Security Aspects of SCADA and DCS Environments

Cristina Alcaraz, Gerardo Fernandez and Fernando Carvajal

October 29, 2015

Abstract

SCADA Systems can be seen as a fundamental component in Critical Infrastructures, having an impact in the overall performance of other Critical Infrastructures interconnected. Currently, these systems include in their network designs different types of Information and Communication Technology systems (such as the Internet and wireless technologies), not only to modernize operational processes but also to ensure automation and real-time control. Nonetheless, the use of these new technologies will bring new security challenges, which will have a significant impact on both the business process and home users. Therefore, the main purpose of this Chapter is to address these issues and to analyze the interdependencies of Process Control Systems with ICT systems, to discuss some security aspects and to offer some possible solutions and recommendations.

1 Introduction

As already commented in Chapter 4, *Process Control Systems* (PCS) are complex systems that perform some defined tasks as part of an industrial production process. In particular, they are considered the main control framework for other critical infrastructures. These systems monitor and supervise remote sensors deployed close to the critical infrastructure, managing automation operations and recording sensitive data measurements. In the existing literature, there are two types of PCSs [1]. They are differentiated by their geographical distribution, i.e.:

- *Supervisory Control and Data Acquisition* (SCADA) System. A SCADA system is a distributed network over large geographic areas where a set of industrial automation services are offered to control the performance and continuity of other critical infrastructures, such as: electric energy systems, nuclear energy systems, water and sewage treatment plants or transportation systems.
- *Distributed Control Systems* (DCS). These systems have the same functionality as a SCADA system but they are geographically closer to manufacturing operations and industrial facilities. It is very important to

highlight that throughout this chapter, we will use the term SCADA to cover any monitoring and control procedure for both SCADA systems and DCS systems.

Historically, SCADA systems were composed of isolated networks without connection to public communication infrastructures, like the Internet. However, the need to remotely supervise and control critical industrial systems has meant the convergence of state-of-the-art information and communication technologies, such as the use of open software and hardware components (i.e., commercial off the shelf components (COTS)), the Internet and wireless technologies. These last two technologies are precisely the most demanded by today's Industry. Wireless technologies provide mobility and local control with a low installation and maintenance cost, whereas the Internet allows monitoring to take place from any place and at any time. Therefore, the TCP/IP standard is the main communication in SCADA transmissions and its commands and data streams are transmitted over a variety of specific IP-based protocols to facilitate automation and control in real-time over the Internet. On the other hand, the performance and survivability of a critical control system is also very dependent on the type of internal and external organization whose stakeholders (such as other critical systems, government and end users) may have a significant influence on monitoring processes.

From a security point of view, it is very important to take into account that technological convergence in critical control systems could give rise to new security risks, and challenges to resolve, some of them related to the secure management of ICT systems in both SCADA systems and corporative networks, and also related to the constant monitoring of threats and failures in the whole system. Any potential attack, failure or threat could have a significant impact on any of the different interdependent critical systems (see Chapter 4 for more detail). All of these security issues will be the main focus of this Chapter, where a set of security requirements and solutions including policies, standards, methodologies and software components will be discussed to facilitate the control and automation in SCADA and DCS systems.

The chapter is organized as follows: Section II presents the SCADA architecture, its technological advances and its functionality using some existing ICT systems, in addition to discussing interdependencies and their consequences between critical control systems and ICT systems. Section III describes secure management needs beyond the ICT of SCADA systems due to their peculiarities as survivable complex systems. Likewise, in Section IV an exploration of current researches regarding intrusion detection systems and forensic needs for the analysis of incidences is presented. Finally, Section V concludes the Chapter and some future lines of work are outlined.

2 Advances in the SCADA Architecture and Security Issues

Since SCADA Systems were first introduced in the 1960s, three main generations have been emerged: *Monolithic, Distributed and Networked*, all of which share a number of characteristics. Firstly, they have adopted the existing ICTs in order to improve the monitoring processes in real-time, as well as the performance and availability of controlled infrastructure (e.g. large industrial lines of oil pipelines). Secondly, they share three types of sub-networks: (i) the central network, (ii) remote substations and (iii) the corporative network. The operations carried out in the central network are related to the control and management of the critical infrastructures. Such operations are managed through specific operator consoles or human-machine interfaces (HMIs), which allow operators to read specific physical parameters (e.g. pressure, electrical signals, temperature, etc) or alarms received from remote substations, or even transmit certain commands (e.g. open/close pumps) to specific field devices localized in remote substations. On the other hand, the operations carried out in the corporative network are directly related to the general supervision of the system whose accesses databases and servers installed in the central network are rather more restricted.

The first SCADA networks were designed in the *Monolithic* generation under a centralized control in a mainframe system. This mainframe was configured as the primary control system; while another mainframe system was configured as the standby in order to cover any functionality of the system in the event of a failure in the main system (see Figure 1, left). Both systems had to register critical data streams, manage and make decisions to efficiently coordinate the monitoring processes developed in the whole system. The architecture of a substation was basically based on one or several special remote terminal units (RTUs), which had limited memory and processing capabilities (e.g. 8-bit microprocessor and 4-16 KB RAM) with output/input (O/I) interfaces to measure/actuate physical signals. These signals had to be retransmitted to the central system via telephone or radio with a low data transmission rate and through property automation protocols such as for instance Modbus serial or IEC-101. Although it meant a great advance in the Industry, the use of property components limited the coexistence with other hardware and software industrial components.

Later, in the second *Distributed* generation of SCADA systems, (see Figure 1, right) new technologies were integrated based on IP addresses so that the monitoring processes were distributed among different network components. The distributed approach significantly substituted the centralized systems whose main components were based on data base servers to register alarms and measurements, master terminal units (MTUs) to establish communication with the substations and HMIs. In addition, the network architecture helped the whole system to improve the primary/standby scheme of the Monolithic generation, as any active device in the network could immediately cover the functionality of

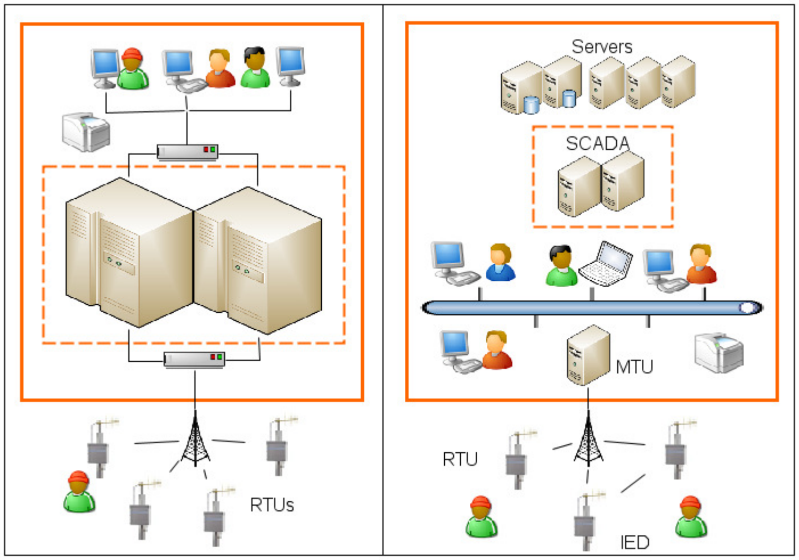

Figure 1: A centralized and distributed SCADA system.

another one without having to wait for the change from primary to secondary. The communication with remote substations was established using large (distributed or hierarchical) local-area networks, which were controlled by MTUs installed in the central system. The RTUs, configured in such substations, were equipped with advanced serial I/O interfaces with faster microprocessors, memory and math coprocessors to support complex applications, becoming more intelligent and autonomous than previous RTUs. However, both automation protocols and telemetry components continued to be properties.

Finally, the latest advances in SCADA systems are seen in the third generation of *Networked* generation. This generation broke with the isolation concept of the previous generations by including in its network designs open connections using the TCP/IP (Transmission Control Protocol/Internet Protocol). These connections made possible monitoring in real-time, peer-to-peer communication from anywhere at any time, multiple sessions, concurrency, maintenance, redundancy, security services and connectivity. All these technical advances also came to substations, where RTUs were able to provide hierarchical and inter-RTU communication (i.e., interconnectivity among RTUs) under TCP/IP, wired and wireless communication interfaces, Web services, management and forwarding to other remote points. This fact helped RTUs work as data concentrators to store large data streams or as remote access controllers to autonomously and remotely reconfigure/recover parts of the system.

The migration to TCP/IP also involved the standardization and implementation of new SCADA protocols capable of understanding TCP/IP connections.

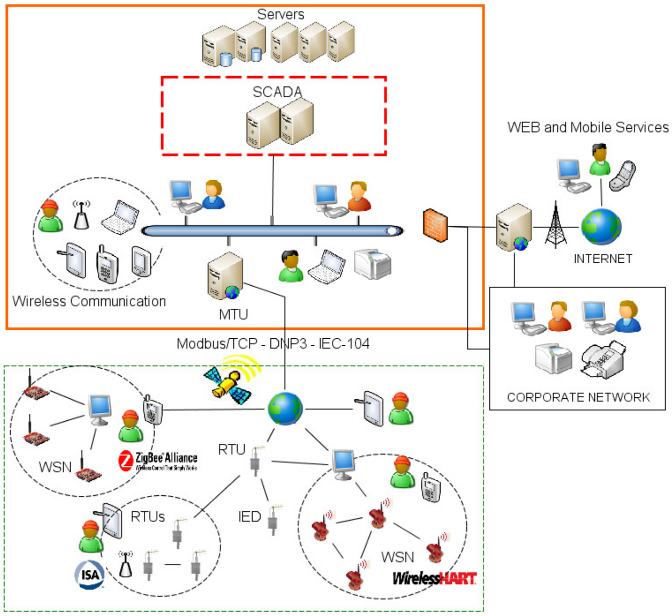

Figure 2: A current SCADA system.

Currently, there are several IP-based SCADA protocols, such as Modbus/TCP, DNP3, IEC-104 and ICCP/TASE2. The three first ones are for the automation, whereas ICCP is specific for the inter-communication between telemetry control systems. However, these protocols lack authentication and data encryption mechanisms at present. For this reason, new standards have been recently specified, such as for example the IEC-62351 or DNP Secure Authentication (SA). Basically, IEC-62351 provides confidentiality with SSL/TLS, authentication and integrity while DNP SA ensures authentication with HMAC and challenge-response.

2.1 The Internet and Wireless Communication in the Networked Generation of SCADA systems

Following on with the Networked Generation and observing Figure 2, it is possible to note that for a recent future, the control Industry might be one of the main sectors that might be more demanding on the use of wireless technologies and the Internet for the control. Both technologies offer a set of suitable services for control in real-time. Wireless technologies allow operators in the field to locally manage substations, providing mobility and at the same time coexistence with a low installation and maintenance cost. In contrast, the Internet offers remote control of substations, where the SCADA center and operators in the field can interact independently of their geographical location. To understand in detail the advantages of these technologies, an overview is provided below.

2.1.1 The Internet

As was previously commented, the Internet is one of the most demanded technologies by Industry. This special interest is due to the fact that the Internet provides global connectivity independently of the physical locations of components/members of a system. Its public communication infrastructure offers Web solutions, as well as flexibility in the data acquisition and management, data dissemination, maintenance, diagnosis, and interfaces to visualize data streams and resources in real time. In addition, the use of open standards and open Web protocols (e.g. HTML, HTTP or HTTPS) can also significantly reduce costs in terms of hardware and software, time, personnel and field operations [2]. As a result, researchers, engineers and commercial companies are jointly working to study the impact of using the Internet and Web solutions in critical control systems. For instance, Qui et al. proposed in [3] a WSDS (Web-based SCADA Display Systems) system to access the system through the Internet. The same authors also proposed a Web-based SCADA display system based on very-large-scale integration (VSLI) information technologies in [4]. Similarly, Leou et al. proposed in [5] a database management system to centralize the critical data received, providing a Web-based power quality monitoring system. Li et al. presented in [6] a Web-based system for intelligent RTUs with capability for interpreting HTTP. Jain et al. presented in [7] a Web-based expert system for diagnosis and control of power systems. Lastly, several commercial companies, such as for instance Yokogawa [8] or WebSCADA [9], have some Web control solutions already available for the market.

Nevertheless, the use of the Internet could give rise to new security threats and reliability problems in the system. Examples of attacks may be intercepted communication channels, disruption of services, isolation or data alteration. One way of protecting the communication channels could be to use SSL (Secure Sockets Layer)/TLS (Transport Layer Security) services offered by the TCP/IP standard, hard cryptographic primitives, hash functions, key management systems and intelligent mechanisms, such as Intrusion Detection Systems (IDS), Firewalls or Virtual Private Networks (VPNs). This last security mechanism may even be considered a cost-effective high speed communication solution between substations and the SCADA central network over a shared network infrastructure, while simultaneously providing both the functionalities and the benefits of a dedicated private infrastructure [10]. On the other hand, it is also necessary to configure authentication mechanisms to verify the authorized access resources and services in the system, as well as authorization mechanisms to prove an entity's identity and rights in the management of critical data and commands. Data redundancy mechanisms should also be installed to ensure the data availability at any time and from anywhere, as well as registering incidents or anomalous events occurring. Security policies should be put in place and frequent training courses should be available to users to avoid unintentional actions.

2.1.2 Wireless Communication

Another essential technology in automation and control processes is wireless communication, for several important reasons. This technology is able to provide (1) control as a wired infrastructure but with a low installation and maintenance cost, (2) mobility and (3) connectivity with other control components independently of the environmental conditions. To be more precise, many of the critical infrastructures control conditions which are impossible for humans to monitor in person (e.g., high/low temperatures, high/low pressures, noise, underground water/oil pipelines, etc.). These critical conditions force systems to deploy autonomous and intelligent devices in order to cover certain functionalities in these areas (e.g., robots, automation vehicles, sensors, active RFID devices, etc.). In fact, the vast majority of wireless technologies have already been proposed to be included in industrial control networks, such as Bluetooth, WiFi, Mobile technology (UMTS, GPRS or TETRA), Satellite, Global Positioning System (GPS), WiMAX, microwave, Mobile Ad-hoc Networks (MANETs), or Wireless Sensor Networks (WSNs).

Furthermore, a hybrid configuration with different technologies could improve the monitoring processes since each technology could incorporate its own inherent capabilities into the subsystem or the whole system. For instance, WSNs could offer control as an RTU while ensuring prevention of abnormal situations thanks to their sensor nodes, which are equipped with a 4MHz-32MHz micro-processor, 8KB-128KB RAM, and 128KB-192KB ROM, and constantly measure environmental data associated to temperature, pressure, vibration, light intensity, etc. Generally, and depending on the application context, the nodes are linked to an energy supplier or to industrial equipment in order to maximize their lifetime (by between 5 and 10 years). Their sensor nodes, smart and autonomous devices, are capable of processing any information sensed from their sensors and transmitting it to a central system with considerable hardware and software resources, such as for example an RTU working either as a data collection device. Taking advantage of these technical capabilities, field operators may locally access an RTU to manage the real state of substations using for instance a portable device (like a PDA). They can also manage incidences or anomalous events detected by sensor nodes, such as failures (e.g. circuit breaks, leaks) and threats (e.g., environmental changes, strong fluctuations/high voltage in a power line), maximizing the reaction range to prevent a possible effect in cascading. Furthermore, its wireless communication has been recently standardized to ensure the secure control, coexistence with other ICT systems, reliability in the communications and constant performance. Currently, there are three standards: Zigbee PRO, WirelessHART and ISA100.11a, which are depicted in the Figure 2.

However, due to the critical nature of the application context, the nature of wireless networks, which tend to be generally susceptible to attacks, and the vulnerable nature of the technology used, it is necessary to ensure security and reliability in wireless monitoring processes. For example, the security in WSNs is mainly supported by Symmetric Key Cryptography (SKC) primitives because of the high hardware and software constraints of the sensor nodes.

2.2 Interdependencies, Consequences and Security Challenges

So far, we have seen that the vast majority of critical control systems are composed of numerous ICTs for the monitoring and automation. This type of complexity together with the use of TCP/IP connections, wireless communication and open software components have caused a notable increase in weaknesses, vulnerabilities and failures in the system [11]. In particular, a number of logical threats over the last decade have been registered in public databases (e.g. BCIT (British Columbia Institute of Technology), CERT (Carnegie Mellon Software Engineering Institute)), most of which are 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 a city, a region, or even a country.

Some examples in the real life have shown the importance of protecting these types of critical systems. For example, 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 [12]. In that same year, numerous blackouts occurred in United States and Canada, and even in Europe (Italy) because of various failures found in the ICT systems [13]. Furthermore, most of these threats are published on the 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 [14]. 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 not only be 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.

Another 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* because 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 how to expand the network or how 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, to say that SCADA systems have special safeguards that regular computers do not have 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 Intrusion Detection Systems (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 [15]. 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 [16].

Likewise, members of an organization obtain 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 [17]. Finally, multitude attacks may arise (e.g. eavesdropping or Denial of Service attacks), since most SCADA protocols lack up to date security (see Section 2).

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 [18]. TVA is the biggest public energy company in United States, operating 51 energy plants (including 3 nuclear plants), and it 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 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 the 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, special attention must be paid to the protection of control systems, where it is necessary to rigorously define security and access control policies, properly configure traditional security mechanisms (in communication servers or Base Data serves, Operative Systems, HMIs, backup systems, etc.), frequently carry out auditing and maintenance processes, authentication, authorization, and provide training. However, this is not enough. It is necessary to configure intelligent management mechanisms to take over alarms and incidences efficiently and at the appropriate moment, as well as to configure status management and anomaly prevention mechanisms, which must be able to recognize SCADA protocols, such as DNP3, Modbus, IEC-104 or ICCP. Furthermore, these preventive or proactive mechanisms could feed Early Warning Systems (EWSs) to help systems to react to an anomalous event appropriately (see the Chapter 6 titled *Early Warning and Attack Detection Mechanisms* for more detail), and in the worst case to feed forensic procedures and recover protocols based on specific methodologies, techniques, policies and standards. All of these security issues and others are the main focus of this chapter and they will be described in detail in the remainder Sections.

3 Security Management in SCADA Systems

SCADA systems are complex systems that can be compared to a living organism. Managing this complexity and their security aspects, interactions and interdependencies is also a complex task which should be broken into parts; starting for their overall architecture [21], [22] that should be in compliance with corporate policies. Initially, the overall architecture should comply with corporate policies.

We should be aware of the differences between ICT and SCADA systems based on their security properties as noted in ANSI/ISA-99.00.01-2007 standard. SCADA system imposed strong real hard real time response, i.e. imposes fixed constrained on the maximum communication time. Moreover, in some situation such constraint should be also very tight with time response of one millisecond range whereas ICT business systems have a permissible time responses of seconds.

We should not forget that these differences have to be taken into account when applying high level control objectives and technical controls (as defined in ISACA CobiT and reviewed in [23], [24].

These studies show that SCADA systems overall management should not be so different from ICT, depending on their, more or less, critical live environment. Apart from the need of creating a novel brand of applicable security standards, policies controls, recommendations and assessments; still there are a great deal of reusable similarities and common applicable security processes to improve their "survivability" capacity to be effective and sustainable for the entire system lifecycle [24].

3.1 Policies, Standards and Organizational Issues: Managing Complexity

Security Management has been intensively studied on ICT systems in relation to cybersecurity, but SCADA Systems have had more physical security concerns due to the isolation and proprietary protocols historically used. Applying the knowledge acquired in managing ICT systems to the protection of SCADA networks and associated CII (Critical Information Infrastructures) is not so straightforward and it requires some integration efforts and particular adaptations to standard security tools and best practices management.

Currently, several standardization initiatives for applying best management and security practices for industrial communication systems are under way. For any system, a security policy must be defined and the security measures must be derived from that security policy.

For example, the ISA99 Committee SP99 has published three guidance documents on introducing ICT security to existing industrial control and automation systems. The first report ANSI/ISA-99.02.01-2009 [25] provides recommendations for a security architecture, and for procedures to achieve and maintain security, including auditing. It describes elements for setting up a cyber security management system and provides guidance on how to meet the requirements for each element. It covers major topics of security management: policies, procedures, practices, and personnel. ICT also serves as the basis for all the standards in the ISA99 series by presenting key concepts, terminology, and models. The second report ANSI/ISA-99.00.01-2007 is a comprehensive survey of the state of the art in security technologies and mechanisms, and it provides comments on their applicability for the plant floor. The third technical report ANSI/ISA-TR99.00.01-2007 provides an updated assessment of various cyber security tools, mitigation counter-measures, and technologies that may be effectively applied to SCADA networks and electronically based industries and critical infrastructures. It describes an overall view of control system-centric cybersecurity technologies: threats, cyber vulnerabilities, and recommendations guidance for using these cybersecurity control objectives.

SCADA security management means the implementation of technical and operational controls coupled with the organization's business model in terms of investment and return of inversion subject to requirements. This means that security governance has to be a continuous effort to keep a system secure in operation and should deal with two major concerns: security architecture design, operational management and effective, survivable and sustainable system lifecycle: design, installation, operation, maintenance, continuous assessment and retirement [26] ISO/IEC TR 17971, [27]. The security issue should be enforced by using a good security policy, together with a security plan and implementation guidelines. All of them can be drawn together by the existing processes interdependencies of the organization and can be structured through common building blocks [28]. This managing tasks means implementing a security policy, knowing the risks and threats, enforcing the principles of least privilege, need to know and segregation of functions; open security design instead of relying on security by obscurity, classifying information, implementing defense-in-depth, using proven cryptographic algorithms, protocols and products; and last but not least, being conscious of human factor needs: behavior, awareness and formation. Without being exhaustive, there are widely accepted standards for security related to ICT systems widely accepted, which in conjunction form the basis for establishing a security control framework. The ISO/IEC families ISO/IEC 13335-X, ISO/IEC 270XX, 27001, 27002; the corporate governance of information technology standards ISACA CoBit and ISO/IEC 38500:2008, ISO/IEC 20000. In addition to U.S. GAO documents "Challenges and Efforts to Secure Control Systems" [29], NIST 800-XX Guides, especially [30] (SP800-82), and its Forum "Process Control Security Requirements Forum" (PCSRF). In the EU CPNI SCADA protection guides [31] and the recompiling effort of ESCoRTS project (European Network for the Security of Control and Real Time Systems) [32].

Security management is a continuous improvement process that for SCADA systems needs a extended and complementary approach beyond traditional ICT security processes. In one hand this implies developing proper metrics based on the existing enterprise risk assessment strategies and other hand developing a comprehensive framework that should allow risk reduction by selecting, applying and assessing an appropriate and integral set of sustainable security control objectives that meet the company's business goals [27]. Furthermore, this may involve modelling a complex system that may have many possible configurations, that even may be inconsistent with the operational system security policies. Such a complex system would offer multiple functions with a complicated internal structure of architectural components that are being part of an overlying CII. However accepting residual risks for these operational systems means evaluating them as a whole, through a well-defined configuration management plan, an auditing program and assessment plan that could make possible acceptance of their certification or/and accreditation [26] ISO/IEC TR 17971. Nevertheless, in part our lack of understanding these systems and cope with their risks arises (in part) from our inability to understand complex systems and modeling them through conceptualizing their component parts and security domains at the required decomposition level in which they can be described, evaluated and assessed [33]. Hence, to provide a complete security perspective for protection of the whole specific system, it should be necessary to establish a certifiable methodology that contributes to the adequate protection, detection and communication mechanisms, based on the current risks, interdependencies and interoperability needs of the whole system.

3.2 Risk Assessment

According to the principle of proportionality, almost all Security Management best practices agree that risk management must be aligned with business goals and used continuously to evaluate the need for protection during the operational system lifecycle, helping in this way to determine the selection, implementation and assessment of security controls in order to mitigate risks and to counter or minimize current existing security risks to a system.

SCADA systems are somewhat special because they can be an essential part of a Critical Infrastructure (CI), they are not isolated inside the company and their current threats are slightly different from those of ICT systems [34]. Their risks can change more frequently than those of ICT systems; which raises three main points of concern to deal with: the need of an *inventory catalog* that may identify assets, threats, impacts, attacker potentials, possible applicable controls and a *clear evaluation criteria* for selecting each of them and a *communication model*, with a dynamic approach, for risks analysis results, threats and incidents information exchange in order to improve crisis management and coordinate response of involved actors.

3.3 Focus on Security Assessment

As stated previously the evaluation and security assessment of operational systems has not been as methodical as expected; but somewhat crafted. This can be feasible for in house developed components or systems parts; but not for a system that may have many external or internal dependencies and may be part of a critical infrastructure. Current security assessment efforts [26] ISO/IEC TR 17971 propose a methodological approach which is an extension of the ISO/IEC 15408-x to enable the security assessment (evaluation) of operational systems. This approach offers guidance on assessing both the information technology and the operational aspects of these operational system and can be reinforced by other methodological specifications (ITSEC, Common Criteria, OWASP, SSE-CMM/ ISO/IEC 21827).

The currently undergoing eCID project[35] is developing a new certifiable methodology approach focused on protecting CI and their SCADA systems as a whole composed of industry sectors security domains. This methodology should be technologically applied through an underlying architecture of controls based on current risks that could be evaluated depending on the defined protection profiles requirements. This project tries to fill some of the gaps for accreditation and assessment described in the I3P Institute report [33]. Basically, this approach proposes a framework for protecting SCADA systems jointly with ICT systems involved. The problem must be tackled from a defense in depth perspective in which, at least, there are five layers to develop: prevention, protection, alert, measurement and response coordination within the lifecycle for both; operational processes and technical control protection measures.

3.4 Technical Controls and Components Security

SCADA systems are important elements of CII and the current safeguards of ICT can be applied to protect them (technology, policy/practice and people), but human factor plays an important role in the defense for system survivability.

	Security Policy	Organizational Security	Risk assessment and vulnerabilities	Asset Classification and control	Personnel Security	Physical and environment Security	Communications and operations management	Access control	Systems development and maintenance	Incident management	Business continuity management	Compliance	Certification procedures and Audit
BS 25999											✓		✓
ISO/IEC 27001	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ISO/IEC 27002	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
ISO/IEC 27005			✓	✓									
ISO/IEC 27006													✓
ISO/IEC 24762											✓		
ISO 19011													✓
MAGERIT			✓	✓									✓
NIST SP800-27									✓				
NIST SP800-30			✓						✓				
NIST SP800-34											✓		
NISP SP800-53		✓	✓									✓	
NIST SP800-61										✓			
NIST SP800-64									✓				
NIST SP800-100	✓	✓	✓		✓		✓		✓	✓	✓	✓	✓
ISO 15408	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
ISO 19791		✓			✓	✓	✓	✓	✓	✓	✓		✓

Table 1: Organizational standards control objectives comparison.

Examples of selecting applicable controls to SCADA systems can be reviewed in [36], [37]. They are a not sector specific practices recommended to increase the security of control systems from both physical and cyber attacks that can help in the development of a framework for a cyber security program. More sector specific are the NERC CIP reliability Standards [38] that provide, using reasonable business alignment, a cyber security framework for the identification and protection of critical cyber assets to support reliable operation on an Electric System.

The following tables 1 and 2 show a comparative summary of organizational and technical security normative standards applicable to IT and SCADA systems related to their common security control objectives. These standards offer guidance on how to secure SCADA systems and an overview of possible system topologies.Typical threats and vulnerabilities to SCADA systems are identified and security countermeasures are recommended to mitigate the associated risks.

As a conclusion we can deduce the need of a unified subset of SCADA fo-

	Risk assessment	Communications and operations management	Access Control	Systems development and maintenance	Incident management	Business continuity management	Industrial Control Systems (ICS)
ISO/IEC 27005	✓						
MAGERIT	✓						
NIST SP800-30	✓			✓			
NIST SP800-34						✓	
NIST SP800-41		✓					
NISP SP800-53	✓						✓
NIST SP800-54		✓					
NIST SP800-63		✓	✓				
NIST SP800-64				✓			
NIST SP800-82			✓				✓
NIST SP800-83					✓		
NIST SP800-92		✓	✓				
NIST SP800-92		✓					
NIST SPP-ICS	✓						✓
ISA-TR99.00.01-2004 & ISA-TR99.00.02-2004		✓	✓		✓		✓
GAO-04-140T		✓	✓	✓			✓
FIPS Publication 199	✓		✓	✓	✓		
ISO 19791		✓	✓	✓	✓	✓	

Table 2: Technical standards control objectives comparison.

cused standards that comprises both the technical and organizational issues aligned to the overall IT governance and controls. Also, we need to apply dynamic risks changes to measure and evaluate the whole system security and their internal/external needs of ”security status” communications to a certain degree of trust. Fortunately, it seems to be a current trend in applying system Protection Profile (PP) [30], [39], [35] referred to Common Criteria, for both the information technology based components and the non-information technology based elements implemented via policies and operating procedures for securing the whole system and their subsystem or security domains.

Hence, it seems that there are four areas of security controls in which further development is needed to improve its current state of the art. First, the weakest points to consider for securing SCADA are communications that should be improved to reduce costs and increase efficiency. Second, and related to this, is enhancing SCADA protocols and strengthening networks with cryptography using secure-software design principles [40]. Third, monitoring and detection controls through firewalls and intrusion detection systems should be set-up to ensure access policy compliance and detect suspicious behaviors [22], [27]. Finally, a problem that has not been deeply addressed: SCADA information classification. Depending on their levels of classification and range of risks, it should affect the current security classification of their overlying infrastructures as critical.

3.5 Authorization and Access Processes

SCADA networks do not have a usual defined perimeter for proper access control. Improving access control to the networks has to be done firstly, through more tightly, clearly and detailed network access control policies based on the company general access control policy. Secondly, it is necessary to develop proper security mechanisms to ensure authentication, confidentiality, integrity, and privacy of data both in SCADA network components and in the many existing different SCADA protocols. On this regard Network Admission/Access Control (NAC) solutions can help in the task of authenticating distant devices [41]. Thirdly, human factor problems of authenticating humans' users still are of highly importance even in SCADA network.

Who the users are (authentication) and what the users can do (access management) on an operational system depends on the implementation of two intertwined managing concepts: Identity and Access. Access control can include the control of physical access to facilities and computer and electronic systems. Allowing access requires authentication for either a human or a device. They can use a token, that usually says something about whom posses it, to prove that their claimed identity is known, at least, to that system.

The more number of authentication factors the most secure authentication access control is supposed to be. In order to establish a good access policy into a network it is necessary to take into account unauthorized personnel and critical components and, if necessary, to define a perimeter and strong access control policies for both the human and the machine interaction, where it is relevant the bidirectional exchange of credentials among network nodes and devices [31]. Access Control has to be improved from a management point of view with all the existing policies and guidelines like ISO/IEC 27001:2005, ISO/IEC 27002:2005, NIST SP800-82, NIST SP800-53 that addresses some control needs: business requirement for access control, user access management, user responsibilities, network access control, operating system access control, application and information access control, mobile computing and telecommuting. Also, technical solutions should start earlier in the development and support processes and a bunch of evaluable controls be set; as for example the development focused classes (Class FDP: user data protection, access control policy (FDP_ACC), access control functions (FDP_ACF)) specified in ISO/IEC 15408-X:2009 under Common Criteria Methodology.

3.6 Cyber Assessment Methodology

SCADA systems have a high requirement on availability and should be so when performing security vulnerability assessments that identify and resolve vulnerabilities to improve the security of SCADA systems and over/underlying critical infrastructure process [42]. Due to software code complexity it should have a detailed plan that specifies a schedule and budget, targets and goals, expected deliverables, hardware and resource requirements, rules of engagement, and a recovery procedure.

Vulnerabilities assessments performed under the US National SCADA Test Bed (NSTB) [43] had shown the need of categorizing assessment findings and grouping them into general security dimensions and sub-categories according to a settled taxonomy. It seems that there are no clear vulnerability assessment methodologies for SCADA protocols. Currently, there are works on the run that are developing taxonomy of vulnerabilities to provide a framework for the security assessment of these protocols [21], [42]. They are using some of the existing general security assessment methodologies and taxonomies to generate a list of potential vulnerabilities in the target protocols. On the other hand, a good approach to do and define an assessment plan is applying Common Criteria [26] for Securing Operational SCADA systems implies specifying adequate targets of evaluation (TOEs) to be tested for both; products, and security functions of ICT systems. In this case, a TOE usually should be a subset of the SCADA or control system. As an example, a TOE for a SCADA system might be the alarms and commands to and from the field components in response to a man-in-the-middle attack.

Evaluation of operational system requires configuration management that is not usually found in ISO/IEC 15408 product evaluation. As ISO/IEC 15408 treats the life cycle of ICT products from the perspective of a developer, the life cycle only considers operational concerns as they impact the next version of the product. But almost a system has many other process components and manual procedures that need to be taken into account. Extending this capacity the technical report for assessment of operational systems ISO/IEC TR 17971 [26] put a step forward for operational system security assessment because it also expands the security evaluation to the operational processes carried out by personnel.

3.7 Alarm and Incident Management

While policies and mechanisms presented in this Section cover determined security aspects for a control system, it is also necessary to provide intelligent response mechanisms to incidents in order to avoid further increased damage due to an improper collateral impact. A particular case is precisely the alarm management, which is considered to be a field still unexplored. A first approach was proposed by Alcaraz et al. in 2009 [19]. They presented an automated adaptive response mechanism capable of estimating the most suitable operator to effectively respond to incidents and alarms in a control system, and ensure that a critical alert is attended timely. To this end, the mechanism has to make use of a reputation module to store values associated to operators' behaviors and to their reactions when dealing with incidents. The part of decision-making is managed by an incident manager, called as *Adaptive Assignment Manager* (AAM). Both the reputation module and the manager have to be decoupled from the operational activities of the system in order not to affect on the availability and performance of the whole system.

The assignment of alarms is relatively easy. The AMM component takes an alarm as an input, and it determines which operator and supervisor are the most appropriate to provide an early and effective response to the incident, offering all the relevant information to supervisors in a way that they can do their job in an assisted manner. In order to determine which operator or supervisor are the most suitable for taking care of an incident, the AAM considers the following set of four parameters: *Criticality* of the alarm, reputation of the operator and supervisor (member of the organization in charge of monitoring an operator's way to attend an incidence), *Availability* of the operator and supervisor according to their contracts, and *Load of work* of the operator and supervisor, i.e. the overload of critical incidences that an operator/supervisor might be dealing with at a certain period of time. Likewise, the AAM is also in charge of updating the reputation of the operators in the reputation module by using the feedback of the supervisors.

As a result, the alarm management mechanism assures reliability and security. Reliability, identifies the operator that is more suitable for performing a determined activity. Security, provides input information associated to operators and activities to other security mechanisms, such as auditing and forensic mechanisms.

4 Incident Response in SCADA Systems

As part of the security policy to be enforced [49], a procedure must be defined to react when incidences occur. This plan must also include mechanisms to detect attacks, track them and preserve information that can help in the forensic analysis of an incident. Moreover, a restoration process must be specified as well when the functionality of the system is affected by an incident.

As a basis for defining an incident response plan, well-known guidelines proposed by NIST and ISO can be used, expanding the policies and adapting them to the particular circumstances of the scenarios. This is the case with the work presented in [50] where a framework is presented to respond to and manage incidences in a CI. This work introduces a plan for responding to incidents in a Norwegian petroleum industry, focusing on three main phases: (1) prepare a plan for incident response, (2) detect and recover incidents and restore normal operations and (3) learn from the experience of previous incidents handled in the past.

The need for solutions to be applied in phase two is the objective of this section, which will give an overview of the efforts been made to provide an incident response plan with an efficient intrusion detection mechanism and the forensics methodologies to be used. Finally, unresolved issues discovered will be presented as well.

4.1 Detecting intrusions and threats

As part of an incident response strategy it is necessary to deploy detection mechanisms that alert security operators when an attack is performed on some of the components of the SCADA network. This type of solution has been used in the industry for early detection of attacks, and it deals with two main aspects of the incident response strategy: awareness of attacker's initial attempts to detect vulnerabilities in the perimeter of a SCADA network, or also to support the forensic process in the analysis of a system failure because of an attack, by gathering evidence of a successful intrusion.

Although there has been increased activity in recent years in the search for new solutions for intrusion detection, few researchers have paid attention to Critical Infrastructures and SCADA systems. Conventional IDS solutions do not fit well into a Critical Infrastructure scenario because its characteristics differ from common ICT systems deployment. In a SCADA network environment it is common to find proprietary protocols and operating systems that make difficult the adoption of current host-based or network-based intrusion detection systems. Besides this, et al. and other terminal nodes that provide information from the surrounding to the control systems are as critical as the equipment used for managing this information, because they affect they final decision that is adopted by an operator.

According to [46] attacks can be performed at different levels:

- RTUs and edge devices: remotely accessing these devices can compromise the overall functionality of the whole SCADA system because this equipment is used as a source of information for the control of the entire infrastructure.

- SCADA protocols: an attacker can exploit vulnerabilities in the protocols employed for obtaining data from RTUs and for the interconnection between SCADA networks. Disclosure of misleading information, spoofed RTUs and system controls are common threats facing any kind of intrusion detection mechanism.

- Network topology: denial of service attacks can saturate information providers causing its disappearance in the global visualization of the status of the SCADA network.

These SCADA specific threats have to be treated as long as other threats that are present in any IT infrastructure. In [51], an analysis of the impact that malware attacks can have on a SCADA system shows how typical operating systems worms (e.g. CodeRed, NIMDA, Slammer and Scalper) can influence on the overall productivity of a control system, causing malfunctioning and disasters in minutes.

Moreover, intrusion detections systems must face other problems which are more specific to this kind of environment. For instance, specific protocol-based network attacks that can harm the infrastructure by employing legacy protocol commands in a misleading way can cause denial of service and other kinds of malfunctioning effects [52]. SCADA systems have another requirement: an IDS must not disturb normal operations by increasing delays in the communication between RTU, control systems and interface applications like HMIs. High-speed traffic analysis is another topic that an intrusion detection solution has to tackle to succeed, as presented in the results of [53].

Therefore, future solutions for the detection of attacks in CIs should be specialized and adapted to the new scenario explained previously, extending their functionality by also monitoring SCADA specific protocols and taking into account the operational context where they are going to be used.

An evolution of the different intrusion detection advances provided by the research community is presented in [54]. In this work, research activity results have been split into two main categories: new distributed detection architectures and advanced detection mechanisms.

Regarding detection mechanisms, three general approaches are present in current IDS solutions to discover attacks or tryouts:

- Signature based: a set of rules of known attacks is used in order to find any suspicious activity in the current traffic of the SCADA network. Previous knowledge of an attack behavior is needed in order to detect it, although some unknown attacks can be detected by searching in the network traffic for traces of commands launched by intruders in compromised systems.

- Anomaly based: normal behavior is the key element of this kind of solutions. Different implementations try to model the normal behavior of the traffic, applications or messages being transmitted. Anomaly based solutions are able to detect unknown attacks and hard to discover intrusion proofs, because of the anomaly of these events with respect to the normal network traffic.

- Protocol or specification based: sometimes attackers employ legitimate protocol commands to exploit a vulnerability in the specification of the protocol used for communicating elements of the SCADA network. These intrusion detection solutions know these deficiencies and validate each command submitted to/from elements of the network in order to detect misbehaviors.

The effectiveness of these techniques depends on many factors. Basically we can find the following requirements for each category: (1) a complete and updated rule set is needed for the signature based implementations together with a scenario that employs protocols known to the IDS, (2) good training and

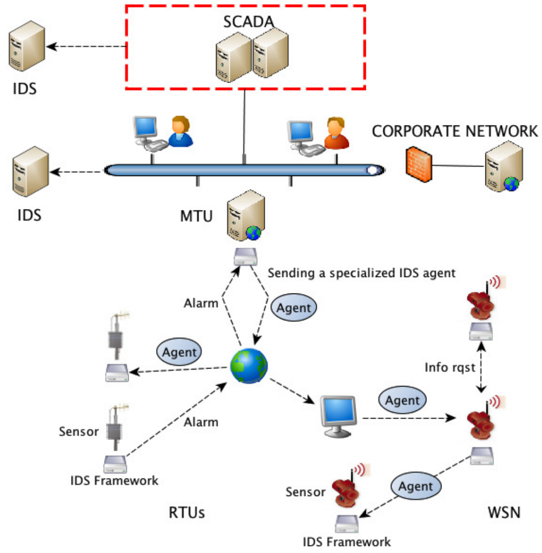

Figure 3: Sending specialized autonomous IDS agents for solving an incidence or gathering more information.

a stable scenario is needed for the anomaly detection of attacks and (3) well-known modelled specification protocol scenario is required for the application of the protocol-based detection approach.

Some signature-based solutions employ a combination of a SCADA specific rule set and pre-processors provided by DigitalBond[55] that inspect protocols widely used in the industry.

Another approach that is commonly used is to adapt an anomaly detection algorithm to better-fit SCADA scenario particularities. This is the case with the work presented in [56] where a neural network schema is used as an anomaly detection mechanism for the intrusion detection. This solution is employed to analyze the traffic between PLCs and control systems, successfully detecting attacks directed to both systems. Although attacks of this kind deployed in the previous work are well known, most of them are not related to the particularities of the communication protocols employed in a SCADA network. Another technique for the anomaly detection work has been adopted in [57], where a SCADA simulator has been used to train a rough classification algorithm that reveals strange values reported by RTUs to the control system.

Although in some situations one of the above mechanisms can be successfully used, in many scenarios a mixture of them is commonly used to take advantage of the combined benefits. This is the idea behind the work presented in [58] where a combination of anomaly and signature detection techniques is used. Indeed, because these systems usually have a small set of specific applications, most of them with a long lifetime and with regular and predictable communication protocols, these elements can be easily modelled for detecting anomalies in SCADA components behavior while also using a signature-based algorithm for detecting known attacks. Model-based detection is the technique used for modelling the behavior of the system components in this work. Models were developed for characterizing the normal behavior of applications processes, machines and users in the systems alerting operators when an attack takes place on these models. In particular two protocols were modelled: ModBUS/TCP and DNP3 over TCP/IP analyzing the content of protocol packets, their expected fields content and relationship. This anomaly detection mechanism has been included in a widely used signature-based intrusion detection open source solution named Snort[61].

Regarding the architecture of detection, the benefits of distributed solutions for detecting attacks based on multi-agent systems instead of using host-centralized approaches for a Critical Infrastructure scenario are listed below:

- Autonomous mobile agents are less vulnerable to attacks than architectures employing coordinated or centralized detection,
- They can work even if one component fails or is compromised,
- It is easy to recover a damaged agent and moved it to a safer place in order to be able continue detecting attacks.

Recent distributed IDSs researches are analyzed and compared in [59], concluding that the multi-agent technology increases the performance and accuracy of IDSs. These two characteristics are of great importance in a Critical Infrastructure scenario. An example of a multi-agent IDS for a CI is presented in [60], although this work distributes the operational process into multiple agents, coordinating them by using at least one coordination agent. These multi-agent architectures are not as fault tolerant as the autonomous multi-agent option, because in the case where one of the main operational nodes fails the overall detection system could be disabled.

To date, mobile autonomous multi-agent architectures have not been used so far for defining specialized agents that can monitor SCADA protocols and applications. The SCADA scenario seems to fit perfectly with the benefits provided by distributing the detection work in autonomous and independent agents across the network. Agents can be specialized for analyzing applications or traffic where they reside, minimizing the amount of resources needed for the detection work and also reducing the need for a frequent update of the rule set or experience used for the detection of attacks. Figure 3 shows a scenario where mobile autonomous agents are propagated both for discovering traces of an attack and gathering information from terminal units to be used for analyzing an incident. In case that one of the terminal units is working suspiciously, specialized agents can be propagated to its surrounding for a deep inspection of the network activity.

This combination seems promising, future research should explore how to obtain benefits from the recent advances in the area of new attack detection mechanism, with the use of autonomous multi-agents specialized in the protocols or applications most commonly used in a SCADA network. These agents could be located in many kind of computing environments, from nodes of the SCADA local network to RTUs that have less computing resources available. In fact, mobile autonomous agents have been tested in resource and energy constrained environments such as WSNs ([62] and [63]) where computing efficiency and low energy consumption are normal topics to deal with.

4.2 Analysis of intrusions

The analysis of intrusions and evidence gathering of malicious activity is another hot topic that requires the attention of the research community. Current forensic methodologies used in the industry need to be adapted for the special requirements that the SCADA systems demand [64]. As reflected in [65] these kinds of systems have the following elements that need to be considered when defining a methodology:

- More than one server in the control system area.
- A human interface (HMI) for the interaction between operators and the system.
- A large number of PLCs deployed in a wide area.
- Numerous remote connections to the central systems.
- A networked intra device environment

Around the middle of 2008 a set of research groups in the digital forensic field met as a working group at the Colloquium for Information Systems Security Education (CISSE 2008), where a list of hot topics in the research agenda of forensic computing for the next few years was compiled. The results of this working group have been gathered together and presented in the work [66]. At the top of this list can be found the need to create forensic methodologies for SCADA systems. Regarding this topic, an overview of open research issues were collected, which includes the need to build new hardware-based capture devices for control system network audit and new IDSs focused on these environments.

In fact, most control systems solutions focus mainly on controlling information while accounting and auditing tasks are not been implemented. As a result, there is a need for research into defining strategies and methodologies that can provide control systems with the forensic capabilities that are needed. To succeed in the application of new forensic methodologies specially adapted to SCADA systems, the following main areas need to be defined: evidence collection, preservation of evidences, analysis of incidents and documentation. But to go forward two of these areas need to be explored by the research community: evidence collection and analysis of incidents. In order to tackle them, new mechanism for analyzing and correlating alerts and intrusion evidences are needed.

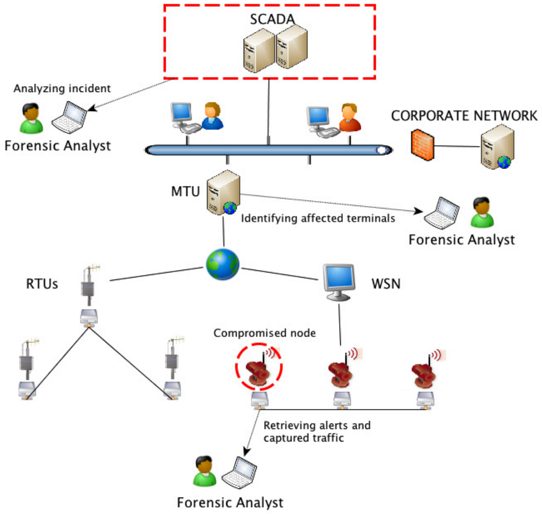

Figure 4: Analysis of an incident.

Evidence gathering and analysis process imply the adoption of new intrusion detection mechanisms that not only rely on detecting known or common attacks, but also discover attacks to the communication protocols and devices used in a SCADA network. Some results have been presented in the previous section regarding the detection of attacks in control systems, but in order to monitor RTU traffic, new devices have to be used that can be integrated into these components for the analysis and registration of attempts or try outs.

A referential implementation of a RTU Data Logger is presented in [66], together with a denial of service attack that compromises the functionality of the overall system by stopping all communication from the control system RTU to the master node. These data loggers in addition to capturing all RTU network activity, also provide encryption and storing of sensitive data to a hard disk for post incident forensic investigation. Figure 4 shows the different elements of a CI that could take part in the forensic analysis of an incident, from SCADA data servers to terminal units affected by an attack.

The analysis of evidence implies that the information gathered must be correlated and categorized appropriately. Intrusion detection agents, monitoring software, accounting process and information gathered from SCADA terminals (RTUs or WSNs) must be correlated and presented to operators in such a way that different levels of abstraction can be used: from a high level view presenting location of incidences and interdependencies with other components of the SCADA system [67], to a low level analysis of logs and captured traffic that reveals anomalies or attacks in the communication between nodes in the network [58].

5 Study Case: SCADA in Smart Grids

Existing SCADA systems play a role in monitoring emerging renewable energy systems such as Smart Grids. A Smart Grid is a critical infrastructure responsible for distributing and efficiently managing renewable energy to end-users. It is managed by other complex infrastructures (e.g., Advanced Metering Infrastructures (AMIs)), where the Internet and a set of things play a fundamental role in optimizing the whole performance of the system. The integration of things in the Internet is known as the Internet of Things or Internet of Energy (if the application context is developed in an industrial environment).

The first conceptual model of a Smart Grid was introduced by the NIST in 2009 [68], where seven domains were identified: customers, market, service providers, operations, bulk generation, transmission and distribution. Each domain encompasses a set of things, such as: end-users, operators, software and devices (e.g. smart meters, sensors, solar panels, electrical intelligent devices, industrial devices, etc.). The cooperation and information exchange among them helps the development of certain applications, such as for instance solar energy generation, management and storage, whose monitoring is centralized in a SCADA system. Nonetheless, new security risks arise in this new infrastructure, like for example privacy issues since smart metering devices manage the user data automatically, using the Internet as a communication mechanism. [44].

These new elements of an infrastructure need new paradigms to facilitate survivability and resilience. Hence, the grid should be 'self-healing' and capable of anticipating and instantly responding to system problems in order to avoid or mitigate power outages and power quality problems. Therefore, security plays an important role in the deployment of new technology, for both physical and cybersecurity, which will allow proactive identification and response to accidental or intended disruptions [45].

As mentioned previously, management of these new systems and their security need to apply old approaches to security. These approaches are based on prevention combined with response and recovery activities developed in the event of a cyber attack. But the overall cyber security strategy for the Smart Grid also has to take into account interdependencies and interoperability to mitigate risks. Furthermore; a new approach is needed in which the definition and implementation of an overall, technical and organizational cybersecurity risk assessment process should end up in the conformity assessment that should have into account common security evaluation criteria for the overall system and its domains ISO/IEC TR 17971 [26]. As these domains included systems from the IT, telecommunications, and energy sectors, the risk assessment process has to be applied to all these sectors, even home and businesses as they interact in the Smart Grid. This gives rise to potential privacy risks that demand the use of privacy-enhancing technologies (PET) for designing, building and managing these networks [44].

The Smart Grid must be security designed. It is expected to last a long time. It must adapt to changing needs in terms of scalability and functionality, and at the same time it needs to tolerate and survive malicious previously, unknown attacks. Research is clearly needed to develop an advanced dynamic evolving architecture protection that made of survivability and resiliency compulsory design and implementation requirements.

Moreover, detecting attacks directed at these devices is of great importance in order to avoid misuse that can affect their performance, reliability and confidentiality. Clearly new attacks are going to appear that could bring still unknown effects locally or to the surrounding components of a SCADA network. IDSs must be designed that analyze traffic directed to or coming from these devices. Also, host-based intrusion detection systems can take advantage of locally running agents that analyze the behavior of the main software components detecting anomalies that could be a signal of compromised status. Some results are starting to arrive regarding this issue. For instance, in [46] a security solution that employs agents to analyze the behavior of Smart Grid devices is explained. This work reveals the benefits of employing a multi-layer intrusion detection mechanism for detecting known attacks in a power grid environment, although SCADA specific protocol attacks have not been taken into account and should be included in future research works.

6 Conclusions

Nowadays, isolated SCADA networks are converging on standard ICT-based systems bringing new security challenges and a large number of potential risks due to threats, vulnerabilities and failures. Some of these are associated to the TCP/IP standard, the use of open (hardware and software) components and wireless communication technologies.

In order to address some security issues, special attention should be paid to the network management. Critical control networks (SCADA or DCS systems) must supervise, through computational systems, the constant performance of other critical systems, whose services are essential for survivability, like for example electric energy. A failure or threat in the control of a critical system could mean the (total or partial) disruption of its services, and therefore massive chaos among interdependent infrastructures whose impact could be devastating for the well-being of our society and economy.

The main purpose of this Chapter has been to analyze technological advances in the SCADA network architecture and to show how different ICT systems have converged in real-time monitoring processes and also to show how the control system is dependent on these ICT systems. Likewise we have analyzed consequences and their impact over the overall performance of the system in order to identify security mechanisms, (security and access control) policies, standards, recommendations, good practices, methodologies and assessments for a secure network management. In addition, we have reviewed some proactive mechanisms existing in the literature which deal with anomalous events, in order to ensure a timely response and we have considered how to control a possible effect in cascading.

Finally, we would like to highlight that several areas of applicability of evolutionary methods and genetic algorithms on power systems opens up new possibilities for critical control systems and the applicability of bio-inspired systems [47], [48]. In fact, the Immune System (IS) is an example of a highly complex system which evolved to protect the body as such, thus we believe that this concept is a good candidate as the basis for the next generation of bioinformation systems from which we could learn about new protection mechanisms. In addition, as ICT systems provide a distributed control and layered protection with a multiple escalating response to hostile actions and errors as a part of an adaptive mechanism capable of memorizing and learning, they could be implemented in SCADA systems to implement secure future new protocols based on these paradigms.

References

[1] IBM Corporation, A Strategic Approach to Protecting SCADA and Process Control Systems, `http://documents.iss.net/whitepapers/SCADA.pdf`, 2007, accessed on March, 2010.

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

[3] B. Qiu, B. Gooi, *Web-based SCADA display systems (WSDS) for access via Internet*, IEEE Transactions on Power Systems, Vol. 5, No. 2, pp.681-686, 2000.

[4] B. Qiu, H. Gooi, Y. Liu and E. Chan, *Internet-based SCADA display system*, Computer Applications in Power, No. 1, Vol. 15, pp. 14-19, 2002.

[5] R. Leou, Y. Chang and J. Teng, *A Web-based power quality monitoring system*, Power Engineering Society Summer Meeting, IEEE, Vol. 3, pp. 1504-150, 2001.

[6] D. Li, Y. Serizawa and M. Kiuchi, *Concept design for a Web-based supervisory control and data-acquisition (SCADA) system*, Transmission and Distribution Conference and Exhibition, Asia Pacific. IEEE/PES , Vol. 1 , pp. 32-36, 2002.

[7] M. Jain, A. Jain and M. Srinivas, *A web based expert system shell for fault diagnosis and control of power system equipment*, Condition Monitoring and Diagnosis, pp.1310-1313, 2008.

[8] Yokogawa, `http://yokogawa.com/scd/fasttools/scd-scada-websuper-en.htm`, accessed on March, 2010.

[9] WebSCADA, `http://www.webscada.com/`, accessed on March, 2010.

[10] V. Gungor, F. Lambert*A survey on communication networks for electric system automation*, Computer Networks: The International Journal of Computer and Telecommunications Networking, ACM, No. 7, Vol. 50, pp. 877–897, 2006.

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

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

[13] J. W. Bialek, 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.

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

[15] S. Choong, Deregulation of the Power Industry in Singapore, IEE Conf. Pub, Vol. 2000, Issue CP478/Vol. 1, pp.11–32, APSCOM, 2000.

[16] J. Pollet, Developing a Solid SCADA Security Strategy, 2nd ISA/IEEE Sensors for Industry Conference, pp. 148–156, 2002.

[17] Riptech, Inc., Understanding SCADA System Security Vulnerabilities, `http://www.zdnet.co.uk/white-papers/riptech/n-1z10rhq/`, 2001, accessed on March, 2010.

[18] N. Barkakati and G. Wilshusen, Deficient ICT Controls Jeorpardize Systems Supporting the Electricity Grid - A case Study, Securing Electricity Supply in the Cyber Age: Managing the increasing dependence of the electricity infrastructure on ICT (NGInfra), Vol. 15, pp. 129–142, Utrecht, The Netherlands, 2009.

[19] C. Alcaraz, I. Agudo, C. Fernandez-Gago, R. Roman, G. Fernandez and J. Lopez, *Adaptive Dispatching of Incidences based on Reputation for SCADA Systems*, Privacy & Security in Digital Business, LNCS 5695, pp. 86–94, 2009.

[20] L. Ronald, *Securing SCADA Systems*, Wiley Publishing Inc, Indianapolis, 2006.

[21] M. Vinay, Igure, S. Laughter, W. Ronald, *Security issues in SCADA networks*, Computers & Security, No. 25, pp. 498–506, 2006.

[22] National Infrastructure Security Coordination Centre (NISCC), *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, `http://www.cpni.gov.uk/docs/re-20050223-00157.pdf`, accessed March 2010.

[23] E. Byres, J. Carter, A. Elramly, and D. Hoffman, *Worlds in collision: Ethernet on the plant floor*, http://www.isa.org/fmo/newsweb/pdf/worlds.pdf, 2002, accessed March 2010.

[24] L. Philip, P. Campbell, *Survivability via Control Objectives*, 3rd IEEE Information Survivability (ISW-2000), pp. 1–4, 2000.

[25] ANSI/ISA-99.02.01-2009 standard, *Security for Industrial Automation and Control Systems Part 2: Establishing an Industrial Automation and Control Systems Security Program*, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821, 2009.

[26] ISO/IEC TR 19791:2006, *Information technology-Security techniques-Security assessment of operational systems*, Draft revision ISO/IEC JTC 1/SC 27 Final text for ISO/IEC TR, ITTF, 2009.

[27] J. Stamp, P. Campbell, J. Depoy, J. Dillinger, W. Young, *Sustainable security for infrastructure SCADA*, SAND2003-4670, 2004, http://www.sandia.gov/scada/documents/SustainableSecurity.pdf, 2004, accessed March 2010.

[28] C. Alcaraz, G. Fernandez, R. Roman, A. Balastegui, J. Lopez, *Secure Management of SCADA Networks*, UPGRADE, No. 6, Vol. 9, pp. 22–28, 2008.

[29] GAO, *Challenges and Efforts to Secure Control Systems*, 2004.

[30] NIST, *SP800-82 Guide to Industrial Control Systems*, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf, accessed March 2010.

[31] CPNI, *Good practice guide process control and SCADA security guide 7*, Establish ongoing governance, http://www.cpni.gov.uk/Docs/Guide_7_Establish_Ongoing_Governance.pdf http://www.cpni.gov.uk/Products/bestpractice/goodpracticearchive.aspx.

[32] *ESCoRTS Security of Controls and Real Time Systems*, TD21, http://www.escortsproject.eu/getfile.php?id=316/, January 2010.

[33] J. James, J. Graham, A. Leger, *Gap Analysis for Survivable PCS*, United States Military Academy Research Report No. 14, www.thei3p.org/publications/ResearchReport14.pdf, 2009, accessed March 2010.

[34] P. Kertzner, D. Bodeau, R. Nitschke, J. Watters, M. Young, M. Stoddard, *Process Control System Security Technical Risk Assessment*, Analysis of Problem Domain, I3P research report No. 3, http://www.thei3p.org/docs/publications/ResearchReport3.pdf, 2005, accessed March 2010.

[35] eCID, *enlightened Critical Infrastructures Defense*, TSI-020301-2009-18, R&D project co-financed by Spanish Ministry of Tourism and Commerce by Plan Avanza, 2009–2010.

[36] P. Robert, Evans, *Control Systems Cyber Security Standards Support Activities*, http://www.inl.gov/technicalpublications/Documents/4192219.pdf, 2009, accessed March 2010.

[37] Department of Homeland Security (DHS), *Catalog of Control Systems Security: Recommendations for Standards Developers*, http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf, 2008, accessed March 2010.

[38] NERC, *Critical Infrastructure Protection (CIP)*, http://www.nerc.com/page.php?cid=2|20], 2008.

[39] NIST, *System Protection Profile-Industrial Control Systems*, version 1.0, 2004.

[40] C. Sandip, D. Ganesh, H. Graham, *Improving the Cyber Security of SCADA Communication Networks*, ACM, Vol. 52, No. 7, 2009.

[41] H. Okhravi, D. Nicol, *Applying trusted network technology to process control systems*, Critical Infrastructure Protection II, IFIP, Springer, Boston, Vol. 290, pp. 57- 70, 2009.

[42] Viking Project, http://www.vikingproject.eu/page3.php,2010, accessed on March 2010.

[43] Office of Electricity Delivery and Energy Reliability, *Common Cyber Security Vulnerabilities Observed in Control*, DoE, System Assessments by the INL NSTB Program, http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages.pdf, 2008, accessed March 2010.

[44] A. Cavoukian, J. Polonetsky, C. Wolf, *SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, Office of the Information and Privacy Commissioner/Ontario, http://www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf, 2009, accessed March 2010.

[45] P. Mazza, *Smart Grid: Powering Up the Smart Grid-Smart Grid News-Grid Modernization and the Smart Grid*, http://www.smartgridnews.com/artman/uploads/1/sgnr_2007_12035.pdf, 2007.

[46] D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, *An integrated security system of protecting Smart Grid against cyber attacks*, Innovative Smart Grid Technologies (ISGT), pp. 1–7,2010

[47] F. Carvajal, *Computer Immune System: An overview-creating a cyberimmune operating system*, Security in Information Systems, Proceedings of the 1st International Workshop on Security in Information Systems, SIS 2002, 2002.

[48] IRRIIS Project, *Overview on Bio-inspired operation strategies*, Deliverable 2.2.3, `http://www.irriis.org/File.aspx?lang=2&oiid=9139&pid=572`,2007 ,accessed on March, 2010.

[49] D. Kilman and J. Stamp, *Framework for SCADA Security Policy*, Sandia National Laboratories report SAND2005-1002C, 2005.

[50] G. Jaatun, E. Albrechtsen, B. Line, I. Tondel, O. Longva, *A framework for Incident Response Management in the Petroleum Industry*, International Journal of Critical Infrastructure Protection (2009), vol. 2 (1-2), pp. 26–37.

[51] I. Nai, A. Carcanoa, M. Masera, A. Trombetta, *An Experimental Investigation of Malware Attacks on SCADA Systems*, International Journal of Critical Infrastructure Protection (2009), vol. 2(4), pp. 139–145.

[52] J. Verba and M. Milvich, *Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)*, IEEE Conference on Technologies for Homeland Security, 2008, pp. 469–473.

[53] N. Cai, J. Wang, X. Yu, *SCADA system security: Complexity, history and new developments*, 6th IEEE International Conference on Industrial Informatics, 2008 (INDIN 2008), pp. 569–574.

[54] M. Marhusin, D. Cornforth, H. Larkin, *An overview of recent advances in intrusion detection*, 8th IEEE International Conference on Computer and Information Technology (CIT 2008), pp. 432–437, IEEE Press, 2008.

[55] DigitalBond, `http://www.digitalbond.com`, accessed on November, 2010.

[56] O. Linda, T. Vollmer, M. Manic, *Neural Network based Intrusion Detection System for Critical Infrastructures*, International Joint Conference on Neural Networks (IJCNN), pp. 1827–1834, IEEE Press, 2009.

[57] M. Coutinho, G. Lambert-Torres, L. Silva, H. Martins, H. Lazarek, J. Neto, *Anomaly Detection in Power System Control Center Critical Infrastructures using Rough Classification Algorithm*, DEST 2009, pp. 733–738, IEEE Press, 2009.

[58] A. Valdes, S. Cheung, *Intrusion Monitoring in Process Control Systems*, 42nd Hawaii International Conference on System Sciences (HICSS 2009), pp. 1–7, IEEE Press, 2009.

[59] N. Patil, C. Das, S. Patankar, K. Pol, *Analysis of Distributed Intrusion Detection Systems Using Mobile Agents*, First International Conference on Emerging Trends in Engineering and Technology (ICETET '08), pp. 1255–1260, IEEE Press, 2008.

[60] C. Tsang, S. Kwong, *Multi-agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction*, IEEE International Conference on Industrial Technology 2005, ICIT 2005, pp. 51–56.

[61] SNORT, `http://www.snort.org`, accessed on November, 2010.

[62] D. Georgoulas, K. Blow, *Intelligent Mobile Agent Middleware for Wireless Sensor Networks: A Real Time Application Case Study*, Fourth Advanced International Conference on Telecommunications 2008, AICT '08, pp. 95–100.

[63] C. Fok, G. Roman, C. Lu, *Agilla: A Mobile Agent Middleware for Self-adaptive Wireless Sensor Networks*, Transactions on Autonomous and Adaptive Systems (TAAS 2009), vol. 4.

[64] J. Slay, E. Sitnikova, P. Campbell, B. Daniels, *Process Control System Security and Forensics: A Risk Management Simulation*, Proceedings of SIMTECT 2009, Adelaide.

[65] J. Slay, E. Sitnikova, *The Development of a Generic Framework for the Forensic Analysis of SCADA and Process Control Systems*, e-Forensics 2009.

[66] T. Morris, A. Srivastava, B. Reaves, K. Pavurapu, S. Abdelwahed, R. Vaughn, W. McGrew, Y. Dandass, *Engineering Future Cyber-Physical Energy Systems: Challenges, Research Needs, and Roadmap*, IEEE North American Power Symposium, October, 2009.

[67] W. Tolone, *Interactive Visualizations for Critical Infrastructure Analysis*, International Journal of Critical Infrastructure Protection (2009), vol. 2, pp. 124–134.

[68] NIST, *Smart Grid Cyber Security Strategy and Requirements*, The Smart Grid Interoperability Panel - Cyber Security Working Group, Draft NISTIR 7628, U.S. Department of Commerce, 2010.