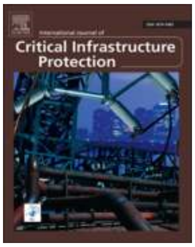
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Critical infrastructure protection: Requirements and challenges for the 21st century

Cristina Alcaraz[a,*], *Sherali Zeadally*[b]

[a]Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain
[b]College of Communication and Information, University of Kentucky, Lexington, Kentucky 40506-0224, USA

ARTICLE INFO

Article history:
Received 17 July 2014
Accepted 11 October 2014
Available online 11 December 2014

Keywords:
Critical infrastructure protection
SCADA systems
Risk
Security
Requirements
Challenges

ABSTRACT

Critical infrastructures play a vital role in supporting modern society. The reliability, performance, continuous operation, safety, maintenance and protection of critical infrastructures are national priorities for countries around the world. This paper explores the vulnerabilities and threats facing modern critical infrastructures with special emphasis on industrial control systems, and describes a number of protection measures. The paper also discusses some of the challenging areas related to critical infrastructure protection such as governance and security management, secure network architectures, self-healing, modeling and simulation, wide-area situational awareness, forensics and learning, and trust management and privacy.

1. Introduction

A critical infrastructure comprises systems and assets, whether physical or virtual, that are so essential to a nation that any disruption of their services could have a serious impact on national security, economic well-being, public health or safety, or any combination thereof [76]. The European Union (EU), through its European Programme for Critical Infrastructure Protection (EPCIP), also stresses the importance of critical infrastructure protection to all its member states and their citizens. To address critical infrastructure protection, the European Commission issued a communication [26] to establish a legislative framework for transparency with regard to critical infrastructure protection and to enable cooperation across national borders. According to EPCIP, critical infrastructures are classified as follows:

- *Energy:* Energy production sources, storage and distribution (oil, gas and electricity).
- *Information and communications technology:* Information system and network protection (e.g., Internet); provision of fixed telecommunications; provision of mobile telecommunications, radio communications and navigation, satellite communications and broadcasting.
- *Water:* Provision of water (e.g., dams), control of water quantity and quality.
- *Food and agriculture:* Food provision, safety and security.
- *Healthcare and public health:* Medical and hospital care; medicines, serums, vaccines and pharmaceuticals; bio-laboratories and bio-agents.
- *Financial systems:* Banking, payment services and government financial assignments.
- *Civil administration:* Government facilities and functions, armed forces, civil administration services, emergency services, postal and courier services.
- *Public, legal order and safety:* Maintaining public and legal order, safety and security; administration of justice and detention.

[*]Corresponding author.
E-mail address: alcaraz@lcc.uma.es (C. Alcaraz).

http://dx.doi.org/10.1016/j.ijcip.2014.12.002
1874-5482/© 2014 Elsevier B.V. All rights reserved.

- *Transportation systems:* Road transport, rail transport and air traffic; border surveillance; inland waterways transport; ocean and short-sea shipping.
- *Chemical industry:* Production and storage of dangerous substances, pipelines carrying dangerous goods.
- *Nuclear industry:* Production and storage of nuclear materials.
- *Space:* Communications and research.
- *Research facilities:* Operation of major research facilities.

The U.S. National Infrastructure Protection Plan (NIPP) [73] as defined by the Department of Homeland Security (DHS) considers the following additional critical sectors:

- *National monuments and icons:* Monuments, physical structures, objects or geographical places that represent national culture or have religious or historical importance.
- *Commercial facilities:* Commercial centers, office buildings, sports stadiums and other places that accommodate large numbers of people.
- *Critical manufacturing:* Transformation of materials into goods, including all the processes involved in manufacturing and transportation.
- *Defense industry base:* Facilities that produce military resources (e.g., weapons, aircraft and ships) and maintenance of essential national security services (e.g., communications).

The connections between critical infrastructure sectors produce special interdependence relationships. The relationships express the fact that one critical infrastructure could depend on products and services provided by another critical infrastructure, and the second critical infrastructure may also depend on the products and services provided by the first critical infrastructure. These interdependencies could trigger cascading effects in multiple critical infrastructures when one critical infrastructure is disrupted, damaged or destroyed [7]. Rinaldi et al. [63] have identified and analyzed four types of interdependencies: (i) physical; (ii) geographic; (iii) cyber; (iv) and logical. A physical interdependency exists when a critical infrastructure requires resources or raw materials from other infrastructures. A geographic interdependency exists when multiple infrastructures share a close spatial proximity, and a problem in one critical infrastructure can reach the other critical infrastructures. A cyber interdependency is the result of a dependency on information and communications systems. A logical interdependency exists when systems, actions or decisions connecting an agent in one infrastructure to an agent in another infrastructure are not physical, geographic or cyber in nature (e.g., bureaucratic or political decisions) [82].

Given the influence of information systems on the performance of other critical infrastructures, this paper focuses primarily on critical information infrastructures and their security issues. A critical information infrastructure consists of information processes supported by information and communications technologies that form critical infrastructures themselves or that are critical to the operation of other critical infrastructures [16]. The vast majority of, if not all, critical infrastructures are dependent on information systems. Thus, a disruption to a cyber infrastructure can lead to serious consequences that affect the performance, reliability, security and safety of the dependent infrastructures. The massive dependence on the cyber infrastructure has created the new research area known as critical information infrastructure protection (CIIP).

According to the European Commission [25], critical information infrastructure protection comprises programs and activities of infrastructure owners, manufacturers, users, operators, research and development institutions, governments and regulatory authorities that aim to maintain the performance of critical information infrastructures in the event of failures, attacks or accidents above a defined minimum level of service and to minimize damage and recovery time. Critical information infrastructure protection should, therefore, be viewed as a cross-sector activity instead of being limited to specific sectors. Critical information infrastructure protection should be closely coordinated with critical infrastructure protection under a holistic perspective [25]. The U.S. Government also emphasizes critical information infrastructure protection in Public Law 107-296 [77], which states that the "protection of critical information infrastructures is important to the national defense and economic security of the nation." This law deems critical information infrastructures to be critical infrastructures themselves because their information is not normally in the public domain and is related to the security of critical infrastructures and other vital systems. In fact, information and communications technologies, which underlie communications links, network topologies and interfaces that manage and transmit sensitive data in a reliable and timely manner, constitute the backbone of critical infrastructures.

One of the most important types of critical information infrastructures is industrial control systems (ICSs) that supervise and control processes in industrial infrastructures such as bulk energy generation systems, electrical distribution and transmission systems, water treatment systems, oil and gas pipelines, and chemical plants and refineries [12]. These systems incorporate communications architectures for connecting control centers to remote substations located at the infrastructures being controlled (Fig. 1). The substations incorporate automated systems called remote terminal units (RTUs) that house sensors for collecting and sending status data to the control center and actuators for performing control actions as directed by the control center.

Industrial control systems include supervisory control and data acquisition (SCADA) systems and distributed control systems (DCSs). A SCADA system is an event-driven centralized network with substations located over a large geographic area (Fig. 1). It incorporates three main components: the control center, substations and a corporate network. The control center is responsible for managing and supervising the overall system. The functionality is supported by SCADA servers and data historians that store process and system information. External access to these resources must be secured using firewalls, demilitarized zones (DMZs), intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and anti-virus software. Access must also be provided to the corporate network, which supports business operations. In contrast, a distributed control system is a process-oriented

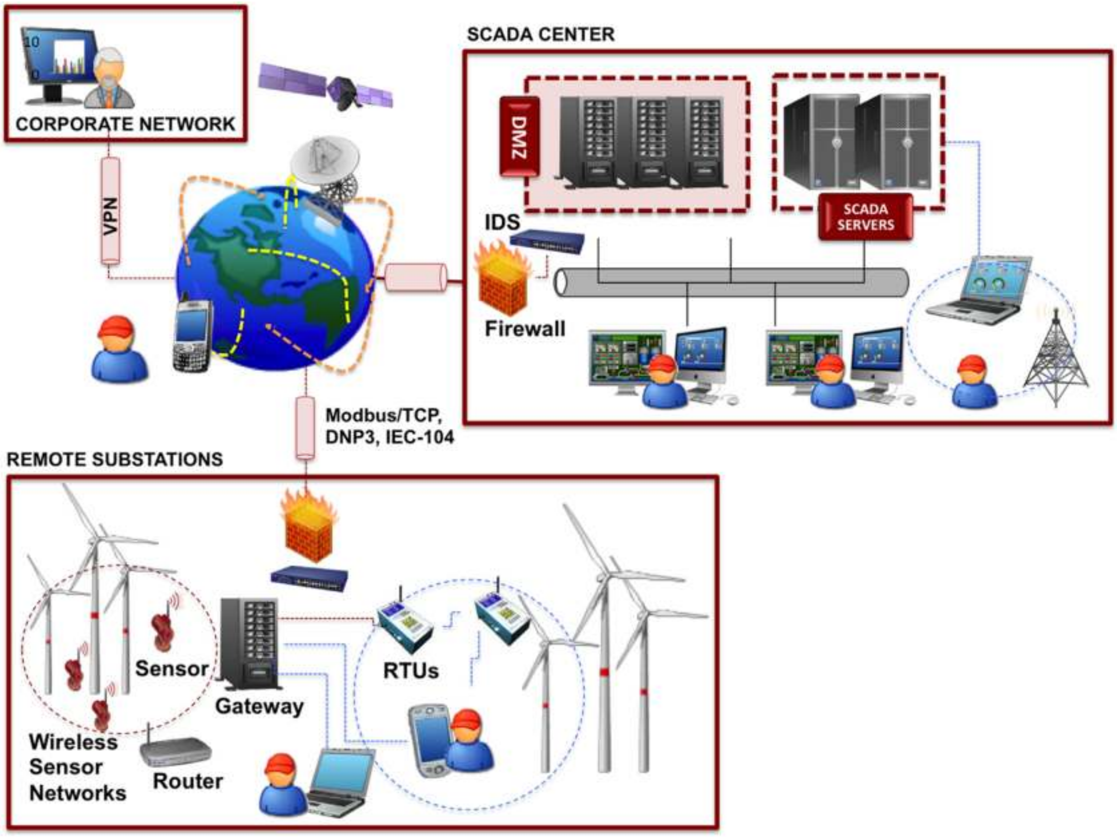


Fig. 1 – General SCADA network architecture.

system, which is limited in terms of its size and geographic distribution.

This paper focuses on SCADA systems for two main reasons. First, SCADA systems are, from a security point of view, one of the most widely researched systems in the literature (see, e.g., [4,49]). Second, and more importantly, SCADA systems constitute the backbone of next generation electrical production and distribution systems (also known as the smart grid) [54]. A smart grid is composed of sub-domains such as (renewable or non-renewable) energy bulk generation systems, transmission and distributions lines, customers, providers, markets and control systems. Each domain comprises various stakeholders and resources, all of them interconnected in order to efficiently manage load demands and reduce unnecessary power generation.

Unfortunately, the nature of SCADA systems means that they are exposed to numerous threats, which may be caused by hardware or software errors, human mistakes (i.e., operational errors) or deliberate (i.e., malicious) actions. Combating these threats, which can jeopardize the security of control systems and their critical infrastructures, requires protection strategies to be designed carefully and implemented properly.

2. Vulnerabilities, threats and protection

Vulnerabilities in hardware and software can be exploited to produce unplanned changes in the services offered and deviations from normal behavior. The resulting faults can be classified as internal faults and external faults. An internal fault corresponds to anomalous changes within a system. An external fault is due to interactions that originate from outside a system such as natural phenomena, malicious actions and accidents. Regardless of the cause, a fault can create an internal system effect that can impact the provision of essential services and the performance of control actions. For example, an attack on a sensor node may cause hardware or software errors that can affect the operation of other essential control resources such as remote terminal units. If this occurs, the control center may be unable to receive vital information from substations and become blind to the real state of the system being controlled. This situation can also occur when communication links stop functioning or are compromised by malicious entities.

Based on an extensive analysis of faults, Harrison and White [30] have proposed a taxonomy of threats that relies on the notion of cause and effect. The taxonomy uses event vectors and effect vectors to define the motivation of a threat, the methodology applied to instantiate a threat and the resulting effects. An event vector describes the threat agent, motivation, objective, and the method or technique used to achieve the objective. In contrast, an effect vector describes the impacts on the affected infrastructure, services and the sector itself, in addition to the cause. Both vectors are dependent on the type of threat and the vulnerability that is exploited to compromise system security; this generally depends on the system state and characteristics. For example, SCADA systems normally prioritize security requirements as availability, followed by integrity, followed by confidentiality

[85]. A threat to availability would render essential control, performance and information resources unavailable, a threat to integrity would seek to manipulate critical hardware, software or information resources, whereas a threat to confidentiality would attempt to eavesdrop on sensitive information.

It is also important to consider the level of dependence between resources, system components, functionalities and services [7]. When the level of dependence is high and one component exhibits anomalous behavior, there is the potential for the entire system and its services to be affected and the effects may cascade to other critical infrastructures. In such situations, it is of paramount importance to be aware of four factors: the scope of the effect, its magnitude, propagation and recovery [24]. The first factor contributes to the loss or unavailability of an element and its impact may be rated according to the geographic coverage (i.e., international, national, provincial/territorial or local). The magnitude of the effect is related to the degree (minor, moderate or major) of the loss according to the public, economic, environmental, interdependence and political impacts. Time is an essential parameter for the last two factors because it measures the criticality of a situation by determining the point at which the loss of an element could have a serious effect, and the point at which it would be possible to recover the functionality of the affected system.

Many of the threats are exacerbated by the adaptation of information and communications technologies to control tasks and operations related to critical services. The reason is that technologies increase the architectural complexity, introducing additional vulnerabilities, security risks and interoperability challenges [7]. These aspects are discussed in the next section.

3. Technological trends and security issues

Information and communications technologies play a crucial role in the connectivity and control of critical systems. This is the case with SCADA systems, where the supervision and control of infrastructure assets depend greatly on the reliability and security of the communications channels and information systems in order to send, receive and process commands, measurements and alarms.

3.1. *Communications systems*

Internetworking offers significant operational benefits with regard to supervisory control and data acquisition. The benefits include global connectivity, flexibility and data dissemination from anywhere and at any time via IP-based communications protocols and web interfaces. To extend functionality and reduce maintenance and installation costs, remote substations have migrated to TCP/IP, expanding their connectivity and ensuring integration with other technologies to balance workload and activities in the field. The use of the standard TCP/IP protocol stack has also led to the specification and standardization of SCADA communications protocols based on the client-server paradigm. Some well-known SCADA protocols include Modicon Communication Bus (Modbus/TCP), Distributed Network Protocol (DNP3), IEC 60870-5-104 and Inter Control Center Protocol/Telecontrol Application Service Element-2 (ICCP-TASE2.0, IEC 60870-6). The first two protocols are designed for automation and control while the remaining protocols deal with interconnections between telemetry control systems (i.e., between SCADA systems).

This modernization of control systems has encouraged researchers and vendors to analyze, design and implement hardware and software solutions for global collaboration and connectivity. For example, Suresh et al. [70] have designed a web-based SCADA prototype for information dissemination using XML encodings. The prototype provides a virtual experimentation platform with the possibility of incorporating GPRS and WAP connections. Salihbegovic et al. [67] have developed a web-based multi-layered distributed SCADA system for supervising truck loading and oil product pipeline shipping terminals at refineries. Jain et al. [43] have implemented a web-based expert system for the automated diagnosis and control of power systems. In the commercial arena, Exemys [27] has designed sophisticated mobile cellular telemetry solutions and hardware protocol converters that translate serial Modbus communications to TCP/IP communications. Similarly, Yokogawa [80] and WebSCADA [78] have developed advanced web-based automation solutions.

As a communications infrastructure, the Internet is exposed to numerous threats, the majority of which stem from traditional TCP/IP vulnerabilities. The vulnerabilities can be exploited to replay control messages, request essential resources to exhaust computational and communications capabilities, eavesdrop on sensitive process information via man-in-the-middle attacks, inject malicious commands to perform inappropriate actions or display fabricated monitored values. An adversary could also bypass security mechanisms to enter a system and once inside conduct many other types of attacks such as reading/modifying files, dumping memory and launching services using fake commands.

SCADA protocols have their own vulnerabilities. For example, Modbus/TCP communications are transmitted in clear text, enabling large portions of payloads (e.g., plant information and network addresses) to be captured and manipulated. Modbus/TCP also lacks authentication mechanisms because Modbus sessions only verify the validity of specific parts of a message such as the address and function code. The DNP3 protocol also suffers from security deficiencies despite the fact that it incorporates cyclic redundancy checking (CRC), data synchronization and multiple data formats (although Secure DNP3, a variant of DNP3, implements challenge-response authentication system along with a session key to verify message sources). ICCP also suffers from limitations with regard to authentication and encryption [47].

Public databases such as the Industrial Security Incident Database (ISID) and periodic reports released by Industrial Control System Cyber Emergency Response Team (ICS-CERT) provide extensive information about threats. According to a recent ICS-CERT report, the number of incidents in critical infrastructure sectors increased from 9 incidents in 2009 to 198 in 2011, with the increase primarily in the energy sector and related to control systems. The vast majority of incidents were due to viruses, Trojans and worms (such as Stuxnet in 2010 and Flame in 2012 [20]) that attempted to compromise system integrity. Recognizing the importance of threat information dissemination in enhancing protection efforts, the European Council approved the Testbed Framework to Exercise Critical

Infrastructure Protection (CloudCERT) Project, which is developing a cloud computing environment to facilitate the exchange of information about threats and incidents between the various critical infrastructure stakeholders [19].

In this context, it is also necessary to highlight the role of cloud computing in critical infrastructure protection [2]. A cloud computing infrastructure provides several operational benefits, including data redundancy, data availability and survivability (when essential system components are isolated or lost). For example, if a SCADA control center loses its operational services, another control center could assume control using the ICCP protocol and the cloud infrastructure could support queries relating to critical information (e.g., alarms, processes and measurements). The use of the cloud paradigm to support data redundancy and data recovery introduces additional benefits such as asset virtualization and private, public or hybrid service-oriented architectures where the services are managed on-demand over the Internet [61]. Virtualization is based on the creation of a virtual platform of hardware resources (e.g., servers, network devices and storage) and operating systems to reduce costs while facilitating information sharing, manageability and isolation. In addition, a cloud computing infrastructure can influence the development of industrial applications that support interoperability and cooperation between organizations and entities.

Information within a cloud is shared by diverse providers and subscribers. Security and privacy mechanisms must therefore be implemented to protect sensitive data at rest and in motion; the mechanisms include cryptographic schemes, authentication and identity management, access control and accounting, as well as trust management, governance, policies and regulations [71]. Data redundancy within the cloud should also be considered carefully along with intrusion detection, alarms and incident handling.

3.2. *Wireless communications systems*

Long-range communication technologies such as mobile cellular (e.g., 3G/4G, UMTS, GPRS, GSM/TETRA, satellite, GPS, WiMAX and mobile broadband wireless access (MBWA)) and microwave systems also enable automation and control tasks at low cost, in addition to providing mobility, collaboration, reliability and coexistence with other technologies. Field operators can directly interact with industrial devices (e.g., RTUs with wireless transmitters) through handheld device interfaces by sending commands and receiving information such as status, measurements and alarms. Other technologies for medium- and small-scale control applications include Bluetooth, WLANs, mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) [58]. Cellular technology is often a relatively inexpensive alternative for connecting small groups of field devices and sending non-critical information to a SCADA control center. However, large numbers of cellular nodes for supervision can increase communications delays and the costs associated with data transfer [58].

Interest in these technologies has encouraged international organizations to specify communications standards such as ZigBee [87], ISA100.11a [41] and WirelessHART [31]. The advanced metering infrastructure of a smart grid depends heavily on these technologies to transfer significant amounts of information associated with customers and utilities (including SCADA systems). An advanced metering infrastructure is designed to measure, collect, present and analyze energy usage, and connect metering devices (associated with electricity, gas, heat and water) to utility business systems; this connectivity is bidirectional in that information is distributed to/from customers and other entities. For example, MBWA operates at 3.5 GHz with data rates of up to 1–20 Mpbs, and WiMAX operates at 2.3, 2.5 and 3.5 GHz with data rates up to 70 Mbps. These transmission capacities could enable the advanced metering infrastructure to send data streams from smart meters to utility business systems, including control systems that supervise energy substations.

Wireless communications networks are also becoming increasingly important for critical infrastructure protection. The networks enable human operators to establish in situ local connectivity without going through a SCADA control center while also providing mobility. This is the case with MANETs, which enable human operators to gain authorized access to system components (e.g., sensors, actuators and RTUs) and carry out operational activities such as data dissemination and management, incident response, parameter configuration and maintenance [10]. In this context, it is worth highlighting the role of wireless personal area networks (WPANs) for applications with less geographical coverage and where the control is limited to a small number of nodes (e.g., Bluetooth, Z-Wave and ZigBee). A variant of WPANs includes low-rate WPANs (LR-WPANs) [35] such as ZigBee, ISA100.11a, WirelessHART and MiWi/MiWi P2P networks [79].

Wireless technologies introduce inconveniences such as operational delays, latencies, electromagnetic and/or radio frequency interference and myriad security issues. The widespread use of repeaters and routers to intensify signals can significantly increase end-to-end delays. Other negative effects include slowing down data transfer and reducing data integrity, which ultimately affect the quality of service.

Other important aspects are the coexistence and reliability of communications between heterogeneous technologies. Some of the challenges relate to device authentication and authorization, information security and the interoperability of messages with different formats. A well-known threat to communications reliability is a jamming attack that alters the radio frequency channel; this attack works despite the frequency hopping used by wireless standards such as WirelessHART [31] and ISA100.11a [41]. Other threats impact the availability, integrity and confidentiality of data and other resources. For example, availability is impacted by denial-of-service attacks that overload communications channels, selective forwarding attacks that selectively send data to the next hop, sybil attacks that impersonate entities, black-hole attacks that drop messages, sinkhole/wormhole attacks that direct data to specific nodes and jamming attacks [6]. Integrity threats are posed by route falsification attacks and sybil attacks. Threats to confidentiality are presented by deliberate exposure attacks that intentionally reveal critical information, sniffing attacks that eavesdrop on communications channels, traffic analysis attacks and various physical attacks. Interested readers are referred to [6] for a discussion of these threats and others, along with the appropriate countermeasures.

3.3. *Embedded systems*

Embedded systems are based on constrained devices (also known as “objects”) with the ability to dynamically and autonomously interact with other devices. This requires that the objects be readable, recognizable, locatable, addressable and/or controllable [65]. The objects are responsible for controlling and managing energy generation and distribution systems that comprise a smart grid, such as RTUs, sensors, actuators, smart meters, phasor measurement units, mobile robots, vehicular nodes, storage devices, RFID tags and even the handheld interfaces used by human operators. The interoperation of these objects under a common communications infrastructure has led to a new concept called the Internet of Energy. The Internet of Energy is an infrastructure that is based on standards and interoperable communications technologies and protocols that interconnect energy networks with the Internet, enabling power units to be available when they are needed [14,46].

Wireless sensor networks also play a crucial role in infrastructure protection. According to [28,64], this technology and its smart objects (i.e., sensor nodes) can autonomously maintain control of a system, as well as detect, track and alert to threatening situations. The collaborative capabilities of wireless sensor networks make them one of the most sought after technologies for deployment in diverse critical infrastructure applications. In addition, their standalone and smart features enable them to adapt to the environmental conditions without losing functionality. Conventional sensors can work with 4 MHz, 1 KB of RAM and 4–16 KB of ROM whereas typical industrial nodes are configured with 4–32 MHz, 8–128 KB of RAM and 128–192 KB of ROM. The deployment of such devices depends on several factors, among them the criticality of the application context and the protection needs. Moreover, the devices can support the construction of prevention and response tools such as early warning systems and intrusion detection systems [3,5]. They can form part of an observation system that is in charge of perception, tracking, detection and alerting about anomalies or anomalous events. This also means that critical systems should require special investments in new technologies for (near) real-time control as well as technological components for security and protection.

The technologies described in this section have been incorporated in automated substations for the power grid. In fact, the American Recovery and Reinvestment Act (ARPA) of 2009 funded the creation of around 100 automated substations with thousands of sensor nodes to detect changes and prevent local and regional power blackouts [72]. The vast majority of these automated substations will be connected to the smart grid using the 6LowPAN standard [50], interacting with system objects compatible with the IPv6 [15] via Internet protocols for the smart grid. However, providing adequate interactivity from anywhere, anytime via the Internet can be a challenging task. Some studies (e.g., [11]) indicate that the full integration of sensors with the Internet using TCP/IP is a problem that remains to be addressed in order to increase connectivity and capacity. For example, if sensors are fully integrated into the Internet, any maintenance procedure of firmware could render portions of the system non-operational. On the other hand, the heterogeneity of objects and their arbitrary connections also increase incompatibilities [65], potentially resulting in an infrastructure that is more susceptible to vulnerabilities and threats.

4. Business continuity

This section focuses on the requirements imposed on critical information infrastructures (e.g., SCADA systems) in order to protect critical infrastructures (e.g., energy substations) and the requirements for protecting the communications infrastructure itself. Much of the discussion in this section is based on [7], which formally analyzed the operational and security requirements for control systems using dependency relationships [62].

In order for critical infrastructures to trust the good performance and reliability of information and communications technologies to manage their sensitive information, a set of functional services and requirements must be satisfied by critical information infrastructures. The requirements include performability, interoperability, scalability, extensibility, availability, reliability, resilience, safety criticality, autonomy and self-healing, usability, trust and collaboration between heterogeneous objects to address anomalous and threatening situations while maintaining fault tolerance and security.

The three first requirements are needed to adapt new hardware and software to existing resources. Interoperability is concerned with the ability of systems and organizations to work together to carry out a common goal. This concept is normally applied to engineering systems that involve various social, technical, political and organizational aspects, all of which play an essential role in business continuity [7]. This also means that control systems should ensure that existing resources as well as new resources can cooperate and interact with each other without impacting system functionality, communications protocols, industrial devices, software-based control components and security services. To this end, it is beneficial if certain portions of a system are responsible for defining and maintaining the governance of the entire system. Governance focuses on the development, implementation and adherence of security policies and technical specifications, as well as the access and availability of technical and legal documents.

Scalability refers to the ability to add or remove hardware resources; extensibility is related to the ability to extend or modify system software resources (e.g., security services and control applications) [17,86]. The introduction of new resources should not trigger changes to the services provided by a critical system. Note that scalability and extensibility do not necessarily guarantee interoperability and compatibility with existing resources. Therefore, it is necessary to specify and comply with technical and legal constructs such as policies, standards, recommendations and good practices.

Availability and reliability are two closely related concepts. Availability corresponds to the probability that a system delivers services when they are required at a time instant T_z. In contrast, reliability corresponds to the probability that a system can deliver services properly and their availability does not drop during the time period $[T_x, T_y]$ where $T_z \in [T_x, T_y]$ [33]. This relationship between the two properties means that if a control system needs to execute certain operations to perform commands (e.g., open or close a valve), the normal sequence of execution of the information infrastructure and the intermediary objects should not be disrupted or delayed. Otherwise, services delivered by the underlying system will not be available when they are needed and, therefore, the system will not be reliable.

Quality of service is also an important property because a disruption or alteration of a system due to faults, incidents, errors or threats could put the performance of an entire infrastructure at risk. Zheng and Lyu [84] have designed an adaptive quality-of-service-aware fault-tolerance strategy for web services based on a service-oriented architecture in order to dynamically adjust system parameters to their optimal fault-tolerant configurations. To develop a suitable quality of service strategy for critical systems, it is advisable to consider additional parameters such as the level of heterogeneity, variable nature and interactivity of the environment, network topology, weaknesses associated with objects, as well as interdependencies between nodes and systems. This would make it possible to adjust the essential parameters and design robust infrastructures with the ability to control faults and incidents.

Resilience and robustness are properties that help face adverse or threatening situations. In general, a system under threat should guarantee its functionality at all times even if certain parts of the system are seriously compromised. A fault could trigger a cascading effect due to internal dependencies existing between resources and system elements. For example, a software error in a network resource (e.g., gateway) could generate a progressive effect that might delay or interrupt essential operations, perhaps even isolate critical system components such as substations. If such an effect is not controlled properly, it could traverse the boundary of a critical system and ultimately impact the business continuity of other critical infrastructures.

Safety-critical aspects must be considered in order to control cascading effects [7]. The property of safety criticality involves avoiding or mitigating the propagation of effects between critical infrastructures, which could result in physical and physiological damage, injuries and deaths. To prevent these situations from occurring, control networks should incorporate autonomous, dynamic and intelligent approaches and ensure prevention and response in an efficient and timely manner.

Another important property is usability. Any user (expert or not) must be able to interact with a system via an intuitive interface. This means that interfaces should be designed to make information (such as alarms and sensor readings) easy to understand and to facilitate options for speeding up critical operations (such as managing actions in the field). In addition, when multiple heterogeneous objects are involved, the interfaces must map and manage information without delaying operational tasks; in threatening situations, they should help identify the exact locations of affected systems so that immediate responses can be implemented. Finally, environmental heterogeneities, the presence of different networks, topologies and objects, and the deployment of myriad services and applications should not impact business continuity and operational activities.

Collaboration between objects is vital in heterogeneous environments. For example, any active object in a system must know how to collaborate with other objects in a secure and transparent manner, and how to perform its tasks. In addition, all the objects should be trustworthy and should trust the information exchange to ensure rapid responses in adverse scenarios. Trust services can be also extended to application contexts where new technologies and infrastructures (such as cloud computing) play essential roles. If a system depends on a cloud computing infrastructure to store backup instances, then the critical infrastructures must be able to trust the cloud infrastructure and its elements (i.e., providers) for its management operations.

Fault tolerance is a requirement that should be considered in any critical environment to ensure business continuity in the face of hardware and software faults. One way to control faults is through strict security policies, maintainability and testability based on validation and verification processes, along with redundancy and dynamic approaches for fault detection, fault restoration and fault removal. These solutions make more sense in environments that incorporate different types of networks and myriad interacting objects [65]. Finally, security aspects should be addressed in the entire SCADA architecture to ensure availability, integrity and confidentiality of information and resources.

5. High priority protection areas

This section discusses high priority areas for critical infrastructure protection. The areas include governance and security management, secure network architectures, self-healing, modeling and simulation, wide-area situational awareness, forensics and learning, and trust management and privacy. These areas constitute the foundation of a "protection pyramid" for a critical information infrastructure.

5.1. *Governance and security management*

Governance is concerned with security controls (i.e., actions) that are used to manage an organization. The controls are defined in terms of security policies, standards, best practices and recommendations.

Security controls and their abstractions help regulate the overall behavior of a system made up of physical and virtual entities. These include human entities (e.g., staff members, providers and customers) and hardware/software entities (e.g., applications, services, resources and objects). To ensure interoperability between entities, a set of behaviors must be specified according to the type of application domain and its criticality, the interdependencies existing between organizations and resources, the information architecture and its coexistence with engineering systems, information management and the associated risks. Important issues that must be addressed by security controls include where, what, how and when an action can change the functionality of a system, and who or what should do it.

According to a control systems security report published by the U.S. Department of Homeland Security [74], security controls can be categorized as: organizational security sub-controls and operational sub-controls:

- *Organizational security sub-controls:* This category refers to security controls that are related to the organizational management (physical and cyber) of a system. The controls include security policy, organizational security, personnel security, physical and environmental security, strategic planning, security awareness and training, monitoring and reviewing control system security policy, risk management and assessment, and security program management.

- *Operational sub-controls:* This category refers to security controls that enable a system to perform activities (e.g., operational control and sensitive information management) securely. The controls include system and services acquisition (e.g., allocation and acquisition of control system assets, software and services), configuration management, information and document management, system development and maintenance, system and communications protection, incident management and response, system and information integrity, access control, audit and accountability, and media protection.

Standards and recommendations dealing with organizational and technical aspects have been proposed. Representative standards for information systems and SCADA communications systems include NIST 800-53 [55], NISTIR 7628 for smart grids [52,53], IEC 62351 [36], WirelessHART and ISA100.11a. Traditional standards, that are also useful, include ISA 99-1 and ISA 99-2 [42], ISO 17799 [37], ISO 27001 [40], ISO 27002 [39], ISO 19791 [38], among others. Aside from these standards, organizations should also use recommendations and guidelines for critical control systems to align their business models with an effective protection framework such as NERC CIP-2 [56], GAO-04-140T [75], IEEE 1402 (physical security of energy substations) [34] and API 1164 [13]. Tables 1 and 2 summarize the security sub-controls described above. Note that the majority of the standards and recommendations in the tables cover the organizational and operational aspects.

Security assessments should be included as part of the governance of a critical system and its security management. An assessment involves detailed reviews of the system architecture, its interconnected objects and entities, and the information system to ensure that they comply with the security policies and the business model. Maintenance and auditing activities facilitate security assessments. Maintenance focuses not only on modifying or repairing faults, but also on satisfying new requirements, improving performance, reducing costs by simplifying future maintenance and enabling adaptation to changing environments. Auditing involves checking whether or not the architecture complies with the requirements imposed on the system. To properly address accountability aspects, issues related to responsibility and activity (e.g., storage, access and format) should also be addressed in security policies.

5.2. *Secure network architectures*

Underlying every SCADA network architecture is a substantial deployment of hardware and software resources, which include the Internet, web-based SCADA interfaces, wireless communications systems and automation and control technologies. Clearly, it is vital to secure the SCADA networks as well as their underlying resources to the extent possible.

The U.K. National Infrastructure Security Coordination Centre (NISCC) [51] has specified good practices for firewall deployment in SCADA and process control networks. The good practices state that a critical network should be divided into three main zones: firewalls, intrusion detection systems and demilitarized zones.

Table 1 – Compliance with organizational and operational standards for critical control systems.

Security control	Organizational and operational standards							
	NIST 800-53	NISTIR 7628	ISA 99-1	ISA 99-2	ISO 177799	ISO 27001	ISO 27002	ISO 19791
Organizational security sub-controls								
Security policies	✓	✓	✓	✓	✓	✓	✓	
Personnel security	✓	✓		✓	✓	✓	✓	✓
Physical and environmental security	✓	✓	✓	✓	✓	✓	✓	✓
Strategic planning	✓	✓	✓	✓	✓	✓	✓	✓
Security awareness and training	✓	✓		✓	✓	✓		✓
Monitoring and reviewing sec. policy	✓	✓	✓	✓	✓	✓	✓	
Risk management and assessment	✓	✓	✓	✓	✓	✓	✓	
Security program management	✓	✓						
Operational security sub-controls								
System and services acquisition	✓	✓	✓	✓	✓	✓		✓
Configuration management	✓	✓	✓	✓	✓	✓		✓
System and communications protection	✓	✓	✓	✓	✓	✓	✓	✓
Information and document management	✓	✓		✓	✓	✓		✓
System development and maintenance	✓	✓	✓	✓	✓	✓	✓	✓
Incident management and response	✓	✓		✓	✓	✓	✓	✓
System and information integrity	✓	✓			✓	✓		✓
Access control	✓	✓		✓	✓	✓	✓	✓
Audit and accountability	✓	✓		✓	✓	✓	✓	✓
Media protection	✓	✓			✓	✓		

Table 2 – Compliance with technical standards, recommendations and guidelines for critical control systems.

Security control	Technical standards					Recommendations and guidelines					
	IEC 62351	FIPS 140-2	WirelessHART	ISA100.11a	ZigBee	AGA 12-1	AGA 12-2	NERC CIP	GAO-04-140T	IEEE 1402	API Sec
Organizational security sub-controls											
Security policies		✓	✓	✓	✓	✓		✓			✓
Organizational security						✓		✓			✓
Personnel security		✓				✓		✓		✓	✓
Physical and environmental security	✓	✓				✓		✓		✓	✓
Strategic planning		✓				✓		✓		✓	✓
Security awareness and training		✓				✓		✓		✓	✓
Monitoring and reviewing sec. policy						✓		✓			✓
Risk management and assessment						✓		✓			✓
Security program management	✓										
Operational security sub-controls											
System and services acquisition		✓	✓	✓	✓	✓		✓	✓		✓
Configuration management		✓	✓	✓	✓	✓		✓			✓
System and communications protection	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Information and document management		✓	✓	✓	✓	✓		✓			✓
System development and maintenance	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
Incident management and response	✓	✓	✓	✓	✓	✓		✓		✓	✓
System and information integrity	✓	✓		✓	✓	✓	✓	✓			✓
Access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Audit and accountability		✓	✓	✓	✓	✓		✓			✓
Media protection						✓		✓			✓

A firewall is responsible for delimiting the system boundaries; it analyzes incoming and outgoing network traffic and determines whether or not the traffic should be allowed based on predetermined rules (e.g., messages IDs should be unique and identifiable). An intrusion detection system monitors network traffic and system processes to detect and mitigate activities that violate the established security policies. A SCADA system may incorporate network intrusion detection systems as well as host intrusion detection systems. A network intrusion detection system is an independent platform that identifies intrusions by examining network traffic; its sensors are strategically deployed at vulnerable locations to enable network packet capture and the analysis of the contents of individual packets. A host intrusion detection system functions in the same manner, except that it concentrates on a host instead of a network. A demilitarized zone is a physical or logical sub-network that exposes limited services to untrusted networks, usually the Internet or corporate networks. Servers are typically configured within a demilitarized zone to maintain historical information (e.g., alarms, measurements and executed processes); the information is usually secured from unauthorized access using authentication and encryption.

The configuration of the three zones according to the NISCC good practices corresponds to the first line of defense for control systems, where access to critical servers is protected using a defense-in-depth approach. However, the proprietary nature of SCADA protocols makes it difficult to use conventional security mechanisms to construct the zones. The vast majority of security mechanisms do not fit in well with SCADA requirements and policies. For example, intrusion detection systems have to employ highly specific rules to model SCADA protocol characteristics, which hinder scalability and extensibility. Likewise, rules created for intrusion prevention systems must be defined so that they do not put the SCADA system at risk. Consequently, it is necessary to identify dependencies between services and applications and use the knowledge to segment, isolate and protect critical areas (e.g., alarm management applications). One way to achieve this is to reduce visibility using appropriate access control mechanisms, privileges or roles, or even hardcoded restrictions in firewalls and intrusion detection systems.

Privileges and roles must be assigned according to responsibility areas, functionality and trust, and knowledge and experience. The access control policies should be supported by security mechanisms, specialized software and electronic devices (e.g., biometric systems, smart cards and electronic keys). However, it is important to be aware that some current SCADA architectures are designed to rely on simple authentication mechanisms based on passwords where responsibilities are created with permissions that limit actions. This forces the system to frequently update security credentials, check and close inactive accounts, limit the number of active/inoperative sessions and automatically block accounts with multiple failed login attempts.

In addition to securing the network architecture, it is necessary to protect communications channels from external access. Confidentiality can be maintained using security mechanisms that support encryption; examples include tunneling mechanisms that provide secure virtual connectivity between networks (e.g., virtual private networks) or "bump-in-the-wire" devices (e.g., a device positioned between the RS/EIA-232 port of an RTU and a modem). One of the first organizations to work on SCADA cryptography was the American Gas Association, which published two key reports: AGA-12 Part 1 [29] and AGA-12 Part 2 [29]. Both reports deal with the use and implementation of cryptographic services in serial channels and protocols based on sessions using authentication services and symmetric keys generated by AES and SHA-1.

Integrity and authentication can be implemented using security mechanisms or services recommended by SCADA security standards such as IEC 62351 [36]. This standard recommends the use of TLS/SSL protocols and digital certificates, message authentication code, key interchange (at least 1024 bits) and cryptographic services such as RSA and DSS.

It is worth mentioning that the TCP/IP security services offered by RFC 6272 for IPv6 was recently specified for smart grid networks [15]. When the environment is composed of objects such as industrial sensors, it is also necessary to consider security services for their communications protocols. Each communications protocol defines its own security restrictions according to its protocol stack. For example, the security in the PHY and MAC layers of ZigBee, WirelessHART and ISA100.11a depend on the IEEE 802.15.4 standard, which offers hardware support for 128-bit AES and a message integrity code (MIC)/message authentication code (MAC) with 32/64/128 bits. The MIC has three main fields: a frame control (that includes a security mode, unique counter for relay and key identifier), security control and data payload. In addition, IEEE 802.15.4 provides sensor nodes with an access control list containing trusted neighbor nodes for authenticating peers involved in communications.

Depending on the application context (e.g., open or closed environment) and the computational capabilities of the embedded devices (e.g., sensor nodes), network designers must define the security and network parameters necessary to provide adequate protection. An ideal tool for the purpose is SenseKey, an extensible and scalable tool that helps select the most suitable key management schemes based on performance, resilience, scalability, extensibility and global/local communications. SenseKey supports key management schemes for several SCADA communications protocols, including ZigBee, ISA100.11a and WirelessHART [9].

It is vital that changes to network and routing configurations do not cause network congestion or impact the quality of service. The specific protocol being used must be considered when attempting to adapt a network deployment; this is because each protocol has its own stack architecture, requirements and connectivity conditions. For example, most wireless communications standards applicable to wireless sensor networks (e.g., ISA100.11a, WirelessHART and Zigbee) are based on the IEEE 802.15.4 standard that specifies their PHY and MAC layers. The remaining layers, which are implemented above this standard, depend on the protocol features. For example, Zigbee defines its own network layer (where the nodes follow a many-to-one network topology) and application layer. The application layer incorporates two important sub-layers: ZigBee Device Object and Application Framework.

5.3. *Self-healing*

The notion of self-healing has its origins in research on fault-tolerant systems. A self-healing system can handle transient or permanent faults through local and individual actions and reach an acceptable state. In order to achieve fault tolerance, it is necessary to address issues related to redundancy, coordination and self-stabilization [59]. Redundancy enables a system to autonomously recover in adverse situations; this is achieved by maintaining redundant (backup) copies at strategic locations or duplicating functionalities. Coordination enables a system to autonomously handle concurrency and consistency in distributed environments involving interactions between diverse entities (e.g., software processes, human operators and control resources). To achieve this, the coordination must be supported by synchronization mechanisms based on actuation policies that regulate all actions between entities. The actuation policies should preclude unauthorized access and avoid unsuitable actions that result in interruption, alteration or damage during system operations.

Redundancy should also consider synchronization because system components could have transient faults due to coordination problems. For example, redundant (hardware and software) resources can fall into unplanned states due to the discordant execution of processes or inconsistent parameters or variables. One way of mitigating unforeseen states is to use Dijkstra's notion of self-stabilization [23] to dynamically control arbitrary transient faults by converging to normal states in a finite number of steps.

Although self-stabilization research is still in its infancy, some approaches in the literature can be applied to critical systems. For example, Datta et al. [22] have proposed an approach for dynamically controlling mutual exclusion in distributed networks, where critical sections between successive executions are dependent on an arbitrary distributed scheduler. Chen and Welch [18] have similarly proposed a self-stabilizing approach for controlling mutual exclusion using token ad hoc networks with arbitrary mobile resources.

5.4. *Modeling and simulation*

The modeling and simulation of multiple infrastructures is a challenging research area. The goal is to model and simulate normal and anomalous behaviors in order to analyze complexities, infrastructure resilience and the functionality of fault-tolerance mechanisms. This implies a study of the causes, risks, consequences and effects by mapping and visualizing a global representation of the existing entities, objects and resources, as well as their interconnections, irregular behaviors and interdependent relationships.

Modeling and simulation also provide insights into behaviors associated with infrastructures and their interrelationships to improve business continuity from a socio-economic point of view. For example, an organization could (i) compute the long-term technical or economic situation according to existing interdependencies and their impact on economic, social and legal aspects; (ii) locate weak spots in existing infrastructures to optimize future investments; (iii) study the social impact of large-scale disruptions; (iv) optimize the deployment of resources and objects; and (v) define strategic plans for preparedness and mitigation. Modeling and simulation can also be used to refine governance and security management via new policies and strategic business and market plans, contingency and emergency plans, and recovery and mitigation plans.

According to Rinaldi [62], there are six possible ways of modeling and simulating systems: (i) aggregate supply and demand approaches that analyze the loss of infrastructure assets; (ii) physics-based models using standard engineering techniques to evaluate the physical aspects of infrastructures; (iii) agent-based models for expressing operational functionalities and physical states of infrastructures; (iv) population mobility models for understanding how mobile consumers affect the integrity of an infrastructure; (v) Leontief input-output models for analyzing risk in interdependent infrastructures under time dependencies; and (vi) dynamic simulation approaches for visually representing infrastructure operations and the effects of disruptions. Interested readers are referred to [60] for an analysis of many of these techniques along with the modeling and simulation challenges. Among the most important challenges are the complexity of interdependent infrastructures, simulation time frames, types and numbers of samples and observed events, and data collection.

5.5. *Wide-area situational awareness*

One of the challenges that must be addressed is the avoidance and mitigation of the collateral effects caused by faults and attacks. According to the National Institute of Standards and Technology (NIST) and Federal Energy Regulatory Commission (FERC), this is a priority research area for critical infrastructures such as smart grids. This priority area, known as wide-area situation awareness [8,54], focuses on monitoring critical systems located over large geographic areas in near real-time, ensuring the prevention, detection and response to problems before they escalate and cause serious disruptions.

Prevention and detection focus on anticipating and detecting internal or external faults that produce deviations from the normal state. This requires effective proactive tools that are normally supported by high-level security services. For example, an anomaly prevention service would ideally recognize anomalous occurrences at any given instant of time (i.e., fault detection) or in advance (i.e., fault prevention). The former (fault detection) is performed by intrusion detection systems that monitor network traffic using patterns, rules and knowledge of past events. The latter (fault prevention) relies on automated, dynamic tools such as early warning systems that can predict the presence of faults.

Incident response makes use of reactive and recovery tools that enable a system to automatically and rapidly address threatening situations. The tools must be configured to ensure business continuity. An example reactive tool is Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD), which can trace malicious activities across large networks and initiate attack isolation and automated response [69]. Recovery tools are responsible for addressing faults as well as enabling a system to move to its normal operating state. An example is a tool developed by the SELFMAN Project [68], which implements self-healing in large-scale distributed systems by automatically and dynamically handling, reconfiguring and recovering from anomalous states. These protection services depend on technologies such as the Internet, GPS, mobile ad hoc networks and wireless sensor networks [10]. The Internet and GPS offer global connectivity, geolocation and visualization of the physical points that require particular attention. Mobile ad hoc networks provide local connectivity to attend to a situation in situ and in real time while wireless sensor networks support continuous monitoring, detection, tracking and alerting to threatening situations. Despite many advances, much research remains to be done in the area of wide-area situational awareness. In particular, many situational awareness approaches do not ensure complete protection based on prevention, detection and response [54], nor do they satisfy the unique conditions and prerequisites of industrial control environments (e.g., efficient, rapid and 24/7 operational performance) [7].

5.6. *Forensics and learning*

After anomalous symptoms, faults or failures have occurred, it is important to promptly conduct comprehensive analyses to determine the root causes and ultimately develop and implement countermeasures. This task is primarily forensic in nature. For this reason, the Colloquium for Information Systems Security Education (CISSE) [21] has created a working group to devise dynamic techniques applicable to mission-critical environments that are based on sound forensic methodologies. Given the geographic scale of critical infrastructures, forensic methodologies should be applicable remotely, on demand and in any mode (on-line, off-line or in situ) without impacting system performance or business continuity. One way to address this challenge is to ensure that redundant systems are available when applying forensic methodologies.

It is important to consider the constraints imposed by the operational environment when implementing forensic methodologies. The constraints may be associated with architectural complexities and interdependencies, dependencies on information and communications technologies and components developed by third parties (i.e., COTS components), and the deployment of heterogeneous technologies. The computational and storage limitations of field devices could limit the application of forensic methodologies for gathering and analyzing evidence. Therefore, it is necessary to develop lightweight mechanisms to support evidence collection, analysis and correlation from constrained field devices such as sensors, handheld interfaces, smart meters and RTUs. One solution for evidence collection is to use powerful external storage devices to capture traffic without affecting system performance. Network traffic and network event data from intrusion detection systems and network sensors could also be leveraged for forensic analyses.

The results of correlations and analyses could serve as valuable input to learning techniques. The learning techniques could endow a system with dynamic and autonomous decision making capabilities. A system could, for example, learn from sequences of anomalous events and automatically generate new patterns and rules to implement rapid response. Data mining [81] techniques have been leveraged to predict and discover new behaviors using sequential patterns [32] and time series and statistical analyses [66]. Research on lightweight learning mechanisms is a priority for complex and dynamic systems used in critical infrastructures and other mission-critical environments.

5.7. *Trust management and privacy*

As mentioned previously, a simple way to compute trust is through reputation – a mathematical concept that enables a system to enhance its decision making processes and its ability to compute the level of reliability of observed entities. An initial incident management framework for control systems that leverages these benefits is proposed in [1]. This framework monitors and assigns alarms based on incident severity and the availability of experienced personnel to assist in emergency situations. Computations of trust or reputation can be performed using approaches based on logic, graph theory or Bayesian networks [44].

Concerns about privacy have recently been raised regarding smart grids. The bi-directional advanced metering infrastructure used in smart grids enables electric utilities to increase efficiency and reduce costs, but the data pertaining customer usage behavior that is collected, stored and analyzed can pose significant threats to personal privacy. In particular, customer activity patterns can be deduced from signals received from home appliances called load signatures or power fingerprints [83]. Kalogridis et al. [45] have proposed a power management model based on the use of batteries in appliances to register different load signatures within smart meters, thereby hiding the real electricity usage patterns. Additional research is needed to develop cost-effective, robust privacy solutions for home appliances and smart meters.

Concerns about location-based privacy should also be addressed with regard to the locations of industrial devices and other sensitive assets [85]. Most of the approaches proposed for protecting location information rely on intrinsic features of signals (e.g., strength and coverage) and network traffic [48]. It is imperative to prevent unauthorized entities from inferring device location by analyzing network traffic [57]. Additional research is needed in this area, especially with regard to developing flexible, lightweight solutions for protecting field devices.

6. Conclusions

The scale and diversity of critical infrastructures, and in particular, industrial control (SCADA) systems, require the design and deployment of numerous protection measures. Protection efforts should focus on traditional security mechanisms for detecting and responding to threats as well as intelligent systems that can proactively identify vulnerabilities and faults that can be exploited by attackers. This paper has analyzed the relevance of new technologies in automation and control, along with the need to protect industrial control systems that integrate new and legacy technologies. Several requirements and challenges related to infrastructure protection are discussed. Priority areas for research include governance and security management, secure network architectures, modeling and simulation, wide-area situational awareness, forensics and learning, and trust management and privacy. It is hoped that the discussion of requirements and challenges will stimulate renewed efforts at protecting critical infrastructure assets in general and industrial control systems in particular.

Acknowledgment

This research was supported by the Marie Curie COFUND Programme U-Mobility, the University of Málaga, the European Commission FP7 Project under GA no. 246550 and the Ministerio de Economía y Competitividad (COFUND2013-40259).

REFERENCES

[1] C. Alcaraz, I. Agudo, C. Fernandez-Gago, R. Roman, G. Fernandez, J. Lopez, Adaptive dispatching of incidents based on reputation for SCADA systems, in: Proceedings of the Sixth International Conference on Trust, Privacy and Security in Digital Business, 2009, pp. 86–94.

[2] C. Alcaraz, I. Agudo, D. Nunez, J. Lopez, Managing incidents in smart grids a la cloud, in: Proceedings of the Third IEEE International Conference on Cloud Computing Technology and Science, 2011, pp. 527–531.

[3] C. Alcaraz, A. Balastegui, J. Lopez, Early warning system for cascading effect control in energy control systems, in: Proceedings of the Fifth International Conference on Critical Information Infrastructures Security, 2010, pp. 55–67.

[4] C. Alcaraz, G. Fernandez, F. Carvajal, Security aspects of SCADA and DCS environments, in: J. Lopez, R. Setola, S. Wolthusen (Eds.), Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense, Springer, Berlin, Heidelberg, Germany, 2011, pp. 120–149.

[5] C. Alcaraz, C. Fernandez-Gago, J. Lopez, An early warning system based on reputation for energy control systems, IEEE Trans. Smart Grid 2 (4) (2011) 827–834.

[6] C. Alcaraz, J. Lopez, A security analysis for wireless sensor mesh networks in highly critical systems, IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. 40 (4) (2010) 419–428.

[7] C. Alcaraz, J. Lopez, Analysis of requirements for critical control systems, Int. J. Crit. Infrastruct. Prot. 5 (3–4) (2012) 137–145.

[8] C. Alcaraz, J. Lopez, Wide-area situational awareness for critical infrastructure protection, IEEE Comput. 46 (4) (2013) 30–37.

[9] C. Alcaraz, J. Lopez, R. Roman, H. Chen, Selecting key management schemes for WSN applications, Comput. Secur. 31 (8) (2012) 956–966.

[10] C. Alcaraz, J. Lopez, J. Zhou, R. Roman, Secure SCADA framework for the protection of energy control systems, Concurr. Comput. Pract. Exp. 23 (12) (2011) 1414–1430.

[11] C. Alcaraz, R. Roman, P. Najera, J. Lopez, Security of industrial sensor network based remote substations in the context of the Internet of Things, Ad Hoc Netw. 11 (3) (2013) 1091–1104.

[12] C. Alcaraz, S. Zeadally, Critical control system protection in the 21st century, IEEE Comput. 46 (4) (2013) 74–83.

[13] American Petroleum Institute, API Standard 1164: Pipeline SCADA Security, 2nd ed., American Petroleum Institute, Washington, DC, 2009.

[14] ARTEMIS Project, Internet of Energy for Electric Mobility, SINTEF, Oslo, Norway, 2011.

[15] F. Baker, D. Meyer, Internet Protocols for the Smart Grid, RFC 6272, 2011.

[16] U. Bendisch, S. Bologna, G. Le Grand, E. Luiijf, Towards a European research agenda for CIIP: results from the CI2RCO Project, in: J. Lopez, B. Hammerli (Eds.), Critical Information Infrastructures Security, Springer, Heidelberg, Germany, 2008, pp. 1–12.

[17] A. Bondi, Characteristics of scalability and their impact on performance, in: Proceedings of the Second International Workshop on Software and Performance, 2000, pp. 195–203.

[18] Y. Chen, J. Welch, Self-stabilizing mutual exclusion using tokens in mobile ad hoc networks, in: Proceedings of the Sixth International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, 2002, pp. 34–42.

[19] CloudCERT, Testbed Framework to Exercise Critical Infrastructure Protection, National Institute of Communication Technologies, Leon, Spain, 2012.

[20] T. Cohen, M. Lubell, Nations must talk to halt "cyber terrorism:" Kaspersky, Reuters, June 6, 2012.

[21] Colloquium for Information Systems Security Education, Belleville, Michigan ⟨www.cisse.info⟩, 2014.

[22] A. Datta, M. Gradinariu, S. Tixeuil, Self-stabilizing mutual exclusion using an unfair distributed scheduler, in: Proceedings of the Fourteenth International Parallel and Distributed Processing Symposium, 2000, pp. 465–470.

[23] E. Dijkstra, Self-stabilizing systems in spite of distributed control, Commun. ACM 17 (11) (1974) 643–644.

[24] European Commission, Critical Infrastructure Protection in the Fight Against Terrorism, COM(2004) 702 Final, Brussels, Belgium, 2004.

[25] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 Final, Brussels, Belgium, 2005.

[26] European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 Final, Brussels, Belgium, 2006.

[27] Exemys, Exemys, Buenos Aires, Argentina ⟨www.exemys.com⟩, 2014.

[28] V. Gungor, G. Hancke, Industrial wireless sensor networks: challenges, design principles and technical approaches, IEEE Trans. Ind. Electron. 56 (10) (2009) 4258–4265.

[29] M. Hadley, K. Huston, AGA 12, Part 2, Performance Test Plan, National SCADA Test Bed, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy, Washington, DC, 2006.

[30] K. Harrison and G. White, A taxonomy of cyber events affecting communities, in: Proceedings of the Forty-Fourth Hawaii International Conference on System Sciences, 2011.

[31] HART Communication Foundation, WirelessHART Technical Notes ⟨en.hartcomm.org/hcp/tech/articles/wiHART_resources/witech_witechnote.html⟩, 2014.

[32] S. Hou, X. Zhang, Alarm association rules based on a sequential pattern mining algorithm, in: Proceedings of the Fifth International Conference on Fuzzy Systems and Knowledge Discovery, vol. 2, 2008, pp. 556–560.

[33] Institute of Electrical and Electronics Engineers, IEEE Standard 610-1990—IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries, Piscataway, New Jersey, 1990.

[34] Institute of Electrical and Electronics Engineers, IEEE Standard 1402-2000—IEEE Guide for Electric Power Substation Physical and Electronic Security, Piscataway, New Jersey, 2000.

[35] Institute of Electrical and Electronics Engineers, IEEE Standard 802.15.4d-200p—IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), Amendment 3: Alternative Physical Layer Extension to Support the Japanese 950 MHz Bands, Piscataway, New Jersey, 2009.

[36] International Electrotechnical Commission, IEC 62351: Power Systems Management and Associated Information Exchange—Data and Communications Security, Geneva, Switzerland, 2013.

[37] International Organization for Standardization, ISO/IEC 17779: 2005, Technology of Information Techniques Related to Security Code for the Practice of the Security Management of Information, Geneva, Switzerland, 2005.

[38] International Organization for Standardization, ISO/IEC TR 19791:2010: Information Technology—Security Techniques—Security Assessment of Operational Systems, Geneva, Switzerland, 2010.

[39] International Organization for Standardization, ISO/IEC 27002:2013: Information Technology—Security Techniques—Code of Practice for Information Security Controls, Geneva, Switzerland, 2013.

[40] International Organization for Standardization, ISO/IEC 27001:2013: Information Technology—Security Techniques—Information Security Management Systems – Requirements, Geneva, Switzerland, 2013.

[41] International Society of Automation, ANSI/ISA-100.11a-2011 Wireless Systems for Industrial Automation: Process Control and Related Applications, Research Triangle Park, North Carolina, 2011.

[42] International Society of Automation, Security for Industrial Automation and Control Systems, Security Technologies for Industrial Automation and Control Systems, ISA-TR62443-3-1 (99.03.01), Research Triangle Park, North Carolina, 2012.

[43] M. Jain, A. Jain, M. Srinivas, A web-based expert system shell for fault diagnosis and control of power system equipment, in: Proceedings of the International Conference on Condition Monitoring and Diagnosis, 2008, pp. 1310–1313.

[44] A. Josang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2) (2007) 618–644.

[45] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, R. Cepeda, Privacy for smart meters: towards undetectable appliance load signatures, in: Proceedings of the First IEEE International Conference on Smart Grid Communications, 2010, pp. 232–237.

[46] S. Karnouskos, The cooperative Internet of Things enabled smart grid, in: Proceedings of the Fourteenth IEEE International Symposium on Consumer Electronics, 2010.

[47] E. Knapp, J. Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and

Other Industrial Control Systems, Syngress, Waltham, Massachusetts, 2011.

[48] J. Krumm, A survey of computational location privacy, Pers. Ubiquitous Comput. 13 (6) (2009) 391–399.

[49] R. McClanahan, SCADA and IP: is network convergence really here?, IEEE Ind. Appl. 9 (2) (2003) 29–36.

[50] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944, 2007.

[51] National Infrastructure Security Coordination Centre, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, London, United Kingdom, 2005.

[52] National Institute of Standards and Technology, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture and High-Level Requirements, NISTIR 7628, Gaithersburg, Maryland, 2010.

[53] National Institute of Standards and Technology, Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References, NISTIR 7628, Gaithersburg, Maryland, 2010.

[54] National Institute of Standards and Technology, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, NIST Special Publication 1108 R2, Gaithersburg, Maryland, 2012.

[55] National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53, Revision 4, Gaithersburg, Maryland, 2013.

[56] North American Electric Reliability Corporation, CIP-002: Critical Cyber Asset Identification, NERC CIP Standard, Washington, DC, 2009.

[57] S. Pai, S. Bermudez, S. Wicker, M. Meingast, T. Roosta, S. Sastry, D. Mulligan, Transactional confidentiality in sensor networks, IEEE Secur. Priv. 6 (4) (2008) 28–35.

[58] P. Parikh, M. Kanabar, T. Sidhu, Opportunities and challenges of wireless communications technologies for smart grid applications, in: Proceedings of the IEEE Power and Energy Society General Meeting, 2010.

[59] H. Psaier, S. Dustdar, A survey on self-healing systems: approaches and systems, Computing 91 (1) (2011) 43–73.

[60] T. Rigole, G. Deconinck, A survey on modeling and simulation of interdependent critical infrastructures, in: Proceedings of the Third IEEE Benelux Young Researchers Symposium in Electrical Power Engineering, paper 44, 2006.

[61] B. Rimal, C. Eunmi, I. Lumb, A taxonomy and survey of cloud computing systems, in: Proceedings of the Fifth International Joint Conference on INC, IMS and IDC, 2009, pp. 44–51.

[62] S. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, in: Proceedings of the Thirty-Seventh Annual Conference on Hawaii International System Sciences, 2004.

[63] S. Rinaldi, J. Peerenboom, T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, IEEE Control Syst. 21 (6) (2001) 11–25.

[64] R. Roman, C. Alcaraz, J. Lopez, The role of wireless sensor networks in the area of critical information infrastructure protection, Inf. Secur. Tech. Rep. 12 (1) (2007) 24–31.

[65] R. Roman, P. Najera, J. Lopez, Securing the Internet of Things, IEEE Comput. 44 (9) (2011) 51–58.

[66] A. Salah, E. Pauwels, R. Tavenard, T. Gevers, T-patterns revisited: mining for temporal patterns in sensor data, Sensors 10 (8) (2010) 7496–7513.

[67] A. Salihbegovic, V. Marinkovic, Z. Cico, E. Karavdic, N. Delic, Web based multilayered distributed SCADA/HMI system in refinery application, Comput. Stand. Interfaces 31 (3) (2009) 599–612.

[68] SELFMAN Project, Self-Management for Large-Scale Distributed Systems based on Structured Overlay Networks and Components, Catholic University of Louvain, Louvain-la-Neuve, Belgium, 2010.

[69] SRI International, Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD), Menlo Park, California ⟨www.csl.sri.com/projects/emerald⟩, 2014.

[70] K. Suresh, R. Kirubashankar, K. Krishnamurthy, Research of Internet based supervisory control and information system, in: Proceedings of the International Conference on Recent Trends in Information Technology, 2011, pp. 1180–1185.

[71] H. Takabi, J. Joshi, G. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. 8 (6) (2010) 24–31.

[72] The White House, President Obama announces $3.4 billion investment to spur transition to smart energy grid, Washington, DC, October 27, 2009.

[73] U.S. Department of Homeland Security, National Infrastructure Protection Plan (NIPP), Washington, DC, 2009.

[74] U.S. Department of Homeland Security, Catalog of Control Systems Security: Recommendations for Standards Developers, Washington, DC, 2011.

[75] U.S. General Accounting Office, Critical Infrastructure Protection, Challenges in Securing Control Systems, Robert F. Dacey, Testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, GAO-04-140T, Washington, DC, 2003.

[76] U.S. General Accounting Office, Critical Infrastructure Protection, Cybersecurity Guidance is Available, but More can be Done to Promote its Use, Report to Congressional Requesters, GAO-12-92, Washington, DC, 2011.

[77] U.S. Government, Homeland Security Act 2002—Public Law 107-296, Washington, DC, 2002.

[78] WebSCADA Corporation, WebSCADA, Irvine, California ⟨www.webscada.com⟩, 2014.

[79] Y. Yang, Microchip MiWi P2P Wireless Protocol, AN1204, Microchip Technology, Chandler, Arizona, 2010.

[80] Yokogawa, Yokogawa Electric Corporation, Tokyo, Japan ⟨www.yokogawa.com⟩, 2014.

[81] S. Zanero, S. Savaresi, Unsupervised learning techniques for an intrusion detection system, in: Proceedings of the ACM Symposium on Applied Computing, 2004, pp. 412–419.

[82] S. Zeadally, G. Martinez, H. Chao, Securing cyberspace in the 21st century, IEEE Comput. 46 (4) (2013) 22–23.

[83] S. Zeadally, A. Pathan, C. Alcaraz, M. Badra, Towards privacy protection in the smart grid, Wirel. Pers. Commun. 73 (1) (2013) 23–50.

[84] Z. Zheng, M. Lyu, An adaptive QoS-aware fault-tolerance strategy for web services, Empir. Softw. Eng. 15 (4) (2010) 323–345.

[85] B. Zhu, A. Joseph, S. Sastry, A taxonomy of cyber attacks on SCADA systems, in: Proceedings of the International Conference on the Internet of Things and the Fourth International Conference on Cyber, Physical and Social Computing, 2011, pp. 380–388.

[86] Q. Zhu, Y. Yang, E. Scholte, M. Natale, A. Sangiovanni-Vicentelli, Optimizing extensibility in hard real-time distributed systems, in: Proceedings of the Fifteenth IEEE Real-Time and Embedded Technology and Applications Symposium, 2009, pp. 275–284.

[87] ZigBee Alliance, ZigBee-2007 Layer PICS and Stack Profiles, Revision 3, ZigBee Document 08006r03, San Ramon, California, 2008.