network is self-organizing and can be easily deployed without any infrastructure while allowing operators to access determined points in real-time to attend critical alarms, in addition to facilitate them a quick reaction and reconfiguration of a part of the system by receiving a high level of incidences. However, the control in these types of networks could be limited to a determined distance range and a number of nodes.

On the other hand, the Internet is nowadays considered by the Industry as an important element on the deployment of new infrastructures, giving birth to Internet-based or Web-based SCADA systems. The reasons are simple. This public communication infrastructure allows the whole system to improve the control processes independently of the geographic locations and at any time, covering a set of important operational and commercial needs, for instance, real-time performance, flexibility in the acquisition and management, dissemination of information, visualization of data streams and resources (through interfaces, diagrams and multimedia), and maintenance and diagnostic processes. Thus, authorized operators can remotely access a substation from anywhere in order to check the state of the electrical generators, transmit commands or acquire/disseminate data streams. In addition, the use of open standards and open web protocols (e.g. HTML or HTTP) significantly reduces the investment in Hardware/Software (HW/SW) components. The costs are also minimized by reducing time, personal and operations in the field [**?**].

3.2 Framework: integration and security challenges

Considering the technologies discussed in the previous section, the next step is to analyze how to combine them in the same context without risking the business continuity. The result of this action will be a framework whose main objective is to assure a full coverage in the monitoring processes by taking advantage of the benefits of using the Internet and mobile ad-hoc networks. Besides, such framework has to be able to detect anomalous phenomenons and faults in the system, to constantly register the interactions among different elements and events, and to alert about failures and threats as soon as possible to respond in time.

To understand in detail the design of our approach, a set of properties (summarized in the Table **??**) have to be discussed. These properties are associated to the management, mobility, collaboration, detection, alert and response. The management is referenced to an operator's action to manage a substation (through an RTU/the station base of a WSN) with commands and queries.

Technologies	*Management*	*Mobility*	*Collaboration*	*Detection*	*Alert*	*Response*
WSN	✓ $RTU+WSN$	-	-	✓	✓	-
MANET	✓ RTU	✓	✓ $Local$	-	-	-
Internet	✓ RTU	-	✓ $Global$	-	-	-
WSN-MANET	✓ $RTU+WSN$	✓	✓ $Local$	✓	✓	✓
WSN-Internet	✓ $RTU+WSN$	-	✓ $Global$	✓	✓	✓
MANET - Internet	✓ RTU	✓	✓ $Global$	-	-	-
WSN-MANET-Internet	✓ $RTU+WSN$	✓	✓ $Global$	✓	✓	✓

Table 1: Analysis of Properties using WNSs, MANETs and the Internet

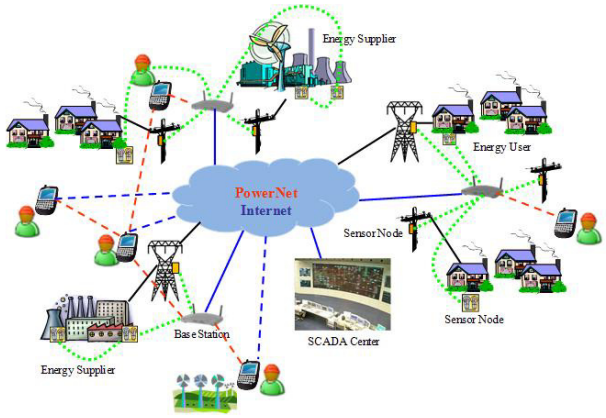

Figure 2: Integration of WSNs, MANETs and the Internet in a same Context.

Mobility is an operator's ability to move without losing the control from a substation. Collaboration is an operator's capability for interacting with another components (e.g. MANETs devices, sensor nodes, the SCADA centre). Both detection, alert and response are the ability of the system to prevent an anomalous events. In particular, the response is associated to an operator's capability to react to anomalous events. As can be noted in the table, each technology offers by themselves a set of properties useful for our approach. However the individual use of these technologies do not help achieve the requirements of our approach: control and prevention (an essential parameter for the protection). For instance, an isolated WSN in a substation can offer both management and detection but no response. To avoid this, it is necessary to use all of these technologies in a same context.

For the sake of clarity, the Figure **??** depicts an overview of how different communication technologies can interact with each other in a same industrial context. Here, the sensor nodes are deployed in the whole system, from energy suppliers to energy users for the data acquisition. These smart devices allow the system to obtain the measurements regarding energy generation, distribution and consumption, which are sent back to the SCADA center to remotely control and manage the energy distribution. In addition, as existing standards for WSNs such as ZigBee, WirelessHART and ISA100.11a provide some services

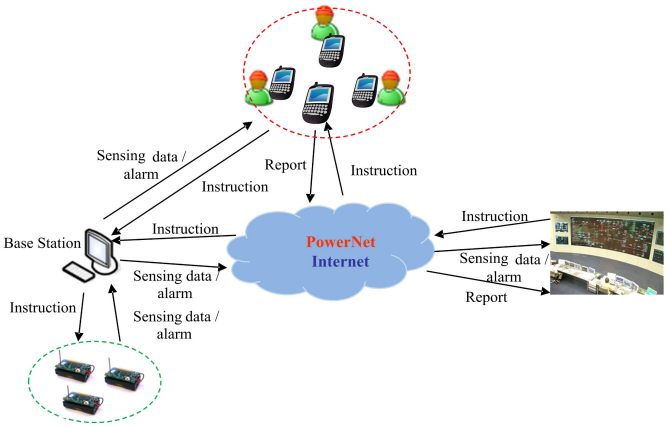

Figure 3: Conglomeration of Entities and their Communications

that allow the coexistence with other technologies, it is possible for operators in the field equipped with diverse mobile communication devices (such as a PDA, a laptop, a cell phone, and any other lightweight, easily transportable computing device) to interact with them. In fact, the connectivity WSN-MANET facilitates operators to locally manage data streams and locate a problem detected by sensors. Furthermore, MANETs allow the creation of collaborative links with other operators in order to respond immediately during extreme situations (like for example, a circuit break).

Regarding to the Internet, as we show in the Figure **??**, it glues some of the previous technologies and elements (WSNs, MANETs and the SCADA Centre) together. A WSN deployed in a remote substation can be managed by distant operators or by a SCADA centre, who receive queries in real-time, carry out control processes, and manage anomalous behaviors in real-time. Furthermore, the sensor nodes of the WSN could even access the Internet by themselves, generating alerts (due to either a failure or a threat) in order to prevent situations that may damage the normal performance of the services. As a result, the Internet help the system maximize its collaboration capabilities, offering management from anywhere at any time, as well as a timely response to assure reliability and continuity of services.

The data acquisition world (WSNs) and all other elements (e.g. the SCADA centre) are usually connected through an interface known as the base station. The role of such base station will depend on both the communication standard used and on the requirements associated to the network topology. For example, ZigBee PRO is based on a mesh/star network that contains a coordinator (a trust node in charge of managing the deployment, maintenance and control processes), routers (to help devices to transmit data to the coordinator), and sensor nodes. On the other hand, WirelessHART uses gateways, a network manager

(a trust node that could be integrated into the gateway), sensor nodes, and the existing industrial devices (e.g. an RTU). The network manager is a device with enough resources to manage the routing tables, the synchronization schedule, the network configuration and the security in the whole network. ISA.100.11a provides a network architecture that is similar to WirelessHART, but using i) backbone nodes that directly connect the Internet and ii) two specific managers that can be integrated in the gateway, one of them in charge of managing resources and communication, and the other one in charge of providing security. In any case, it is very important to identify the role of the base station. In the case of a ZigBee PRO network, it would be represented by the coordinator, whereas in a WirelessHART and ISA100.11.a network would be represented by the managers.

Another aspect that must be taken into account is the connectivity model that links the WSNs with external networks such as the Internet. Currently, three Internet connectivity models have been identified in [**?**]: *Front-End* Proxy solution (where WSNs are completely independent from the Internet), *Gateway* solution (where WSNs retain their protocol independence but are able to exchange information directly with Internet hosts) and *TCP/IP* solution (where WSNs implement a TCP/IP-compliant stack). In order to find the most adequate solution for our critical application context, it is necessary to consider the complexity and effects of these solutions. In our particular case, the system must access data streams and issue control commands, tasks that can be provided by the Front-End solution. Such solution will centralize all the computational overhead in a set of base stations, whose task will be to parse and store any type of information (allowing the existence of an historic repository and store-and-forward strategies), and interpret and translate control SCADA commands to a protocol that the sensor nodes can understand. On the other hand, in the TCP/IP solution and in the Gateway solution, the external entities will have to interact directly with the sensor nodes. This can be problematic in a critical context, mainly due to the capabilities of the nodes: the sensor nodes will be specially vulnerable against attacks launched by remote entities, and there will be an extra overhead caused by the management of the protocols and the security services. Nevertheless, note that there can exist special nodes (i.e. a "backbone" of nodes) that can connect to the Internet by themselves, sending special messages such as alarm messages.

As for security, it needs to be carefully considered in our framework, as data streams have to be transmitted among different types of networks and processed on different types of devices with very different capabilities. In a particular case, an attacker may, for instance, target some link to isolate determined system parts. To avoid this fact, cryptographic primitives and protocols need to be designed carefully, and the block size of ciphertext and the packet size need to be optimized according to the message type in order to minimize unnecessary padding. The impact is especially important for WSNs so that these will reduce the communication overheads, and thus saving the restricted bandwidth, reducing the traffic jam and packet loss, in addition to save energy consumption to extend their lifetime. Authentication and access control across

different network domains is another example. It should consider the complicated topologies of different networks and the different roles of mobile devices, and authentication issue and access control in a unified way in pervasive mobile networking environment. Following on this same line, the authorization should also be considered to prove an entity's identity and rights to manage measurements, alarms or instructions.

Other security aspects to take into account in critical systems are availability, detection and accountability. Availability allows a system to get services and data streams independent of the real state of a node (e.g. without connectivity or energy) in the network. To this end, it is necessary to implement mechanisms and protocols that provide data redundancy, or manage backup copies in high resource systems, like a base station. Likewise, detection and accountability are achieved by implementing specific incident management mechanisms in charge of registering the sequences of events that happen within the system. Such functionality can be mainly performed by the base station, which acts as the link point among different communication networks. It will analyze the information traffic and the internal behavior of each network, registering anomalies and/or events occurred.

The system must also guarantee reliability in the communications to satisfy the critical infrastructure protection standard [**?**]. This requires that the sensing data streams and alarms should reach the SCADA control center securely, reliably and timely. Attacks that target part of the communication channels spanning different network domains should not stop the transmission of critical information. This dependency implicates that backup communication paths should be available when the normal path is under attack. In addition, it is also important to take into account some security issues related to the integration of a WSN to the Internet [**?**]. For example, in the particular case of a Front-End solution, an adversary could take advantage of the centralized nature of the base station in order to disrupt its functionality. A way of mitigating this fact would be to increase the number of base stations (redundant systems) so as to improve their availability. Also, a base station has to be configured with security mechanisms, which must protect the information flow between it and an Internet host under a formal security standard, and between it and the sensor nodes under a security approach defined for WSNs. Finally, the sensor nodes themselves must be able to manage any type of incidence, guaranteeing a timely response, and allowing reconfiguration and self-healing.

3.3 Case study: an energy distribution and control system from Singapore

A particular case study of an energy system from Singapore is presented here in order to understand the applicability of the framework proposed in the previous Section. Singapore is at present one of the most prepared countries for the electricity business, however this does not exploit the advantages of determined technologies such as the Internet, MANETs and WSNs. In particular, its the energy distribution systems are designed as a completely underground system for

multiple reasons, mostly environmental and aesthetic, but also due to the sever lack of space in the country [**?**]. Regarding remote control substation, Singapore uses a system similar to a SCADA system to monitor and control information. The integrated Substation Control System (SCS) offers a platform for the integration of control, monitoring and protection systems into one efficient system. Furthermore, the system can be supplemented with IEDs (Intelligent Electronic Devices) deployed throughout the energy station for diagnostic and monitoring purposes.

Mainly, the SCS is used for control, monitoring and protection of all primary and secondary equipment within a substation. All components are equipped with self-check and diagnostic functions to ensure functionality and availability of the system. Multiple levels of duplication exist within the SCS to ensure reliability in case of failure of individual components. This duplication is also used as an added security measure. On the other hand, the Network Control Center (NCC) is a collection of computers interlinked via a local area network, with the computations distributed among them to ensure parallel processing. In definitive, a Singapore's NCC network architecture is certainly analogous to a SCADA system with each SCS acting as a SCADA slave.

Communication between the SCS and the subsystems is achieved using fiber optic cables. While this is a reasonably secure communication, there is still no encryption for communication between these levels, and this can be viewed as a security threat. Although, some communication lines between the SCS and NCC is currently done via a PLC (Power Line Communication), these are being quickly replaced by fiber optic cables due to Singapore's small size. In other words, this is a reasonably cost-effective solution. However, these energy lines can potentially be tapped at any given energy supply node, given the right equipment. Lastly, communication between the SCS and NCC are relayed using the IEC-101 protocol. All communication controllers and substation computers between these two levels are equipped with full redundancy [**?**].

Still, we believe that this type of energy system could be improved with the use the Internet, since this allows system to connect in real-time remote SCSs. Thus the NCS and distant operators could known at any time the real situation of a part of the system. The mobility is another issue to consider in these types of networks in order to facilitate authorized and authenticated operators a better functionality in area. This mobility is reached through MANETs whose devices gain accesses to critical information from determined substations. Lastly, these SCSs could even take advantage of the functionality of sensor nodes to assure reliability and continuity of their services. Therefore, we are convinced that the energy system from Singapore may be improved in a future if our framework is considered.

4 Conclusions

Energy distribution and control systems are two of the most important systems serving nowadays in our society, since their services are becoming increasingly

necessaries for the social and economic being-well. Due to this need a set of security and protection mechanisms must be considered, since a failure or threat could mean an drastic change in the distribution of such services. Even, such change may affect the continuity of other critical infrastructures, generating a serious or harmful cascading effect. So far, a set of traditional protection mechanisms and recommendations have been proposed; however it is not really enough. We believe that proactive and intelligent mechanisms must also be recommended within literature, since they could prevent anomalous events before a possible failure/threat occurs. For this reason, we are convinced that sensor nodes belonging to a WSN could help operators in field to timely react to a possible effect. However, this is not still enough. It is necessary to adopt MANETs devices and the Internet to a same context in order to receive queries and alerts in real-time from anywhere and at any time.

As a result, a framework has been proposed in this paper. This connects different communication infrastructures (WSNs, MANETs and the Internet) to provide different capabilities (which are summarized in the Table **??**). The result is a collaborative system where the control, mobility, detection, alert and response constitute the main focus on our framework. On the other hand, some security and integration issues have been also discussed to analyze its applicability in a real context. In particular, in an energy control system from Singapore.

Acknowledgments

This work has been partially supported by the projects: A*STAR (SEDS-0721330047), PROTECT-IC (TSI-020302-2009-10), ARES (CSD2007-00004) and SPRINT (TIN2009-09237), being the last one also co-funded by FEDER. The first author has been funded by the Spanish FPI Research Programme.

References

[1] Peerenboom J., Fisher R., Analyzing Cross-Sector Interdependencies, IEEE Computer Society, HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences, IEEE Computer Society, 2007, pp. 112-119.

[2] Alcaraz C., Fernandez G., Roman R., Balastegui A., Lopez J., Secure Management of SCADA Networks, New Trends in Network Management, CEPIS, 2008, vol. IX, no. 6, pp.22–28.

[3] U.S. Department of Energy, 21 Steps to Improve Cyber Security of SCADA Networks, white paper, 2005.

[4] Rahkonen T., Cegrell T., A Study on Techniques for and user requirements on Systems Integration in SCADA/EMS, Royal Institute of Technology, Power Industry Computer Application Conference, 1995.

[5] Khatib A., Dong X., Qiu B., Liu Y., Thoughts on Future Internet Based Power System Information Network Architecture, Virginia Tech, Power Engineering Society Summer Meeting, 2000.

[6] ZigBee Alliance, http://www.zigbee.org/, [March 2010].

[7] HART Communication Foundation, http://www.hartcomm2.org/hart_protocol/wireless_hart/hart7_overview.html, [March 2010].

[8] ISA100, Wireless Systems for Automation, http://www.isa.org/Content/NavigationMenu/Technical_Information/ASCI/ISA100_Wireless_Compliance_Institute/ISA100_Wireless_Compliance_Institute.htm, [March 2010].

[9] IEC 60870-5-101, Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks, Second edition 2003-02.

[10] Modbus-IDA the architecture for distributed automation, http://www.modbus.org/, [March 2010].

[11] DNP3, DNP Users Group, http://www.dnp.org, [March 2010].

[12] IEC 60870-5-104, Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles, Second edition 2006-06.

[13] IEC 60870-6, Telecontrol Equipment and Systems, International Electrotechnical Commission, http://www.iec.ch, [March 2010].

[14] IEC-62351, Power Systems Management and Associated Information Exchange - Data and Communication Security, International Electrotechnical Commission, http://www.iec.ch, [March 2010].

[15] EPRI, DNP Security Development, Evaluation and Testing Project Opportunity, Electric Power Research Institute, http://mydocs.epri.com/docs/public/000000000001016988.pdf,[March 2010].

[16] ISO New England, DRI Project: DNP Secure Authentication, http://www.iso-ne.com/committees/comm_wkgrps/othr/dritwg/mtrls/iso-ne_dri_project_-_dnp_secure_authentication_recommendation.pdf, [March 2010].

[17] European Technology Platform, SmartGrids - Strategic Development Document for Europe's Electricity Networks of the Future, 2008.

[18] Cardenas A., Amin S., Sastry S., Research Challenges for the Security of Control Systems, 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), San Jose, USA, 2008.

[19] BCIT, British Columbia Institute of Technology, http://www.bcit.ca/, 2009 .

[20] CERT, Carnegie Mellon Software Engineering Institute, CERT/CC Statistics, http://www.cert.org/stats/vulnerability_remediation.html, 1988-2009.

[21] Chikuni E., Dondo M., Investigating the Security of Electrical Power Systems SCADA, AFRICON, 2007.

[22] Dacey R., Critical Infrastructure Protection: Challenges in securing control systems, Information Security Issues. U.S. General Accounting Office, 2003.

[23] Bialek J., Critical Interrelations between ICT and Electricity System, Electricity security in the cyber age: Managing the increasing dependence of the electricity infrastructure on ICT (NGInfra), Utrecht, The Netherlands, 2009.

[24] NERC Power Industry Policies, IEEE Industry Applications Magazine, 2004.

[25] Riptech, Understanding SCADA System Security Vulnerabilities, WhitePaper, Riptech, Inc., 2001.

[26] Choong S., Deregulation of the Power Industry in Singapore, APSCOM, 2000.

[27] Pollet J., Developing a Solid SCADA Security Strategy, Sensors for Industry Conference, 2002.

[28] Riptech, Inc., Understanding SCADA System Security Vulnerabilities, 2001.

[29] Barkakati N., Wilshusen G., Deficient ICT Controls Jeorpardize Systems Supporting the Electricity Grid - A case Study, Electricity security in the cyber age: Managing the increasing dependence of the electricity infrastructure on ICT (NGInfra), Utrecht, The Netherlands, 2009.

[30] Lopez J., Alcaraz C., Roman R., On the Protection and Technologies of Critical Information Infrastructures, On Foundations of Security Analysis and Design IV, LNCS 4677, Springer, 2007, pp. 160-182.

[31] Smith M., Web-based Monitoring & Control for OilGas Industry, SCADA's Next Step Forward, Pipeline & Gas Journal, 2001.

[32] Roman R., Lopez J., Integrating Wireless Sensor Networks and the Internet: a security analysis, Internet Research, 2009, vol. 19, no. 2, pp. 246–256.

[33] Lopez J., Montenegro J., Roman R., Service-Oriented Security Architecture for CII based on Sensor Networks, International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06), Lyon, France, 2006, pp. 1–6.

[34] Chang S., Chua K., Siew C., Tan T., Power Quality Initiatives in Singapore, CIRED2001, Singapore, 2001.

[35] Yoon K., Teo D., Controlling and Monitoring Singapore's Underground Grid, 1999.