enisa
European Network and Information Security Agency

Protecting Industrial Control Systems

Annex I: Desktop Research Results

[Deliverable – 2011-12-09]

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on CIIP & Resilience, please use the following details:

- E-mail: resilience@enis.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to industrial control systems' security, please use the following details:

- E-mail: Evangelos.Ouzounis@enisa.europa.eu

Contents

1 Desktop Research Results

In the following sections we will present various chapters describing the most interesting current aspects in the world of security in Industrial Control Systems. This section is part of the results of the Desktop Research phase.

Chapter 1.1 starts by providing an overview of the different types of ICS, their components, architecture and role inside Critical Infrastructures and other organizations that make use of them. It then continues analyzing, from a security point of view, the dependencies of ICS on third-party ICT infrastructures. It considers both the underlying ICT communication infrastructure as well as dependent ICS. Chapter 1.1 also highlights that real incidents are already happening and affecting ICS and presents a thorough analysis of the different threats that could affect these systems. Furthermore, it also presents the current risk factors from a high level perspective and what make these systems highly vulnerable. Finally, this section reviews the main differences between ICS and regular IT systems stressing the fact that different and adapted technologies, procedures and management controls should be put in place.

Chapter 1.2 is devoted to analysing emerging issues in the context of ICS security. Targeted attacks against ICS are presented, reviewing the well known Stuxnet and Night Dragon cases. This chapter also introduces cloud computing as an emerging technology that could bring benefits to the industrial control arena. Drawbacks are also included as a counterpoint. Finally, the interrelationships between the new Smart Grid and more classic ICS are reviewed, analyzing potential synergies and risks.

Chapter 1.3 is a compendium of the current challenges to ICS security that have been identified during the desktop research phase. Challenges might affect multiple types of stakeholders and sheds light on the current needs, tendencies, and deficiencies that should be addressed in the near or long term.

Chapter 1.4 introduces the current policy context through which the protection of ICS should be viewed, and mainly those ICS included in critical infrastructures. It provides an overview of recent European legislative history, listing and briefly describing all the EC's relevant Communications and Directives. It also goes over the main legislative actions that have been undertaken in the context of the main member states. Additionally, this section also presents the policy context of other non-member state countries but of high international relevance.

Chapter 1.4.5 provides a thorough analysis of the different technical solutions that are currently being applied for securing ICS. No commercial product has been advertised but their capabilities have been considered when preparing this chapter.

Finally, chapter 1.6 goes over a large number of standards, guidelines, regulatory documents as well as actives groups and initiatives in the field of ICS security. The lists do not try to be exhaustive but to present the most relevant ones at an international and local level.

1.1 General considerations on ICS Security

This section provides an overview of the different types of ICS, their architecture and role inside Critical Infrastructures. It also presents an analysis of the dependencies of ICS on third-party ICT infrastructures. Additionally, this section provides a review of some real security incidents, as well as the different threats that could affect these systems. Furthermore, it summarizes the key risk factors that make these systems highly vulnerable. The section concludes with an overview on the main differences between ICS and regular IT systems.

1.1.1 ICS Systems overview

According to NIST SP 800-82 (1) an Industrial Control Systems (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures".

Even though there are different types of control systems, all of them share similar security properties facing comparable challenges and risks that will be described later in this report. SCADA systems, DCS and PLCs can operate as autonomous systems as well as in a cooperative fashion. However there are other control components and supportive technology which are also included inside the scope of the ICS term: Remote Terminal Units (RTUs) and Intelligent Electronic Devices (IEDs) are just some examples.

SCADA systems, DCS and PLCs can operate in an autonomous way and are normally oriented to different types of applications. It is important to highlight the differences so that the reader can easily identify the types of ICS systems that can be found, depending on the activity and the sector. For this purpose, we will proceed to specify the definition of the different systems encompassed by the ICS term.

Supervisory Control and Data Acquisition (SCADA) systems are vital components of many nations' critical infrastructures. They control oil and gas pipelines, wastewater collection systems, electrical power grids, railway transportation, and a wide variety of manufacturing operations distributed across a wide geographical area.

SCADA systems provide managers with real-time data on production operations, implement more efficient control paradigms, improve plant and personnel safety, and reduce costs of operation. These benefits are made possible by the use of standard hardware and software in SCADA systems combined with improved communication protocols and increased connectivity to outside networks, including the Internet. However, these benefits are acquired at the price of increased vulnerability to attacks or erroneous actions from a variety of external and internal sources.

Listed below are two typical definitions of a SCADA system:

- SCADA is the technology that enables a user to collect data from one or more remote facilities and/or send limited control instructions to those facilities (2).
- A system operating with coded signals over communication channels so as to provide control of RTU (Remote Terminal Unit) equipment (3).

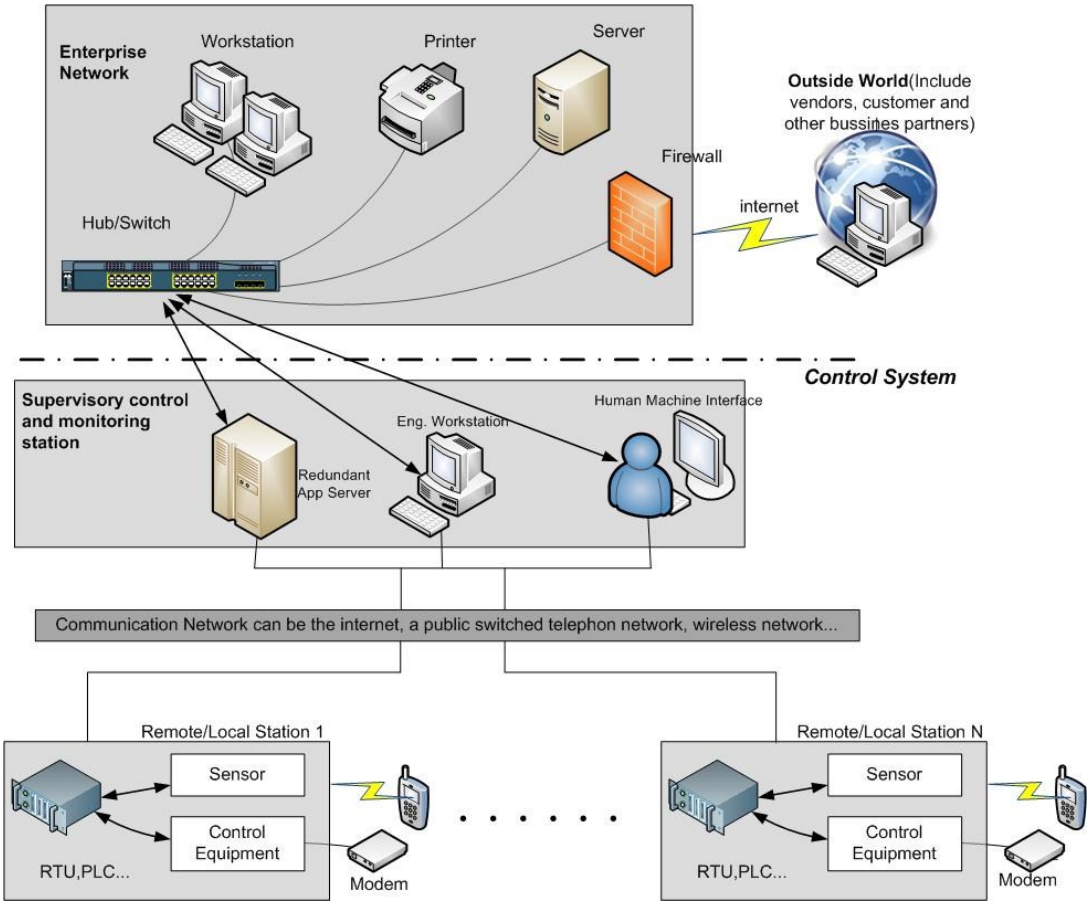

Figure 1: SCADA system general layout (4)

Distributed Control Systems (DCSs) are systems used to control industrial processes such as electric power generation, oil refineries, water and wastewater treatment, and also in chemical, food, and automotive production. Therefore, these systems are typically associated with the control of a process in a plant-centric area. These systems are more related to the concept of automated control and encompass two major operations; the transmission of feedback signals (information flow) back and forth and **the calculation of control actions** (**decision making**) based on this control information. Carrying out these operations requires a set of hardware and instrumentation that serve as the platform for these tasks. DCS are integrated as a control architecture containing a supervisory level of control overseeing

multiple, integrated sub-systems that are responsible for controlling the details of a localized process.

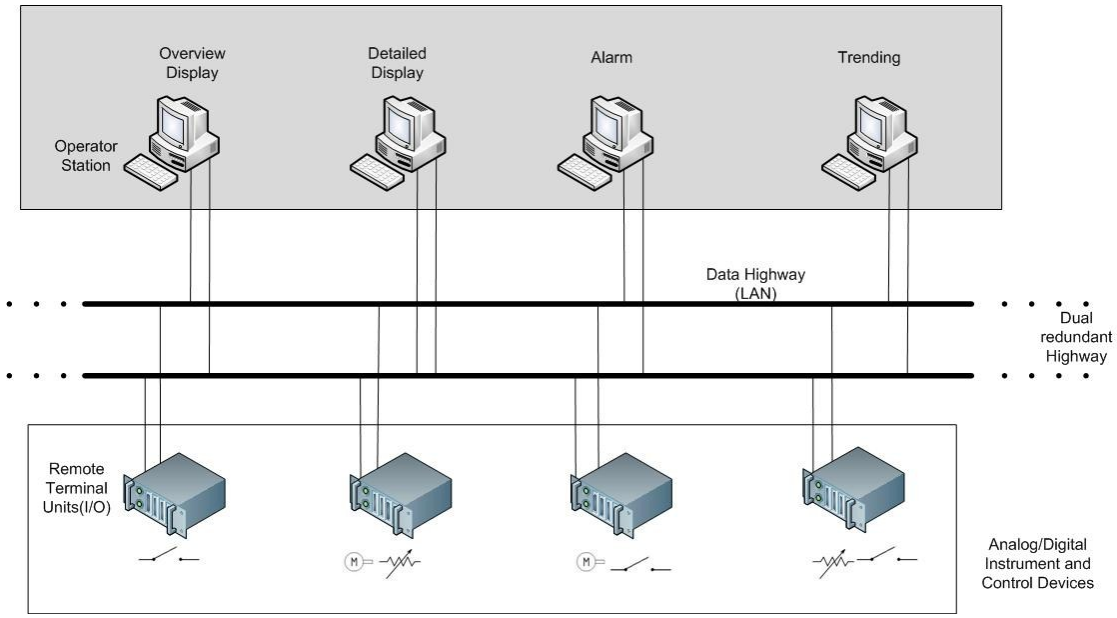

Figure 2: DCS implementation example (5)

PLC-based control systems are control systems where a PLC has a central role. A PLC is a device used to simplify the execution of a machine and the basic idea is to produce the intended output based on the input conditions and the prescribed time limits. In general, a Programmable Logic Controller (PLC) can be considered as a hard real time system since its mechanism depends on the time constraints. PLCs can handle a combination of inputs at a particular instance and produce the required output which can in turn be a combination in itself. The specialty of Programmable Logic Controllers is that they can withstand external physical limits like electrical noise and extreme temperatures where normal computers tend to wear down. This kind of device is used extensively in almost all industrial processes, and nowadays they provide the same rich functionality that was provided by stand alone control systems in the past.

It is important to mention that PLC's can also be control system components used throughout SCADA and DCS systems, at the same level as other control components such as Remote Terminal Units (RTU's) or Intelligent Electronic Devices (IED's).

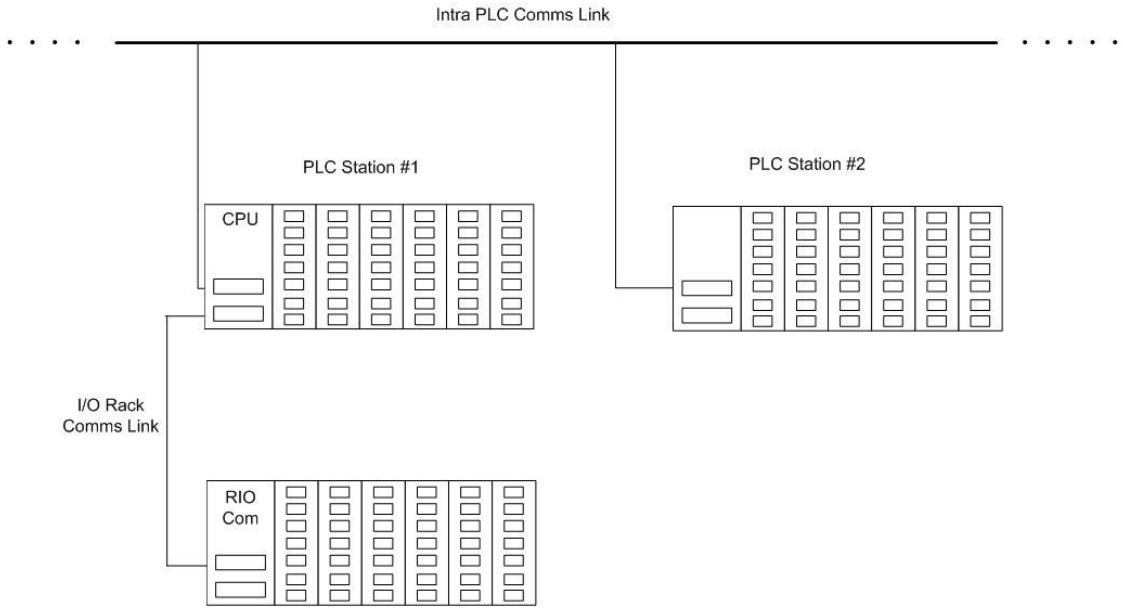

Figure 3: PLC control system implementation example (5)

There is some controversy in distinguishing between DCS and SCADA systems. The following lines present the different approaches existing in several publications:

For example, according to (6) the main difference between DCS and SCADA systems is that the DCS's systems are focused on the **automated control of a process**, **usually within a confined area**, being directly connected to the equipment that it controls. Additionally, it is usually designed on the assumption that this equipment **is always available**. On the other hand, SCADA systems are usually oriented to allow for monitoring and control of a **geographically dispersed group of systems in direct contact with the physical process**, and **they rely on communications that can be intermittent**.

In presentation (7) the following differences between DCS systems and SCADA systems are described:

- The key word in SCADA is "**supervisory**." This indicates that decisions are not directly made by the system. Instead, the system executes control decisions based on control parameters by operators or management. SCADA systems are typically deployed across **large geographical areas** (e.g. electric grid).

- DCS provides **real-time monitoring and control of a given process within a plant**. All major components of the system are usually confined to one or several nearby facilities (e.g. refinery).

Also, the authors of this presentation consider that as technology evolves the terms are getting blurred. In fact they mention that it will be common to hear policy makers and even control professionals referring to "SCADA" systems when they are really talking about a different type of Industrial Control System.

Finally, the document (8) indicates that the "**supervisory**" aspect of a SCADA system as well as the use of **intermittent communications** between the MTU and the RTUs distinguish SCADA systems from other control system like DCS's.

Therefore, we can determine that SCADA systems monitor (supervise) and control geographically dispersed systems or processes, and rely on communication systems that can be intermittent. On the other hand, DCS systems are focused on the automated control of a process within a plant, and are usually designed on the assumption that they are always available. Finally, it is important to highlight that PLCs are widely used as primary controllers in discrete processes to control automobile assembly lines, and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant.

ICS's make use of several control and communication components. It is out of the scope of this document to explain in detail their purpose and we encourage the reader to look at NIST SP 800-82 (1), or any other guidelines addressing the security of ICS, for a high-level but thorough description of most of the main components involved. What follows is a brief list of the components that the reader will find in these documents:

Control components	Communication components
	• Fieldbus Network. • Communications Routers and switches. • Firewall. • Modems • Remote Access Points.

ICS are an essential part of a manufacturing, production, distribution or any other industrial process. Therefore, having a high level overview of the whole process is of key importance in understanding the relevance of the security of ICS for the Business as well as the interdependencies of ICS and other organizational sub processes, such as business planning and logistics or operations management. For this purpose we recommend the reader to read through the reference model provided by ISA99 standards which describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels.

This reference model proposes five logical levels to understand a manufacturing or production activity:

Level 4 – Enterprise Systems: defined as "including the functions involved in the business-related activities needed to manage a manufacturing organization: production scheduling,

operational management and maintenance management for an individual plant or site in an enterprise".

Level 3 – Operations Management: defined as "including the functions involved in managing the work flows to produce the desired end products: dispatching production, detailed production scheduling, reliability assurance, and site wide control optimization".

Level 2 – Supervisory Control: defined as the **"**level that includes the functions involved in monitoring and controlling the physical process: operator human-machine interface, operator alarms and alerts, supervisory control functions, and process history collection".

Level 1 – Local or Basic Control: "This level includes the functions involved in sensing and manipulating the physical process: reading data from sensors, executes algorithms if necessary, and maintains process history. Also included in Level 1 are safety and protection systems that monitor the process and automatically return the process to a safe state if it exceeds safe limits. This category also includes systems that monitor the process and alert an operator of impending unsafe conditions".

Level 0 – Process: "Level 0 is the actual physical process. It includes the sensors and actuators directly connected to the process and process equipment".

ISA99 standards also propose a slightly different view of the reference model for SCADA applications which makes clear the use of long-distance communications networks and remote stations for local control and monitoring. In the following figure it is possible to compare both reference models.

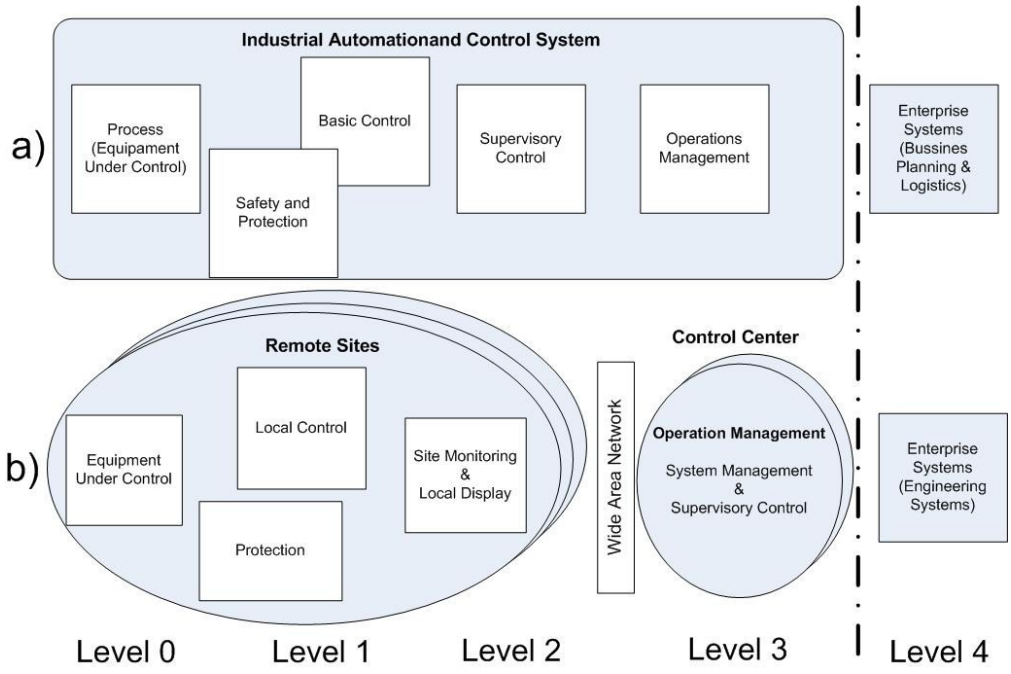

Figure 4: a) Reference Model for ISA99 Standards; b) SCADA reference model (9)

1.1.2 Dependencies of ICS on third-party ICT infrastructures

Distribution processes such as electricity, water, oil and gas distribution, or railway transportation are supervised and controlled by SCADA systems. As already mentioned in this report, SCADA systems span large geographical areas with multiple remote field sites interconnected to one or several central locations which at the same time might also be sharing communication data amongst each other. It is clear that these systems need to make use of WAN technologies, many times being part of the infrastructure of a Telecommunication service provider company. Due to the stringent requirements of SCADA systems regarding communication quality parameters (e.g. delay, jitter, etc.) these communication links represent one of the major channels of propagation of disturbances and adverse events.

Not only SCADA systems make use of third-party ICT communication infrastructures. SCADA systems and DCS systems are often networked together. According to NIST SP 800-82 (1) this is the case for electric power distribution SCADA control centres and electric power generation DCS: “although the electric power generation facility operation is controlled by a DCS, the DCS must communicate with the SCADA system to coordinate production output with transmission and distribution demands”. As a result different ICS are dependent on communication infrastructures and in many cases are not under the control of the same organization. Therefore, when defining a corporate security program that deals with ICS security, it is of great importance to also include these factors in the risk analysis phase.

It is important to note that the dependencies of ICS on the underlying ICT communication infrastructure are just one example of the multiple interdependencies that can arise when addressing the security of Critical Infrastructures. This topic is out of the study of this report and it will not be covered here but we suggest the reader looks at ‘Identifying, understanding, and analyzing Critical Infrastructure Interdependencies’ (10) for more information. Nevertheless the following example illustrating the dependency of the electricity transmission process on the generation process and the deriving interdependencies with other sectors will provide a better understanding on this great problem.

“The lack of monitoring and control capabilities could cause a large generating unit to be taken offline, an event that would lead to loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid. This could result in large area blackouts that could potentially affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for electric power” (1).

1.1.3 The cyber security problem of ICS: Incidents real cases.

ICS and CIs are already facing problems deriving from intentional or unintentional cyber security attacks. This section will provide a brief summary on different experiences that demonstrate that the importance of cyber security on ICS is not only a theoretical exercise but (unfortunately) has practical foundations, with real consequences that may include: “personal injury, threat to a nation’s security, risk to public health and confidence, equipment damage,

inferior product quality, lost production capacity, environmental impact, or violation of legal and regulatory requirements" (11).

According to Rose Tsang (12) there are three broad categories of documented attacks or incidents on ICS operating in critical infrastructures.

- Intentional targeted attacks such as gaining unauthorized access to computers within the network infrastructure, performing a Denial of Service (DoS) attack, or spoofing.
- Unintentional consequences or collateral damage from worms, viruses or control system failures.
- Unintentional consequences caused by internal personnel or mechanisms. This may include the testing of inappropriate software on operational systems or unauthorized system configuration changes.

In the following lines we briefly summarize a real security incident for each of these three categories. For more information on registered cyber security incidents affecting ICS and CIs we recommend the reader to check NIST SP 800-82 (1) and Tsang (12).

Intentional targeted attacks: In June 2010, the malicious software Stuxnet was detected. This piece of malware has the properties of a worm since it exploits several vulnerabilities in order to infect other systems and at the same time it is considered an ICS rootkit since it inadvertently modifies the way in which PLCs behave. This worm was conceived as a cyber weapon for sabotage. It focuses on Siemens specific software and hardware, modifying the logics of Siemens S7 PLC microcontrollers and hiding this from the supervisory software application/operators. Stuxnet is a very advanced piece of software: it exploits several zero-day vulnerabilities, it makes use of valid (stolen) digital certificates, and it masters Siemens WinCC SCADA application. Public press reported that security experts consider that only Governmental services may have the capacity and resources to produce and release such a sophisticated attack tool. There is no official confirmation but security experts think that Stuxnet's target was the Iranian Natanz nuclear facility which is considered by many to be a key part of Iran's nuclear weapons program. Moreover, it was confirmed that since Stuxnet they have suffered numerous faults with no straightforward explanation. The reader will find very detailed information in the Symantec Dossier (13).

Unintentional consequences or collateral damage: In August 2003 the CSX Train Signalling System was affected by the Sobig Virus. This virus rapidly spreads by email and also installs a back door that lets a hacker gain access without detection. According to Tsang (12), "Sobig was blamed for shutting down train signalling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signalling, dispatching, and other systems. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long distance trains were also delayed between four and six hours".

Unintentional consequences caused by internal personnel or mechanisms: In March 2008 the Edwin I nuclear power plant in Georgia (USA), was forced to make an emergency shutdown for 48 h due to a software update. This software update was applied to the computer system in charge of monitoring chemical and diagnosis data of one of the plant's primary control systems. After applying the update, the computer was rebooted and this lead to a lack of monitoring information. Safety systems misinterpreted this and signalled that the water level in the cooling systems for the nuclear fuel rods had dropped, which caused an automatic shutdown. There was no danger to the public, but the power company lost millions of dollars in revenue and had to incur the substantial expense of getting the plant back on-line.

1.1.4 Differences between IT Systems and ICS Systems

Most ICS that are currently behind the control and supervision of many critical processes like water treatment, electricity generation and distribution, railway transportation, gas distribution, etc. were developed years ago with performance, reliability and safety requirements but with no consideration of cyber security at all. Security was synonymous for safety (i.e. protecting lives and business) and physical security (i.e. controlling access to critical facilities and systems, e.g. CCTV, guards, etc.). During the 1980's and 1990's microprocessor-based systems, new networking technologies and applications appeared. Their mass adoption thanks to the Internet, the personal computer and mobile telephones during the 1990's and the first years of 2000's brought a drastic change to the way in which companies worked, people interact with computer systems, etc. This was a change of mentality that started to influence the way people interacted with ICS and even their design. The mass use of the Internet, and associated technology (i.e. IP protocol, Ethernet), of OS such as Windows, etc. made them be introduced into ICS designs in late 1990's since they allowed the reduction of costs, improvement of efficiency and productivity. By that date, computer attacks and viruses had already started to be a reality. Nowadays, malicious software of all classes and directed attacks are common. Some experts even believe we are in the beginning of an era where wars could happen in cyberspace: the cyber war era. However, while in the corporate IT domain (e.g. desktop computers, corporate servers, etc), many technical and organizational solutions are available, special precautions must be taken when introducing these solutions to the ICS environments.

ICS have characteristics that make them very different from traditional information processing systems. Probably there are two main differences driving most of the others: ICS systems have different priorities and imply risks with a much broader scope and impact. As we already mentioned, ICS were designed to meet tight performance and reliability requirements which are not typical in a conventional IT environment. At the same time, many of these ICS are behind the supervision and control of critical processes (e.g. nuclear power generation). This means that the risks managed here include impact on the health and safety of human lives, serious damage to the environment, production losses, impact to a nation's economy, etc.

What follows is an extract of some of the typical differences between IT systems and ICS. A more detailed version on this can be found at NIST SP 800-82 (1).

Performance requirements: IT systems are normally non-real-time systems, where high data throughput is demanded (and available) and where high delay and jitter may be acceptable in data being communicated as long as data is consistent. On the other hand, ICS sometimes need to operate in real-time and therefore delay/jitter is not acceptable. Throughput is not so important, and as a result the underlying communication infrastructure is sometimes limited on this aspect.

Availability requirements: Outages of ICS are not acceptable in most cases and therefore components redundancy is common practice. Moreover, many control systems are not easily stopped or started without affecting production. This means that common IT system practices such as rebooting are not acceptable.

Risk management requirements: In traditional IT systems information confidentiality and integrity are the main concern. For ICS systems human safety, environmental impacts and the process itself (loss of equipment/production) are the main concerns. For this reason, from the three fundamental characteristics of computer security, availability and integrity are the priorities for ICS.

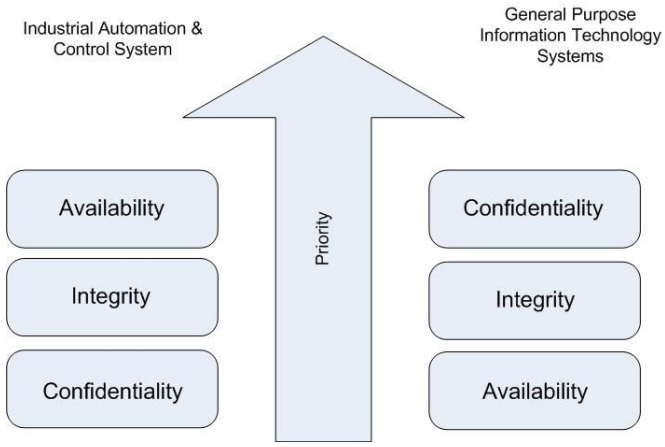

Figure 5: Comparison of risk management objectives (11)

Time-Critical machine-human interaction: ICS system response to human interaction is very critical. Requiring password authentication should not hamper or interfere with emergency actions.

System operation: Legacy systems are vulnerable to resource unavailability and timing disruptions. Control networks are often more complex and their operation require a different level of expertise (e.g. are typically managed by control engineers). Software and hardware applications are more difficult to upgrade and many systems do not have desirable security features (e.g. encryption, error logging, password protection, etc.) and it may be difficult to include them since they are resource-constrained systems.

Change management: software updates on ICS systems need to be thoroughly tested by the vendor and end user before being implemented and ICS outages often must be planned and scheduled days/weeks in advance. Moreover, many ICS systems utilize older versions of operating systems that are no longer supported.

Cyber Security Assessments are a good example to show how these differences can influence the way in which security procedures, techniques and technologies should be used when dealing with ICS. As mentioned in 'Cyber security assessments of industrial control systems' (14) "Cyber security testing activities may have adverse effects on any target system, but especially on an ICS. Cyber security tests often employ port and vulnerability scanners that make rapid requests to an Internet Protocol (IP) address, often with invalid data. These scans alone often cause a victim process or entire machine to fail. When the target is an active ICS server, this failure could have serious and drastic consequences. All cyber security testing should be well planned and communicated with the equipment owners and operators so that potential faults are resolved or mitigated."

This is just one example of how a security procedure should be different when dealing with an ICS system instead of a regular IT system. However, there are many other examples where technical, operational and management controls should also be different from their classic IT security counterparts. NIST 800-53 rev. 3 guideline includes a comprehensive set of security controls that need compensatory alternatives and supplemental guidance. Some examples of these controls that need some tailoring are: account management, separation of duties, least privilege principle, concurrent session control, remote access, auditable events, configuration change control, contingency plan testing and exercises, maintenance tools, remote maintenance, malicious code protection, security functionality verification, etc.

1.1.5 Vulnerabilities and Risk factors

ICS were not conceived with cyber security in mind. As a result, these systems lack many cyber security capabilities, do make use of inappropriate network architectures, and applications and hardware are developed without taking into account secure development good practices. Moreover, since many times communications infrastructures are the responsibility of control engineers they are maintained and deployed with the sole goal of allowing data and commands to be exchanged; cyber security is left out.

Paradoxically, CI operators have been, in most cases, well aware of the importance of digital security. Actually, they have evolved in parallel with the evolution of cyber security in many ways, but not from a holistic point of view. For instance, it is quite normal to find multi-year security plans which include aspects like risk analysis, criteria for establishing security of information assets, security policies (e.g. network access policy), procedures for security incident handling, etc. Unfortunately, in many cases these plans have excluded other cyber security factors characteristic of control systems, like control applications security functionalities, control networks and buses protection, field control devices shortcomings, digital access from SCADA solutions providers, or security threats deriving from control system

integrators. Most of the time, physical security has been well addressed in many cases and safety systems are a main part of critical infrastructure operation.

During recent years, several risk factors have contributed to increase the risk to control systems and in turn to many CI operators. These can be summarized as follows:

Weak communication protocols: ICS communication protocols were never designed with security in mind. Many of these protocols were initially conceived as serial protocols with no built in message authentication, which means that devices will accept connections from any device trying to communicate with them. None of them used encryption or message integrity mechanisms, which exposes the communications to eavesdropping and session hijacking and manipulation. Even though these vulnerabilities have been around for years, new factors have augmented the real risk. For instance, "ICS vendors have begun to open up their proprietary protocols and publish their protocol specifications to enable third-party manufacturers to build compatible accessories" (1). Organizations are also transitioning from proprietary systems to common networking protocols such as TCP/IP (i.e. Modbus/TCP, IEC 104, etc.) or new standard open protocols such as OPC to reduce costs and improve performance (1). The introduction of commercial off the shelf (COTS) protocols is making these systems susceptible to the same software attacks and hacking tools already present against business and desktop devices and networks (11). To make things worse, "all associated communication stacks were never tested outside of normal, SCADA-specific data. Testing shows that these devices are very prone to simple denial of service attacks and buffer overflows" (15).

COTS operating systems and applications and general-purpose hardware: Not only communication protocols have been modified or replaced by standard open ones. For similar reasons of costs and performance, operating systems and applications in ICS have also transitioned from closed ad-hoc developments to *de facto* standard operating systems (e.g. MS Windows or Unix-like) and applications (e.g. MS SQL Server, MS Excel, etc.). This in turn makes "these systems susceptible to the same software attacks as are present in business and desktop devices" (11). Moreover, most of these systems are not patched (this would violate the vendor's service contract (15) or hardened from a security perspective. At the same time, general-purpose hardware is being used in RTU, PLCs, Industrial PCs, and other control components. Consequently, Security through obscurity could not be a basic security principle any longer.

Connectivity of ICS: ICS systems and other corporate IT systems are nowadays interconnected. Since it is already quite common to have IP-based ICS communications, interconnectivity capabilities have been drastically improved. The result is that many services operations have been simplified and associated costs have been reduced. Now, it is quite normal to perform remote administration of control systems and associated network devices. Likewise, "ICS engineers and support personnel are provided access to monitor and control the ICS from points outside the control network" (1). Moreover, "many organizations have also added connections between corporate networks and ICS networks to allow the organization's decision makers to obtain access to critical data about the status of their operational systems and to send instructions for the manufacture or distribution of product"

(1). As a result, the once isolated systems are now being connected to larger open networks. Moreover, "the use of joint ventures, alliance partners, and outsourced services in the industrial sector has led to a more complex situation with respect to the number of organizations and groups contributing to security of the industrial automation and control system" (11). Now vendors, maintenance contractors, other CI operators, etc. have wide access to critical ICS elements and are more exposed to IT threats than ever before.

Lack of appropriate ICS networks segmentation: After understanding the consequences of the previous point it is important to highlight that there is a lack of an overall ICS network segmentation strategy within most CI operators. "When firewalls are used, they are typically not well configured and only provide protection between the corporate network and the control centre. Once the perimeter of the PCS network is breached, then the network is wide open" (15).

Inappropriate and insecure connections: Many times ICS vendors deliver systems with dial-up modems so that they can provide maintenance services to CI infrastructure technicians. Sometimes organizations use similar and other access links for remote diagnostics, maintenance, and monitoring. Indeed, it is quite common that all such access links are not well protected with strong authentication and/or encryption mechanisms. Something similar happens with the interconnection between corporate and ICS networks. The reason for this is that "many control engineers have little if any training in security and often IT security personnel are not involved in ICS security design. As a result, access controls designed to protect control systems from unauthorized access through corporate networks are usually minimal" (1). As a result, communications are exposed to eavesdropping and session hijacking (15) which worsens the connectivity risk panorama described above.

Applicability of standard ICT security technology and procedures: Standard security procedures and technologies which are effective inside business and desktop devices and networks do have their own specific problems when applied to ICS. Initially, many vendors did not support anti-virus applications since they "may require adopting special practices including compatibility checks, change management issues, and performance impact metrics. These special practices should be utilized whenever new signatures or new versions of antivirus software are installed" (1). Many DCS or SCADA systems are including specific ad-hoc developments for each customer, making this testing and impact assessment a very heavy process. Something similar occurs with patching. "Patches should be adequately tested (e.g., off-line on a comparable ICS) to determine the acceptability of side effects. It is not uncommon for patches to have an adverse effect on other software. A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective" (1). Moreover, most of the distribution SCADA systems are in fact turn-key projects. This means again, that the responsibility for upgrading and patching systems is confided to the vendor by the CI operator. IT firewalls as well as IDS are also a good example of how well-proven technologies in the office environment cannot be directly applied to ICS. "Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning

to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP" (1). Likewise, IT firewalls are generally unaware of ICS protocols and therefore, packet filtering of ICS protocol messages is uncommon. IT firewalls operate in an inline fashion; therefore it is reasonable to argue that they might have an impact on real-time protocols, introducing unacceptable latency into time-critical systems (16) – the same would apply to IPS –.

Widespread availability of technical information about control systems: It is quite easy to find publicly available information (e.g. www) on ICS applications and systems design, characteristics, communications, etc. This kind of information normally helps a potential end user to decide among several choices: the larger set of characteristics compared to your competitor, the more attractive your product is for a potential buyer. Moreover, the fact that another peer company has already chosen that solution also helps with this. This kind of information is also many times available in the vendor's news section in their website providing an attacker with a good way to gather initial knowledge on a potential target. At the same time, ICS vendors sell toolkits and also provide Application Programming Interfaces (APIs) for free. This helps integrators or even end users to develop their own ad-hoc application enhancements while potential attackers can also develop targeted attack toolsets. At the same time, contractors, employees, and probably other people in the same sector are aware of the operation of the control systems and processes of a CI. These people can be a valuable source of information for criminal groups and other threats. Moreover, since security on CIs became a main research topic, an increasing number of technical papers, research results, laboratory tests, etc. are available. More and more attention is focused on ICS and as a result more and more people are becoming specialists on their particular security aspects. This increases the number of potential attackers. Finally, Stuxnet has provided malware developers an excellent reference model for their new "creations" (see section 1.2.1). The reader is encouraged to read more on this topic at NIST SP 800-82 (1).

Lack of a global security policy in CI operators: "Driven by increasing cyber security risks, many organizations have taken a proactive approach towards addressing the security risks of their information technology systems and networks." (11). For instance, it is quite normal to find multi-year security plans which include aspects like risk analysis, criteria for establishing security of information assets, security policies (e.g. network access policy), technical security procedures, etc. However, these security plans and even the whole corporate security governance have not included ICS in their scope. "Historically organizations providing and supporting business information systems and industrial automation and control systems operated in two mutually exclusive areas. The expertise and requirements of each organization were not understood or appreciated by the other […]. Security practices were in opposition to normal production practices which are designed to maximize safety and continuity of production" (11). As stated in NIST SP 800-82 (1) "ICS security plans and programmes should be consistent with and integrated with existing IT security experience, programmes, and practices, but must be tailored to the specific requirements and characteristics of ICS technologies and environments. Organizations should review and update their ICS security plans and programmes regularly to reflect changes in technologies,

operations, standards, and regulations, as well as the security needs of specific facilities". For instance, third parties connecting to the ICS via dialup access or the Internet bring in new threats from outside of the organisation. Therefore, third parties supporting ICS maintenance, operation and development must be engaged as part of the process control security programme (17). To be able to accomplish all this, CI operators should establish a security governance committee with full responsibility for process control security risk and impacts (18).

An evolution of the threat[1] landscape: Hacking tools are commonly available on the Internet and have started to include ICS specific add-ons. During recent years malware has proliferated on business and personal computers. Many ICS incidents have evolved from unintentional incidents or amateur script-kiddies to directed attacks from disgruntled employees, organized crime, terrorists, and even foreign governments – as can be inferred from 1.1.3–. Probably there is one clear example that draws together all these previous statements; this is Stuxnet. Being considered one of the most advanced pieces of malware ever created, it was created by a very well prepared, funded and coordinated organisation. It was a directed weapon (probably the first one ever), presumably against the Uranium centrifuges in Iran and contained specific pieces of code targeting specific ICS applications and devices. It is now considered as a reference model, a step by step guideline, for a future generation of malware against ICS.

1.1.6 Threats

Threats can be defined as "possible actions that can be taken against a system" (11). However it is quite usual to find partial descriptions of threats affecting ICS based on specific characteristics, such as the threat agent behind it, the degree of intentionality, the way in which the threat agent is organised, etc. In this section we will compile an overview of the current threats that could affect ICS from a set of various documents where this topic is addressed.

Depending if threats are accidental or deliberate it the following classification can be made:

- **Accidental/Inadvertent threats:** Security threats to assets can result from inadvertent events. In fact, often more actual damage can result from safety breakdowns, equipment failures, carelessness, and natural disasters than from deliberate attacks. CIs are accustomed to worrying about equipment failures and safety-related carelessness. However, someone unfamiliar with proper procedure and policy still causes an accidental risk. At the same time, it is also likely that an organization does not know all the risks and may uncover them by accident as it operates complex industrial automation and control systems. Fortunately what is changing is the

[1] *See a more detailed analysis in chapter 1.1.6*

importance of protecting Information which is becoming an increasingly important aspect of safe, reliable, and efficient process operations.

- **Deliberate threats:** it is important to highlight that the reactions to successful deliberate attacks can have tremendous legal, social, and financial consequences that could far exceed the physical damage.

Accidental/inadvertent threats may be further divided into:

- **Safety failures:** "Safety has always been a primary concern for CIs. [...] Meticulous procedures have been developed and refined over and over again to improve safety. Although these procedures are the most important component of a safety programme, monitoring of the status of key equipment and the logging/alarming of compliance to the safety procedures through electronic means can enhance safety to a significant degree, and can benefit other purposes as well" (19). For instance, electronic monitoring of safety measures inside electric power substations can also help to prevent some deliberate attacks, such as vandalism and theft.

- **Equipment failures:** These are the most common and expected threats to the reliable operation of the power system. Significant work has been undertaken over the years: redundant components and networks, equipment status monitoring, etc.

- **Carelessness:** Often carelessness is due to complacency ("no one has ever harmed any equipment in a substation yet") or laziness ("why bother to lock this door for the few moments I am going into the other area") or irritation ("these security measures are impacting my ability to do my job"). Examples of carelessness threats include: permitting tailgating into a substation; not locking doors; inadvertently allowing unauthorized personnel to access passwords, keys, and other security safeguards; applying updates, corrections and other changes to operating systems and control applications without a previous test in a controlled environment; etc.

- **Natural disasters:** storms, hurricanes, and earthquakes, can lead to widespread power system failures, safety breaches, and opportunities for theft, vandalism, and terrorism.

Based on how the threat agents are related to the target company/system, we have:

- **Insiders:** "An insider is a trusted person, employee, contractor, or supplier who has information that is not generally known to the public. An insider can present a threat even if there is no intent to do harm. For example, the threat may arise as a result of an insider bypassing security controls to get the job done" (11).

- **Outsider:** "An outsider is a person or group not trusted with inside access, which may or may not be known to the targeted organization. Outsiders may or may not have been insiders at one time" (11).

Depending on how the threat agents organise themselves and the resources and support they have, we could consider the following threats:

- **Lone/small groups:** this type of threat agent would include disgruntled employees, highly skilled hackers, script-kiddies, etc. Script kiddies are often challenged by the notion of gaining unauthorized access and are sometimes open to using untested pieces of code without knowing their consequences. On the other hand, highly skilled hackers have the ability to find unique vulnerabilities in existing software and to create working exploit code. It is important to note that most highly skilled coders/hackers are not malicious. The disgruntled insider is a principal source of computer crime and sabotage. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data.

- **Rival companies:** Rival companies could be interested in causing damage to the corporate image of a rival company or in Industrial espionage to acquire intellectual property and know-how by clandestine methods.

- **Criminal groups:** Criminal groups seek to attack ICS for monetary gain by means of extortion. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International organized crime organizations are able to conduct industrial espionage and large-scale damage and to hire or develop attacker talent.

- **Terrorists:** "Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence" (1). "A group with a long enough time horizon and enough financial backing may develop capabilities on par with nation-states" (12).

- **Nation-states/foreign intelligence services:** Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrines, programmes, and capabilities. Some of these capabilities include: gaining access to the source code for proprietary software and thus identify vulnerabilities unknown to the general public; persuading vendors or their employees to intentionally insert "backdoors" or other zero-day vulnerabilities into their software code or hardware

devices; obtaining (usually buying) the system of interest in order to understand its operational strengths and weaknesses as well as its vulnerabilities.

Based on the attacking techniques in use we can have:

- **Physical destruction:** these threats are aimed at destroying or incapacitating physical components (i.e., hardware, software storage devices, connections, sensors, and controllers) that are part of the industrial automation and control system. These attacks can come in the form of a physical attack on the components themselves or through a cyber attack that causes the system to perform actions that lead to physical damage, destruction, or incapacitation of the component.
- **Theft:** the attackers take something (equipment, data, or knowledge) that they are not authorized to take. Generally, the motive is financial gain as the motive, although other motives are possible as well.
- **Malware:** malicious software can be described as a piece of software that allows an attacker to gather information about systems or users, destroy system data, install a backdoor for further intrusion into the system, falsify system data and reports or cause a DoS to system operations and to the interaction with maintenance personnel. Malware can take the form of viruses, worms, automated exploits, trojans, botnets, spyware, etc.
- **Communication threats:** this category includes threats where the intention is to disrupt, alter or spy on communications of an industrial automation and control system.
- **Escalation of privileges:** by means of exploiting a vulnerable system an attacker is able to increase their current privileges on that system. As a result the attacker can take actions that would otherwise be prevented.
- **Data Base injection:** injection attacks are used to steal information from a database from which the data would not normally be available and/or to gain access to an organization's host computers through the computer that is hosting the database.
- **Denial of Service:** this kind of threat aims to affect the availability of a network, operating system, application (e.g. control server, data historian, etc.) resources or any other computational resources like memory, processor or file system.

- **Replay:** data and control packets can be captured from control system communications paths and replayed later to provide access to secured systems or to falsify data in the industrial automation and control system.
- **Spoofing/impersonation:** this type of threat includes a variety of ways in which hardware and software can be fooled: IP spoofing, MAC spoofing, DNS poisoning, e-mail header spoofing, etc.
- **Social engineering:** the victims of social engineering are tricked into releasing information that they do not realize will be used to attack the ICS. Several ways of achieving this exist, such as a telephone call where the caller impersonates someone the victim trusts or by means of a phishing attack.
- **Phishing:** phishing techniques involve stealing identities or information that might be helpful for a more sophisticated attack. A fake website or maliciously crafted emails are some of the techniques that can be used. It is a social engineering technique.
- **Spam:** spamming within the ICS context allows attackers to distribute malware by distributing unsolicited e-mails with appealing false information.

Depending on the impact of the threat we can classify them into:

- **Passive:** These threats refer to passive information gathering. The type of information that can be compiled with no active work include shift changes timetable, equipment operation, supply logistics and patrol schedules. Passive information gathering may be difficult to detect: being observant of unusually curious persons, photographers, and personnel often outside their areas of responsibility can help recognize passive information gathering.
- **Active:** Active threats include deliberate or unintentional acts that actively interact with the systems and people involved. This includes the use of malware, vandalism, theft, DoS, social engineering, etc.

1.2 Emerging issues

In this chapter we will deal with three relevant topics that can be considered emerging issues on the security domain of Industrial Control Systems, explaining for each one the scenario, challenges, pros and cons, etc.

Due to the critically of ICS, it is important to talk about targeted attacks affecting ICS. In particular we will refer to two well known recent examples that affected several energy companies: Stuxnet and Night Dragon. Targeted cyber attacks have changed the security landscape of ICS and CI's. The second topic that will be addressed is on what the role of Cloud Computing inside the Industrial Control environment could be. The main advantages and disadvantages of this technology with regard to the particular characteristics of ICS are presented. And finally, we will introduce the Smart Grid concept and how it can be related to SCADA systems in power distribution operators. We will briefly present the risks being introduced and how the work done for ICS security can avoid having to reinvent the wheel again for protecting the future power grid.

1.2.1 Targeted attacks on ICS

Targeted attacks are currently a hot topic among security experts. These attacks are the reason why the security community starts to talk about the concept of cyber war, cyber terrorism, etc. Cyber war and cyber terrorism are no longer just potential threats against critical infrastructures, since real world examples can already be found in the public domain. Furthermore, these threats are already targeting industrial control systems, as a way to do big damage to their targets. Due to the criticality of the environment in which many ICS operate, these attacks can pose big risks to society, both in terms of economic losses, human lives, and even the future of a county. This section focuses on two of the best known targeted attacks against ICS: Stuxnet and Night Dragon.

Stuxnet, was designed to target Siemens' industrial control systems (specifically, Programmable Logic Controllers and engineering software). It changed the logics of a Siemens S7 series PLC to alter the frequency converter drives of the controller. The worm was the first to simultaneously exploit four zero-day vulnerabilities for propagation, infection and hiding purposes. It also used stolen digital certificates to sign and legitimize its malicious content and avoid Operating System malware protection mechanisms. It was demonstrated that the authors of Stuxnet also had considerable knowledge of their targets, their control systems as well as the process being controlled and monitored by these control systems. Stuxnet did not collect personal information, such as online banking data or user account credentials, nor did it infect systems to convert them into zombie stations as part of a botnet. It has been speculated that its main motivation could have been sabotage, probably of the Iranian nuclear programme. Due to this and because Stuxnet was the first piece of malware designed to attack industrial control systems, a big worldwide stir took place, lasting some months. Currently, US cyber security experts are warning that the Stuxnet virus can become more threatening. The U.S. Department of Homeland Security has devoted the last year to study the sophisticated virus and although companies have developed computer security protections against Stuxnet, the Department fears that hackers can create hybrid variants of the virus which may be able to avoid detection and attack other installations. Furthermore, Stuxnet is now considered as a step by step recipe for the development of new malicious software targeting control systems by less prepared and experienced malware programmers (20).

Night Dragon was the name given to a number of targeted attacks. Their main objective was to compromise the industrial control system of several energy companies in the United States. According to the report by the company McAfee (21), attacks are believed to have their origin in China. These attacks relied on a combination of several techniques, tools and vulnerabilities (i.e. spear-phishing, social engineering, Windows bugs and remote administration tools –RATs–). Although the attacks were not very sophisticated and did not exploit any zero-day vulnerability, the information obtained by attackers was very valuable for competitors. That information included financial documents, related to oil and gas field exploration and big negotiations, as well as operational details of production supervisory control and data acquisition systems.

Attacks were conducted on a step-by-step basis. They first looked to compromise the perimeter security through SQL injection attacks on extranet web servers, targeted phishing attacks aimed at mobile workers' laptops and compromising corporate VPN accounts. Once they got over the perimeter defences, attackers tried to compromise local administrator accounts and Active Directory administrator accounts in order to monitor network and software applications.

As can be seen, these targeted attacks are already making use of a large variety of techniques designed to compromise the integrity, confidentiality and availability of industrial control systems. These techniques range from sophisticated rootkits[2] hiding running processes on the SCADA equipment, or simply well-know attacks that create backdoors into control centres' computers. All of them share a common characteristic; they have all achieved their target objective.

There is a lot that needs to be done in ICS security. The main stakeholders must be aware that there is work to do, adapting their systems to the new laws and standards.

1.2.2 Cloud Computing and ICS

Cloud computing is an IT technology solution and paradigm that provides computation, software, data access, and storage services that do not require the end-user to know about the physical location and configuration of the systems that deliver the services. This technology fills a need in the IT world, a way to increase capacity or to add capabilities on the fly without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet or intranets, extends IT's existing capabilities. The principal benefits of cloud computing are increases in storage, flexibility, availability and mobility.

Experts are beginning to debate if cloud computing technology could be applied to the ICS domain, arguing that the fundamental reason for its adoption, as with virtualization, will be availability. But the adoption of cloud computing in the Industrial control systems will not be

[2] *A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.*

easy. A number of problems exist which must be solved before this can happen. For example, many industrial control systems existing today are comprised of machines that are still running obsolete operating systems such as Windows 95. They make use of many software applications which are not compatible with newer versions such as Windows 7 or Vista. As a result, some of the enterprise wide benefits of implementing cloud computing may not be feasible in a manufacturing environment. Another issue to take into account is that applications used in cloud computing may also not be useful in industry. While 'on demand' accounting software and office functionality might be ideal for the back office, in a manufacturing environment, much of the software used in ICS is highly specific and specialized. On the contrary, thin client computing is an increasingly popular technology in manufacturing, particularly where provision of a GUI is the principle function of the machine. In this case, where information processing is being performed at server, rather than client level, there is no real need for that server to be local; it can just as easily be located in the cloud.

Apart from the applicability of this technology or the business case behind it, there are several security aspects that should be considered. According to Gartner (22), Cloud computing entails seven unique security risks that should be considered first. These are the following:

- **Privileged user access:** if cloud computing is implemented as a method for providing outsourced services, it is of major importance to understand that these services bypass the physical, logical and personnel controls defined in the corporate security policy. It would be of major importance to ask providers to supervise privileged administrators.

- **Regulatory compliance:** Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider.

- **Data location:** when you use the cloud you probably won't know exactly where your data is hosted (i.e. in which country) and therefore what jurisdictions are they affected by.

- **Data segregation:** the cloud is normally a shared environment, therefore encryption schemes are normally applied to guarantee segregation of data among different customers. However, encryption accidents can make data totally unusable giving rise to availability problems.

- **Recovery:** In case of a disaster it would be important to get guarantees from the provider that redundancy schemes are implemented and that backup procedures are defined.

- **Investigative support:** cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres.

- **Long-term viability:** the cloud computing provider might go broke or get acquired by a larger company which might affect the services being offered.

As a conclusion, cloud computing could be an interesting technology to consider but any move in such a direction in a manufacturing environment should be planned and considered carefully.

1.2.3 Smart Grid and ICS security

Smart grid is a type of electrical grid which attempts to predict and intelligently respond to the behaviour and actions of all electric power users connected to it, in order to efficiently deliver reliable, economic, and sustainable electricity services. The transition to a sustainable energy system will be a huge task for society. It will mean addressing significant new challenges, including large-scale use of renewable energy sources and the electrification of the transport sector.

Some experts consider the smart grid to be comprised of only the smart meters and their associated communication infrastructures and head-end systems. However, many others also include as part of the smart grid, the whole set of automation, and supervisory control devices and applications which are essential for the distribution of electricity. Even if the smart grid is only considered to be the smart metering infrastructure, it is quite probable that most of it would share some systems and locations with substation automation equipment and other head-end control systems. From the point of view of security, the smart grid connects the customer's home to the ICT infrastructure of the Distribution System Operator (DSO). This means that new entry points and new threats have to be considered. Moreover, if the smart metering systems and head-end systems do share a common underlying infrastructure, they will be likewise threatened by new risks. It is therefore important that operators assess the consequences that this new smart grid will have from a security point of view on their older and not so well protected ICT systems, particularly ICS.

Smart Grid is still a relatively new technology, so it still has time to avoid taking on the same security problems that ICS are now facing, since they were designed without taking into consideration security as a basic requirement. It is necessary that the security concept is introduced in the design phase of the new Smart Grid systems, avoiding problems that are very expensive and almost impossible to solve in the future. A principle of efficiency is not to try to reinvent the wheel, adopting security solutions that have been proved effective in similar environments, such as in this case the ICS sector. An example of this might be the use of encrypted communications based on digital certificates, which could be applied to secure the existing connections between Smart Grid devices. A more general approach could be to apply good practices guidelines/standards already published for ICS environments to ensure

the appropriate level of security. All this coupled with the ongoing and new efforts of organizations, manufacturers and utilities to publish standards can set a good starting point for achieving a secure and efficient smart grid.

1.3 Challenges to ICS protection

In this chapter we present a list of challenges related to the protection of ICS. These challenges can affect security vendors, ICS manufacturers, ICS operators, research bodies, public bodies, or even standardization organizations. The topics included range from the technical domain to the political one, including also organizational, awareness, dissemination, and economical domains. They are not listed in any order of priority and they may overlap one to another in certain aspects.

1. ICS end users need to build **security programmes** that integrate all aspects of cyber security, including desktop and business computing systems together with industrial automation and control systems. Many organizations have fairly detailed and complete cyber security programs for their business computer systems, but cyber security management practices are not as fully developed for ICS (11).

2. In many end user organizations there is a **lack of collaboration and coordination** between departments that should work together in the face of security challenges. For instance, for control systems practical administration of the systems may be handled by process engineers, who have no knowledge of logical security in control systems. **Allocation of roles and responsibilities** for the administrative information systems and control systems should be co-ordinated. For instance, there should be clarification of which systems are administrated by the organization's central IT support and which systems are administrated locally out in production (23).

3. The **IT and manufacturing or production organizations** should work collaboratively and bring their knowledge and skills together to **tackle security issues**. This is important since, in some cases, the security practices are in opposition to normal production practices designed to maximize safety and continuity of production. The traditional IT security vision considers security dimensions in the following order of importance: confidentiality, integrity and availability while, for control engineers, availability first and also integrity are the two key factors to consider, since they are directly related to safety aspects. Furthermore, organizations providing and supporting business information systems and industrial automation and control systems have historically operated in two mutually exclusive areas (11).

4. Vendors might need to consider **differentiating their ICS products based on the security functionalities they include**. Vendors may offer a product with few options

targeting a very specific SCADA system at a corresponding low price or may offer products with extensive security options and flexibilities at a higher price. It is interesting to highlight that an end user, after a risk assessment, could decide that the compromise of a particular ICS facility is of minimal operational or economic consequence. Therefore it would make little economic sense to include high-end security devices (e.g. RTUs) in it. Moreover, there can be occasions where the end user rejects including security capabilities (taking on the risk themselves) since there could be an unaffordable degradation in performance (e.g. cryptography may add unacceptable latency to a very time critical SCADA application) (24) and (25).

5. Standardization groups consider that the **Industry should adopt a single cryptographic system** rather than a diverse mix of systems that have not undergone public expert review. However, this should be flexible to permit the introduction of new algorithms (ciphers) and new technologies once they are validated as cryptographically secure. "Security through obscurity" was the ruling principle when ICS systems were isolated and they did not communicate with other corporate system. At this moment, ICS are very complex systems, with many and heterogeneous communications so this principal should no longer be applied [3] (24) and (25).

6. The information infrastructure in ICS is not typically treated as a coherent infrastructure, but is viewed as a collection of individual communication channels, separate databases, multiple systems, and different protocols. Often SCADA systems perform some minimal communications monitoring, such as whether communications are available to their remote terminal units (RTUs), and then they flag data as "unavailable" if communications are lost. However, it is up to the maintenance personnel to track down what the problem is, what equipment is affected, where the equipment is located, and what should be done to fix the problem. In the mean time, the power system is not being adequately monitored, and some control actions may be impossible. There is a need for **IT security monitoring technologies** that allow maintenance personnel to quickly solve the problem or even to trigger automated actions that can minimize the impact (26).

7. ICS end users, manufacturers, certifying companies, etc. will need to be able to **verify and validate the security configuration aspects, capabilities and interoperability of ICS** including security features. A reference standard has to be used for this purpose

[3] *As the reader will notice, during the analysis phase of the interviews and questionnaires, it can be concluded that this is still a controversial topic.*

and facilities should be available and configured and appropriate detailed test procedures should be defined for this purpose (24) and (25).

8. **Education and awareness** are key aspects for creating a security culture inside the organization. This in turn is critical for successfully addressing ICS cyber security risks. Solutions, procedures and security management aspects for ICS can differ widely from their counterparts in classic ICT systems. There are several options to be considered by end users:

    a) Training the ICS personnel to understand the current information technology and cyber security issues;

    b) Training IT personnel to understand ICS technologies, along with the Process Safety Management processes and methods;

    c) Developing practices that unite the skill sets of all the organizations to deal with cyber security collaboratively (11) and (23).

9. Many CIs that operate ICS are privately owned. A private company's primary goal is profit and therefore it is essential to make them see that **securing ICS is a key aspect** that they should consider, also **from an economical point of view**. Sometimes there are many other investments that might be seen by companies as more urgent since their monetary benefits are more tangible or visible in the short term.

10. ICS end users should establish a process for **surveying industrial control systems and for conducting risk analysis**. It is important to understand what the information flows and system dependencies are, based on the consequences that a fault or disrupted function could have, both for the physical process being controlled and the organization itself (23).

11. Many control systems environments are deployed in domains that are considered to be critical infrastructures. Risks to these environments are not limited to the company operating the infrastructure. Remote accesses to a control system by vendors, maintenance contractors, management staff accessing from their homes, etc. do expose some aspects of the architecture to remote manipulation. **Security for remote access must be introduced** as long as it does not impede or degrade the normal operational processes that are critical for the control system to function normally (27).

12. Some sectors are already starting projects to improve the security of their ICS. This is the case of the energy sector mainly due to the fact that there are specific regulations

in place like the NERC CIP standards for the bulk electricity transportation or the NRG 5.71 for nuclear power plants. However, there are other sectors that seem to be waiting for a **specific mandate from public organisms** before accomplishing such tasks.

13. **Controlled management of changes** in control logics parameter configurations, firmware version, settings and data files or any other program/application is important in order to prevent disruptions, unnecessary troubleshooting or serious problems in industrial control systems. Therefore it is important to establish a process for change management in industrial control systems (23).

14. Many ICS software and hardware vendors are not aware of **programming good practices and methodologies**. Penetration tests and white box audits in controlled laboratories have shown that there are basic security bugs in devices and applications that could be properly identified if security development good practices were included into the development cycle (28).

15. **Security requirements** should be included from the very beginning **in system specifications and requirements** analyses. It is always difficult and more expensive to implement compensating controls that solve the security deficiencies of those products designed and developed with no security requirements in their specifications (23).

16. **Implementing security programmes** that incorporate ICS under their umbrella can be very costly. Many large operators are making use of compensatory controls to avoid investing lots of money in renewing old insecure devices, operating systems and software applications. However, smaller end users might find even this approach unaffordable.

17. Many **technical, operational and management security controls should be tailored** for each ICS since their applicability differ widely from their classic IT counterparts. CI operators should follow guidelines such as (29), which includes a comprehensive set of security controls that need compensatory alternatives and supplemental guidance. Some examples of security controls that need some tailoring are: account management, separation of duties, least privilege principle, concurrent session control, remote access, auditable events, configuration change control, contingency plan testing and exercises, maintenance tools, remote maintenance, malicious code protection, security functionality verification, etc. (29).

18. **Quality of Service (QoS) parameters of the underlying ICT communication** infrastructure are of paramount importance since many of the ICS need real-time performance, where delay and jitter are unacceptable. Monitoring and guaranteeing these performance metrics should be included as part of the security objectives when implementing security controls. At the same time they should be an essential requirement to be considered when implementing secure communication capabilities into ICS components as well as when developing and implementing security inline tools into an ICS network (1).

19. In many CIs physical security has been an important aspect of the whole security programme. In fact, physical security and safety aspects are the only security domains in place for protecting ICS. Physical security programmes focused on preventing unauthorised access to facilities accommodating critical machinery which is part of the process being controlled or of the ICS itself. However, nowadays many **cyber attacks can be combined with physical attacks to ICT systems** to which access is not restricted. These systems might have not been considered critical for the process but they might be logically interconnected with critical systems (23).

20. **ICS components** in use nowadays are often resource-constrained systems that usually **do not include typical IT security** capabilities. Moreover, many of them do not have enough computing resources available to accommodate current security mechanisms. Additionally, **third-party security solutions are not allowed** due to ICS vendor license and service agreements (1).

21. Typical IT components have a lifetime in the order of 3-5 years. For ICS systems where technology is developed in many cases for very specific use and implementation, the **lifetime is often in the order of 15-20 years** and sometimes longer. This makes it very difficult for ICS components to be secure against new threats that might appear in the years to come (1).

22. Field devices' **evolution from mechanical to electronic devices**, replacing relays with microprocessors have introduced operating systems and high level programming languages in ICS. The increased complexity of the software base may also increase implementation flaws (**software bugs**). Control systems were generally made up of proprietary software but now many controls systems have standard programs or OS, or use IT systems such as TCP/IP networks. Consequently, industrial control systems have inherited the vulnerabilities accompanying these technologies.

23. **ICS security is becoming more fashionable**. Moreover, these systems are already using open systems and commercial off-the-shelf operating systems and protocols (e.g. TCP/IP suite). As a result, the **hacking community is becoming more interested**. They can make use of their standard attacking tools and they have easy access to the knowledge necessary for many of these control systems.

24. Hardening of computer solutions implies removing unused, unnecessary or unknown software modules/service, selecting the most secure configuration parameters and the installation of security patches. This is fundamental for reducing the attack surface and therefore risks. However, **ICS components cannot normally be hardened without strong support from vendors**. Moreover, in many cases it is very difficult to reach a good security level because of the current design of these systems (23).

25. The use of the **Internet as part of many SCADA systems** has introduced new attack vectors that put many CIs at risk. At the same time, new threats, such as cybercrime or industrial cyber sabotage, are now targeting CIs operating ICS with the main objective of extorting or damaging the corporate image. Other threats like terrorism can now take advantage of these new attack vectors.

26. **New vulnerabilities in ICS software** and devices are discovered every day. Operators are often not prepared to face this issue or many times trust that vendors are addressing it. At the same time, ICS vendors are not providing quick and effective responses to this demand. Sometimes there are tensions between security researchers (who disclose vulnerabilities) blaming Manufacturers for undermining the importance of their findings and not recognizing their seriousness. [Siemens managing recently discovered vulnerabilities – several recent press articles]

27. A **defence in depth approach is the better way to protect ICS**. This paradigm implies including multiple layers of protection and overlapping security mechanisms to act as different barriers against attackers. “These security mechanisms may be of the same type, such as multiple firewalls, or of different, supplementary types, such as firewall as network security protection combined with a strong authentication for access to the IT system” (23) (30).

28. **Following up incidents in industrial control systems** should serve as a basis for risk assessment updates and lead to corrective measures and reprioritising resource allocation. However, organisations should address the challenge of establishing a group that meets regularly to discuss incidents and risk problems and to analyse how

they could impact security in the organisation's control systems. This group must consist of representatives from management as well as process control and IT" (23).

1.4 Current Policy Context and Related Initiatives

In this section we will provide an overview of the current European policy context highlighting the most interesting related initiatives on the context of Critical Infrastructures and ICS protection. This section also takes a similar approach in describing the USA's current situation, since we consider that this country is a fair EU peer to be compared with regarding to CIP, CIIP and ICS protection.

A more exhaustive list and descriptions on the different initiatives in ICS security (i.e. public agencies, standardization organisms, public-private associations, industry associations, security programmes, etc.) are presented in **Error! Reference source not found.**. Initiatives resented here are grouped by country, when they are of local scope, or as international or European when they are considered of worldwide influence or with a pan-European scope. This compilation is the result of desktop research activities complemented with those initiatives identified during the surveying and interviewing phases of this study.

1.4.1 The European Policy Context

Due in part to the terrorist attacks in Madrid, in March 2004, against the suburban railway service, the European Council of June 2004 asked the Commission for the preparation of an overall strategy on critical infrastructure protection.

In October 2004, the European Commission (EC) adopted the Communication on "Prevention, preparedness and response to Terrorist Attacks ", COM(2004) 698 (31), provided a non-exhaustive list of the different policy areas where the Commission was currently contributing towards the implementation of the Union's Plan of Action on Combating Terrorism. This list included: external cooperation, integrating European and national systems, authorities' communication with the public, linking-up with the law enforcement community, the security research priority, the role of the private sector, and explosives.

In the same date, and accompanying three other simultaneous Communications, the Communication from the EC on "Critical Infrastructure Protection in the fight against terrorism, COM(2004) 702 (32), proposes the creation of a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical infrastructure Warning Information Network (CIWIN) as additional measures to strengthen the EU's Critical Infrastructure Protection (CIP) capabilities. This Communication also provides the definition of a Critical Infrastructure and enumerates an exemplary list of generic CI's. It also provides initial discussion on the criteria for determining what CI's are. Critical infrastructures were defined as "*those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States*".

In December 2004, the European Council provided their conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks" in which they endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP).

In November 2005 the EC presented the Green Paper on "A European Programme for Critical Infrastructure Protection, COM(2005) 576 (33)", a follow-up publication which addressed the definition of European Critical Infrastructures (ECI's) and National Critical Infrastructures (NCI's). This Green Paper compiled the main results of two seminars and other participative work in which Member States and industry associations participated. As a result, this document outlined policy options on how the Commission could establish EPCIP, including also specific ones for the CIWIN.

The 2005 December Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection.

The EC responded to this request setting out the principles, processes and instruments proposed to implement EPCIP, by adopting in December 2006 the COM(2006) 786 (34) "on a European Programme for Critical Infrastructure Protection". In this Communication, the purpose (i.e. objective and types of threats addressed) of EPCIP was fixed, recognising the threat from terrorism as a priority even though the protection of critical infrastructure would be based on an all-hazards approach. This Communication also defined the main guiding principles of EPCIP and identified the necessity for creating an EU framework concerning the protection of critical infrastructures. This framework was defined in this Communication and included:

- A procedure for the identification and designation of ECI's
- Measures to facilitate the implementation of EPCIP: an action plan, CIWIN, CIP expert groups at the EU level, CIP information sharing process, and the identification and analysis of interdependencies.
- Support for member states concerning NCI's.
- Contingency planning
- An external dimension, enhancing cooperation beyond the EU.
- Financial measures under the umbrella of the EU programme on "Prevention, Preparedness, and Consequence Management of Terrorism and other Security Related Risks".

During that same year and in the context of its i2010 Program, the Commission also adopted the Communication COM(2006) 251 (35), "A strategy for a Secure Information Society –

Dialogue, partnership and empowerment". Its intention was to revitalize the EC's strategy set out in 2001 in the Communication "Network and Information Security: proposal for a European Policy approach". It reviewed the current state of threats to the security of the Information Society and determined what additional steps should be taken. This Communication proposes a "Dynamic and integrated approach that involves the stakeholders based on dialogue, partnership and empowerment". These policy initiatives complemented the activity being planned to achieve the goals of the Commission's Green Paper on the EPCIP. It was the early stages of today's Pan European PPP for Resilience.

In COM(2008) 676 (36) of October 2008, the Commission presented a proposal for a Council Decision on CIWIN. In this Communication CIWIN was defined as an electronic forum for the CIP related to information exchange, as well as a rapid alert system that shall enable participating Member States and the Commission to post alerts on immediate risks and threats to critical infrastructure. The CIWIN pilot phase was launched in the first half of 2010.

Also in December 2008, the Council Directive 2008/114 was issued (37). This Directive defined the procedure for identifying and designating European critical infrastructure and a common approach to assessing the need to improve the protection of such infrastructure.

In March 2009, the Commission adopted COM(2009) 149 (38) on Critical Information Infrastructure Protection. This Communication was named "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". It recognizes that ICT infrastructures are the underpinning platform of other CI's. In fact, Critical Information Infrastructures (CII's) are defined as "ICT systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures". The Communication defines a plan of immediate actions to strengthen the security and resilience of CII's based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, and criteria for EC infrastructures in the field of ICT. None of these activities were targeting Industrial Control Systems specifically. The Communication also highlights that activities under this plan will be conducted under and in parallel to the EPCIP.

Finally, in March 2011, a new Communication from the Commission on Critical Information Infrastructure Protection, COM(2011) 163 (39), was adopted. This Communication on the "Achievements and next steps: towards global cyber-security", recognizes that new threats have emerged, mentioning Stuxnet as an example of a disruption-purpose threat. Threats with destruction purposes, with a direct mention to ICT in Critical Infrastructures such as the Smart Grids and Water systems were also considered. The Communication goes over the achievements of the plan presented on COM(2009) 149 (38), and proposes activities for the future. These activities are classified under the following categories: promote principles for the resilience and stability of the Internet, build strategic international partnerships, and develop trust in the cloud. None of these activities were targeting Industrial Control Systems specifically. As already happened with COM(2009) 149 (38), none of these activities were targeting Industrial Control Systems specifically.

It is not an easy task to find any information about the legal aspects of Industrial Control Systems only. As they are normally used in infrastructure management and, for several reasons, some of these infrastructures can be classified as critical many ICS systems are regulated under Critical Infrastructure (hereinafter CI) laws. So, the approach made in this paper to ICS regulation will be based on International CI regulation.

1.4.2 European initiatives

Apart from EPCIP and CIWIN, which are initiatives already discussed in the previous paragraph, there are several other initiatives in the European context that are worth mentioning.

1.4.2.1 Action plan on CIIP

In order to enhance the security and resilience of CIIs ,an integrated EU action plan was devised which would complement and add value to existing national programmes as well as to the existing bilateral and multilateral cooperation schemes between Member States.

This action plan was firstly introduced in COM(2009)149 and consisted of five main pillars:

- Preparedness and prevention: to ensure preparedness at all levels.
- Detection and response: to provide adequate early warning mechanisms.
- Mitigation and recovery: to reinforce EU defence mechanisms for CII.
- International cooperation: to promote EU priorities internationally.
- Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures.

With respect to the *preparedness and prevention pillar*, among the different action lines defined, we highlight the **European Public Private Partnership for Resilience (EP3R)** which aims to foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures.

Another interesting initiative within the Euroepan Action Plan on CIIP is **EISAS**, the **European Information Sharing and Alert System**, for which ENISA was commission to produce a roadmap for its development and deployment.

For more information on this action plan, please refer to Annex IV.

1.4.2.2 Study for the Commission on the Availability and Robustness of Electronic Communication Infrastructures (ARECI)

The Commission's strategy for a secure information society developed in COM(2006)251 (35) stressed that critical infrastructures are also becoming increasingly dependent on the security

of their respective information systems. The strategy was endorsed by the Council's Resolution of the 22 March 2007 promoting the creation of an environment enhancing the reliability, resilience, and robustness of communication networks and information systems (40).

In preparation for this new action area, Lucent Technologies carried out this study which resulted in a final report. This report presents ten Recommendations to European Institutions, Member States and Private Sector stakeholders to enhance the availability and robustness of Europe's communications networks. These are based on European stakeholder perspectives, technical policy development experience, expertise in emerging technologies and the insights captured in 100 Key Findings.

1.4.2.3 European Network and Information Security Agency (ENISA)

ENISA is an EC dependent European public agency that was created as it became increasingly clear to the Member States that they were all investing a lot of effort in this area. The prime purpose of ENISA is to enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and respond to network and information security problems.

To this end, ENISA is focusing its activities on:

- Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks;
- Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.

The Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP), COM(2009) 149 (38), focusing on protecting Europe from cyber attacks and cyber disruptions by enhancing preparedness, security and resilience, with an Action Plan calling on ENISA to play a role, mainly in supporting Member States. The result of this new role is the study being presented in this report, as well as several other tasks that have been carried out during the last two years. For instance, recently the Agency has produced an initial comment and brief, high level analysis of the 'Stuxnet' attacks against ICS; on its importance, and its technical implications for Europe. The Executive Director of ENISA, Dr. Udo Helmbrecht commented that "After Stuxnet, the currently prevailing philosophies on CIIP will have to be

reconsidered. They should be developed to withstand these new types of sophisticated attack methods" (41).

1.4.2.4 FP6 and FP7 research and development programmes

The Research Framework Programme (FP) is the EU's main instrument for research funding in Europe. The FP is proposed by the European Commission and adopted by the Council and the European Parliament following a co-decision procedure. Framework Programmes normally cover a period of five years (with the exception of FP7 which lasts for seven years), the last year of one FP and the first year of the following FP overlapping.

FP6 ran from 2003 to 2007, and the Information Society Technologies (IST) efforts within it aimed at contributing directly to creating European policies for the information society. Among the strategic objectives of IST FP6 were (40): A global dependability and security framework; semantics-based knowledge systems; networked business and government; e-Safety for road and air transport; e-Health; cognitive systems; embedded systems; improving risk management; and e-Inclusion. FP6 produced results in the area of CIP, standing out:

- **IRIIS**: IRIIS developed MIT (Middleware Improved Technology) which, by supporting recovery actions and increasing service stability in case of critical situations, tried to enhance the security of large complex critical infrastructures. Additionally, a simulation environment was developed, SimCIP (Simulation for Critical Infrastructure Protection), which allowed for controlled experimentation with a special focus on CIs interdependencies (42).

- **CRUTIAL**: Some of the main activities of CRUTIAL were the investigation of models and architectures that cope with the scenario of openness, heterogeneity and endured by electrical utilities infrastructures (43).

- **CI2RCO:** The main objective of the CI2RCO project was to create and coordinate a European Taskforce to encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and to establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security (44).

FP7 started in 2007 and runs until 2013, lasting for seven years. FP7 includes thematic domains of interest that are continued after the end of FP6 and includes two new areas, space and security. Some interesting projects of the FP7 programme addressing ICS security are:

- **ESCoRTS:** ESCoRTS aimed to be a leading force for disseminating good practice on security of Supervisory Control and Data Acquisition (SCADA) systems, hastening and ensuring convergence of SCADA standardization processes worldwide, paving the way to establishing cyber security testing facilities in Europe (45).

- **INSPIRE:** INSPIRE aimed at identifying techniques to enhance the reliability of communications over unreliable and/or insecure links (WAN, wireless) in SCADA systems (46).

- **VIKING:** This project aimed at investigating the vulnerability of SCADA systems and the cost of cyber attacks on society, proposing and testing strategies and technologies to mitigate these weaknesses and increasing awareness of the importance of critical infrastructures and the need to protect them (47).

1.4.3 The USA policy context

Even though the 11th September 2001 was a clear inflection point in CIP and CIIP in the USA, there were already efforts being made with regards to this since the 1990's. Actually President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, as a first effort to address the vulnerabilities of the information age, and its main conclusion (October 1997) was that it was necessary to foster the cooperation and communication between the private sector and government. Accordingly, in May 1998, Clinton issued Presidential Decision Directive (PDD) 63, PDD-63, by which the government intended to develop, in close collaboration with the private sector, National Infrastructure Assurance Plans for each of the major sectors of the USA economy. As a result, in January 2000, a first version of a National Plan for Information Systems Protection was published. This plan, called Defending America's Cyberspace, focused on securing the cyber-components of critical infrastructures, but not the physical components (40).

In October 2001, after the September the 11th terrorist attacks, President Bush signed two Executive Orders (EO) affecting CIP. EO 13228 established the Office of Homeland Security to coordinate efforts to protect the country and its CI's from terrorist attacks. It also established the Council of Homeland Security which advises and assists the president in all aspects of homeland security. The other EO was EO 13231, by which the National Infrastructure Advisory Council (NIAC) was established. The NIAC shall provide the President with advice on the security of information systems for critical infrastructure and shall be composed of not more than 30 members selected from the private sector, academia, and State and local government. Additionally, EO 13231 created the President's Critical Infrastructure Protection Board, its responsibilities are to "recommend policies and coordinate programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems" (48).

Just some days after President Bush signed these two EO's, he also signed into law the USA's Congress Patriot Act, which, among other things, defined what CI's are: "[…] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (49).

In December 2003, Bush released Homeland Security Presidential Directive (HSPD) 7, which supersedes PDD-63. This directive established a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. This directive reinforces collaboration with the private sector and continues to encourage the development of information sharing and analysis mechanisms. Additionally, it also designates the Secretary of Homeland Security as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources. The Secretary had to "produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources (CIKR) Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, […], the following elements (50):

- A strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;
- A summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;
- A summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector;
- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals".

Finally, by July 2004, the heads of all Federal departments and agencies had to develop and submit to the Office of Management and Budget for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

1.4.4 USA's related initiatives

What follows is a brief overview on some of the major initiatives taken by the government of the USA with regard to CIP and in particular to ICS protection. This overview is not all-inclusive and we refer the reader to consult (51) for more information.

1.4.4.1 National Infrastructure Protection Plan (NIPP)

As a response to the requirements that the President set forth in HSPD-7, the National Infrastructure Protection Plan was presented, with a first version in 2006 which was replaced in 2009 by a second version that captures the evolution and maturation of the processes and programs first outlined in 2006 without changing the underlying policies.

The NIPP and its complementary Sector-Specific Plans (SSPs) provide a consistent, unifying structure for integrating both existing and future CIKR protection efforts. The NIPP also provides the core coordinating processes and mechanisms that enable all levels of government and private sector partners to work together to implement CIKR protection in an effective and efficient manner. Together, the NIPP and SSPs provide the mechanisms for: identifying critical assets, systems, and networks, and their associated functions; understanding threats to CIKR; identifying and assessing vulnerabilities and consequences; prioritizing protection initiatives and investments based on costs and benefits so that they are applied where they offer the greatest mitigation of risk; and enhancing information-sharing mechanisms and protection and resiliency within and across CIKR sectors (52).

1.4.4.2 National strategy for Information Sharing

The NIPP and its complementary SSP highlight the importance of information sharing between different sectors as well as between the government and the private sector. The National Strategy for Information Sharing, published in 2007, builds upon already established organizations and initiatives, and provides guidelines for sharing information to protect critical infrastructures. It states that “the exchange of information should be the rule, not the exception” (53).

1.4.4.3 The US-CERT

Information-sharing is one of the driving factors behind effective early-warning networks and as a result, many information-sharing entities are also engaged in early-warning activities.

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS), and its mission is to improve the nation's cyber security posture, coordinate cyber information sharing and proactively manage cyber risks to the USA (54).

1.4.4.4 The Control Systems Security Program (CSSP) and the ICS-CERT

The goal of the DHS National Cyber Security Division's CSSP is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments, as well as industrial control systems owners, operators and vendors. Under the US-CERT, the CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

As a key part of the CSSP, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Respond to and analyze control systems related incidents
- Conduct vulnerability and malware analysis
- Provide onsite support for incident response and forensic analysis
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of vulnerabilities/mitigations
- Share and coordinate vulnerability information and threat analysis through information products and alerts

The ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems' security can be realized through successful coordination efforts (55).

1.4.4.5 The Industrial Control Systems Joint Working Group (ICSJWG)

The Department of Homeland Security (DHS) Control Systems Security Program (CSSP) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems.

The ICSJWG is a collaborative and coordinating body which provides a vehicle for communicating and partnering across all Critical Infrastructure and Key Resources Sectors (CIKR) between federal agencies and departments, as well as private asset owners/operators of industrial control systems. The goal of the ICSJWG is to continue to enhance the collaborative efforts of the industrial control systems' stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems (56).

1.4.5 The EU-US Working Group on Cyber-Security and Cybercrime

This bilateral initiative between the USA and the EU was established in the context of the EU-US summit of the 20th November 2010 held in Lisbon, to tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend. The EU-US WG intends to address a number of specific priority areas which, amongst others, include a broad commitment to engage the private sector, sharing of good practices on collaboration with industry, and pursuing specific engagement on key issue areas such as fighting botnets, **securing industrial control systems and smart grid** (such as water treatment and power generation), and enhancing the resilience and stability of the Internet. The proposed tasks for this cooperation included the stock taking and comparative analysis of

existing initiatives, pilots, good practices and methods addressing ICT risks, privacy and security.

It is expected that this collaboration will result in a Plan of Action for EU and US public private engagement on cyber security of industrial control systems and Smart grids; this will also draw on an analysis of existing coordination bodies for security of industrial control systems and highlighting best practices developed within them.

For more information on this initiative please refer to Annex IV.

1.5 Technical Solutions

In this chapter we present a list of existing security technologies that allow us to respond to the technical challenges identified in section 1.3. In some cases the solutions presented are "well know" technologies, widely adopted by the IT sector. In other cases the solutions are innovation technologies which can help to improve the level of security of ICS architecture.

1.5.1 Access Control

1.5.1.1 Authentication

There is a whole family of technologies to confirm the identity of a person or entity so it can be trusted. Usually, they are divided into three categories regarding the identifying method:

- By knowledge: The user has to answer with some private information such as a password, PIN or passphrase.
- By object: It is necessary to possess a trusted object, such as a key, smartcard or token.
- By person: If it is necessary to show some biometric evidence such as fingerprints or eye-scans.

Some technologies associated with authentication are:

- Username and Password: The simplest and most common technique. It is just a knowledge question. It is important to have a password enforcement policy to ensure that they are long enough and difficult enough to break.
- Challenge and Response: For this type of authentication the requester and the provider know a secret code in advance. When service is requested a challenge is sent and has to generate a unique answer, so the user gives an answer without revealing the secret.

- Token / Smartcard: They act as object-based authentication methods but usually perform additional functionality such as OTP generation (see below) or run on-board applications.
- Biometric: Those technologies use unique biological characteristics of a human, such as facial geometry, iris signatures or voice patterns.
- Location Based: They provide authentication based on the physical location of the requester. They may involve GPS technologies or fixed IP addresses.
- One Time Password (OTP): Another common solution is the use of hardware or software tokens to dynamically generate passwords that can be used just once. It is usually combined with a username and PIN/password to provide Multifactor Authentication.
- Multifactor Authentication: When different authentication factors have to be used simultaneously to validate a user or system.
- Network Access Control (NAC): A family of technologies that allow or prevent the authentication based on the analysis of the endpoint security status (checking the antivirus, HIPS or vulnerability assessment). It is often implemented through the IEEE 802.1x standard for port-based NAC.

In ICS security, some vendors provide the possibility for the use of fingerprinting technologies which can be used by security to identify univocally devices, even including configuration properties. The aim of this is to build virtual confidence-rings within a network, following a certificate-like procedure.

This kind of security technology is used for the user's access control in the majority of devices (SCADA servers, network devices, field devices, etc.) integrated in ICS infrastructure. For more information on this technology we encourage the reader to have a look to (11).

1.5.1.2 Authorization

More than a technology or family of technologies authorization is the function of specifying rights to resources for a given user and must not be confounded with authentication.

Nowadays, authorization techniques are integrated in company horizontal services such as LDAP (Lightweight Directory Access Protocol) or AD (Active Directory) with role-based technologies.

The authorization techniques are often combined with authentication technologies to allow role-based access to users permitting them to access protected SCADA control network and securing the perimeter network.

For more information on this technology we encourage the reader to have a look to (57).

1.5.1.3 Identity and Access Management

Close to both of the previous technologies (Authentication and Authorization) there is a family of products that guarantee that users have their proper authentication methods and authorization privileges in all systems during their lifecycle in a company. These technologies are called IAM and are able to manage the creation, modification, and elimination of accounts and privileges in an easier way. It is commonly accepted that, even if they are mainly IT management technologies, they provide additional security layers by providing further user control, policy enforcement and validation or delegation processes.

State-of-the-art solutions can also perform data mining of users and roles, bringing to light conflictive or non-compliant privileges.

Like the two previous technologies, the security system presented in this section is used to protect the SCADA network and all devices from inappropriate access.

For more information on this technology we encourage the reader to have a look to (57).

1.5.2 Segmentation

1.5.2.1 Firewalls

Firewalls are also used in ICS Security to permit or deny transmissions between the Corporate and Control networks based upon a set of rules.

The firewall market is very mature and many generations of devices have existed. State-of-the-art firewalls do not just filter packets, as they might provide some response to other input as application, protocol or even Deep Packet Inspection. The different approaches are:

- Packet Filtering: The basic strategy is to operate at layer 3 of the OSI model (network). Matching basic information, such as IP addresses, against a set of rules the device can permit or deny the communication. They are low cost and low impact systems.
- Stateful Inspection: These solutions provide OSI's layer 4 support, so they can perform filtering rules depending on the transport protocol information (TCP, UDP, etc…). This provides control over active sessions, so can be more powerful and complex.
- Application Firewalls: This approach enables checking and filtering for specific applications or protocols. It provides a high level of control on communications, but may cause greater delays, sometimes excessive for ICS environments.
- Deep Packet Inspection: Is a packet filtering technology based on the packet header or the data itself. They can be used to implement extremely granular rules, and enable advanced network management, user service and security functions.

They are commonly used in ICS Security to perform segregation strategies within operator assets. They can block all but accepted communications between a LAN and a Control Network, be used to create internal DMZs, enforce authentication methods and authorization privileges, record flow logs end even isolate Control Systems in case of emergency. There are some efforts invested in developing firewalls to support ICS specific protocols.

For more information on this technology we encourage the reader to have a look at (58).

1.5.2.2 IDS/IPS

Intrusion Detection or Prevention Systems approach is to monitor the activity of a network or system in order to detect malicious activities.

Therefore, there are two main types of IDS/IPS:

- Network based: That check for network traffic abnormalities. They are very often deployed in the DMZ between Corporate and Control networks.
- Host based: Software monitors checking for stations activities by log files, configuration changes and sensitive data access. They are usually installed in general purpose computers or HMI/SCADA servers.

The main difference between both is that IDS is a detector only able to alert administrators, while IPS has blocking capabilities. Network based IPSs are, therefore, installed as in-line appliances and their functionality has more in common with Firewalls.

IDS/IPS technology is very mature and state-of-the-art devices can alarm administrators, drop packets, reset connections or IP addresses, perform virtual patching[4], correct CRC errors, provide Network Behaviour Analysis (NBA) to detect DoS or even DDoS among other functionalities. Recently some vendors have started to support ICS specific protocols such as Modbus, DNP or ICCP.

Due to the nature of ICS traffic, which is generally considered to be different from more traditional business systems, and unique protocols that may be implemented, the use of the IDS/IPS should be carefully examined to ensure that the safe and reliable operation of the system being controlled is not compromised by automated actions of the IDS/IPS.

However, the benefits of this type of protection technology are huge, because it prevents the spread of viruses and cyber attacks on the network, providing a virtual patching of servers within control systems. It is worth mentioning, that IPS technology requires some maintenance work, because as time passes, it is necessary to update IPS's settings including new attacks vectors. For more information on this technology we encourage the reader to have a look at (59).

[4] *Providing advanced protection towards devices that, for some reason, have not been patched.*

1.5.2.3 Data Diodes

Data Diodes are devices designed to transmit information between two networks or devices but just in one direction.

There are different alternatives to implement a DD solution:

- Some providers offer an infrastructure that requires two proxies and the data diode itself. The "sender" proxy concentrates all data from its segment and sends it through the diode to the "receiver", which will propagate the information within its segment. They also have the mission to establish sessions in bidirectional protocols, not designed for simplex communication. The diode architecture might be compatible with FTP, SMTP, CIFS or UDP but in this moment many industrial protocols are not supported[5], and potential users have to take this into account. Anyway, the manufacturers of this kind of technology are focussing their efforts to include ICS protocols in their appliances.

- Other providers offer hardware based solutions to be configured in a control-network to corporate-network most of the time, but that can be reverted in some situations (for example, to configure a remote device through the internet) and even for a limited amount of time. In that cases a physical or electronic key, a numeric keyboard or a biometric system might be used for authentication.

Therefore, the data diode based solution can be used to isolate the control and monitoring network of a corporate network. For more information on this technology we encourage the reader to take a look at (60).

1.5.2.4 Web Application Firewall

WAF devices are placed in the front of Web Application Servers to provide an enhanced security level, providing virtual-patching of the application. They can verify all data transmitted in both directions to guarantee only valid data transmission and avoid attacks such as SQL-injection or Cross-Site Scripting. In some cases they are also able (and need) to terminate and start SSL communications or monitor the session flow.

This technology is used to avoid attacks against corporate network from Internet. In some cases the ICS system has a web interface accessible from the Internet that allows operator users to remotely access the system, so this technology can be exploited here. Therefore, the presented solution is used to protect the network perimeter from malicious users. For more information on this technology we encourage the reader to have a look at (61).

[5] *Some providers are working in the integration of OPC Kepware or Matrikon servers in their solutions.*

1.5.2.5 Segmentation by Encryption

Some products in the market are able to provide encryption to devices within a network, isolate servers, terminals or users providing another level of logic segmentation even within a network.

In the current state of the art it is necessary to install an agent on the device that can be controlled by an administrator from a centralized console. Some solutions make use of certificates signed by the Admin Server or provide AD integration.

1.5.3 Secure Communications

1.5.3.1 VPN

Different products in the market make use of VPN technologies to provide secure access to private networks from the outside. In an ICS environment, VPN connections are mainly used to connect from remote networks to get into the Control Network with a client using a strong authentication mechanism, in most cases multi-factor (see “Authentication”).

VPN technologies have been around for a long time in the IT world, and several implementations have been made with different levels of reliability. The most popular VPN technologies implemented today are:

- Internet Protocol Security (IPsec): Is a set of standards defined by the Internet Engineering Task Force, included in many current OS, to facilitate interoperability across vendors. It supports transport and tunnel encryption. The first mode encrypts the data, but not packet headers. The tunnel encrypts both, so it is more secure. The protocol has been enhanced to fulfil more requirements, but those extensions are very often provided by vendors and may lead to interoperability issues.

- Secure Sockets Layer (SSL): This protocol provides a point-to-point encryption channel for each packet. There have been various different versions of SSL, where the last of them (SSL v3.0) is also called TLS (Transport Layer Security). It is very often used for, but not limited to, securing HTTP traffic. One of the main advantages of this protocol for VPN is that it does not require any endpoint client as most browsers have built-in support for it.

- Secure Shell (SSH): SSH is a secure command interface protocol that can be used in addition to VPN as an alternative to telnet. It is used to control servers, as it is included in most UNIX distributions. The latest version SSH2 is proposed by the IETF.

VPN technologies are widely adopted in Control Systems as they improve security, restricting access to Control Networks even if compatibility tests are necessary in multi-vendor environments. Furthermore, The VPN tunnelling can be used in communications between

field devices and Front-end servers to secure the transmitted information. For more information on this technology we encourage the reader to have a look at (25).

1.5.3.2 Public Key Infrastructure

These technologies provide a solution for secure communications based on the emission and revocation of certificates and public keys by a Certified Authority (CA). They are based on asymmetric cryptography by Public Key, with authentication and non-repudiation methods.

In ICS environment it is often used to provide an additional layer of security for remote access in public networks, as their use in real-time control networks is often discouraged because of additional delays. Nevertheless, elliptic-curve based asymmetric cryptography is helping to change this.

For more information on this technology we encourage the reader to take a look at (25).

1.5.3.3 Wireless Security

In ICS networks wireless technologies are often used to control RTU, PLC, and substations which are located in remote places.

Common security issues with wireless communications often include the residual effects of default installations. Attackers, once having discovered wireless communications points, can leverage the inherent functionality of wireless networks and take advantage for instance of Service Set Identifier (SSID) broadcasting (e.g. Wi-Fi), limited access controls, lack of encryption, and limited network segmentation. When considering the historical characteristics of control system networks, especially those that impact security because of the presence of plaintext traffic and inherent trust relationships, unauthorized access (via a wireless access point) into the control domain can provide an attacker with a very effective backdoor, often bypassing security perimeters.

Therefore, improving security in such environments is necessary, making the architecture more robust against possible attacks. Most popular wireless security mechanisms implemented today are:

- Create a WLAN security policy and educate all employees regarding the policy. The policy should outline a framework for the development of installation, protection, management, and usage procedures.
- Do not rely on default security configurations of WLAN access points and adapters.
- Employ MAC address filtering on the access points. This is a low-level security control on the access point that permits only those stations with Ethernet MAC sub layer addresses on a list contained within the access point to communicate with the access point.

- Disable SSID beacon transmissions so that the WLAN is not advertised to client stations that should not be allowed to connect. When the SSID broadcast is disabled, the client stations must know the SSID of the WLAN to which they want to connect.
- Use non-suggestive SSID naming conventions to avoid focusing the attention of a potential attacker.
- Utilize 802.11i security, not WEP, for Layer-2 security. The 802.11i/WPA2 standard employs both TKIP and AES to provide stronger frame encryption, authentication, and integrity and replaces the original WEP standard.
- Unless absolutely needed, disable direct station-to-station "Ad Hoc Mode" transmission. "Ad Hoc" mode enables stations to communicate with each other directly. Unless an industrial application requires this type of communication, it should be disabled so that a potential attacker cannot try to associate directly with a station on the WLAN.
- Unless absolutely needed, disable station-to-station communication through the access point.
- Protect the WLAN end-points and stations (especially in mobile applications) through technical and administrative hardening methods (disable unnecessary services, restrict management protocols such as SNMP, etc,).
- Firewall appliance placed in front of the end point to inspect and restrict connectivity to the minimum set of trusted host pairs should be considered.
- Employ static IP addressing of devices on the WLAN instead of dynamic assignment if possible when IP is the next higher-layer network protocol.
- Use static ARP entries on WLAN stations and access points.
- Limit RF power transmission to minimum required levels. Limiting the transmit power levels of station adapter cards and access points to the minimum level required to achieve the coverage and data rates required is a sound security practice.
- Use directional antennas if possible.
- Deploy or leverage existing wireless intrusion detection capability. A wireless IDS (WIDS) can monitor the WLAN environment and potentially detect attempted known

attacks. Several vendors sell stand-alone WIDS solutions with 802.11 sensors that act independently of the deployed WLAN.

- If the IP protocol is used as the network layer protocol, employ a private IP addressing scheme to prevent an attacker obtaining the IP addressing scheme.
- Ensure that ARP broadcasts from the wired network do not propagate to the WLAN. Using the principle of segmentation, the WLAN and wired LAN networks should be in different subnets and broadcast domains as well as isolated and separated with a filtering device such as a firewall.
- In a ZigBee environment, use the security services implemented by the technology itself, such as cryptographic key establishment, key transport, frame protection, and device management. The ZigBee security architecture includes security mechanisms at three layers of the protocol stack - MAC, Network, and Application. Each layer has services defined for the secure transport of their respective frames.

Finally, it is important to note that wireless communications are becoming widely used for many applications. Utilities will need to be very careful where and for what functions they implement these wireless technologies, partly because of the noisy electrical environment of substations (potential impacts to availability), and partly because of the very rapid and extremely reliable response required by some applications (throughput). Although security measures are available for many wireless systems, these can increase the overhead (albeit in a similar manner to wired media). For more information on wireless communications in the context of ICS have a look at (62) (63).

1.5.4 Audit and Logging

1.5.4.1 Loggers

Not all ICS devices are prepared to log events, or are not able to transmit them to a centralized server for even very long periods (for example, offshore devices). Some ICS Security manufacturers provide solutions to this, making forensic analysis possible and facilitating compliance needs.

This technology should be implemented in all of the devices existing in the ICS architecture, to permit the administrator to control the security issues of the ICS system at all times. For more information on this technology we encourage the reader to have a look at (51).

1.5.4.2 Security Information and Event Management

SIEM technologies combine the formerly existent SIM and SEM product categories. The objective is to collect and centralize the logs that are dispersed within a network for audit and

compliance requirements (SIM) and to correlate and exploit this information in order to generate alerts, dashboards, reports, etc (SEM).

SIEM technologies can help to facilitate the work of administrators by automatically collecting and correlating the reports generated by the devices, reducing the response time to a threat. More information on SIEM technology can be found at (51).

1.5.5 Vulnerability and Risk Assessments

1.5.5.1 Vulnerability Assessments

These technologies are used to provide a fast, precise and comprehensive exploration of known vulnerabilities among a company network. Assets are checked to get the HW or SW status and correlated with vulnerability databases provided by vendors or trusted authorities in order to identify risks.

In ICS environments vulnerability scanners must be used with caution on production networks to avoid accidental DoS and other undesired effects. However, they are of great importance since they can actively help in security assessments, an essential task for risk assessment of the ICS system, as one key point of a cyber security plan. For a more detailed description of vulnerability assessments, please refer to (51).

1.5.5.2 Vulnerability Management / Host Bastioning

Closely related to Vulnerability are the solutions to manage the vulnerabilities, patching or updating assets, as well as to get reports as a record of the results.

It is important to state that those tasks have a considerably higher cost, as they are unlikely to be automatic or trivial tasks and may have stability issues. However, they can be necessary if the vulnerability assessment results show unacceptable risks. We encourage the reader to have a look at (51) for more information on this topic.

1.5.6 Application and Data Control

1.5.6.1 Antivirus

Antivirus are widely used software technologies to identify, prevent and remove malware. A variety of strategies are used such as signature-based detection, heuristics or rootkit detection.

This type of products is very common in general purpose computers but they are, in general, not oriented for ICS security requirements. In addition, modern antivirus make extensive use of terminal resources, which is often not acceptable for the legacy equipment often found in ICS environments.

Actually, vendors are focussing their efforts on including specific antivirus technologies on the entire field devices such as RTUs, PLCs, MTUs, etc., and control centre computers present in ICS architecture. For more information on this topic, please have a look at (51).

1.5.6.2 Application Whitelisting

Application Whitelisting solutions' idea is to avoid malware activity in a station by permitting the activity of just a set of applications, blocking any other not listed.

It is often preferable to conventional AV technologies in ICS environments because:

- BW, CPU and memory resources are usually more limited
- AV integration with Control Systems is a complicated process

This approach is also interesting because it reduces the need for updating and patching, which might be costly in ICS networks and are often based on legacy technologies.

State-of-the-art whitelisting applications can include:

- Binary identification by name, route, hash, size…
- Kernel service to check out before starting a new executable, or an associated dll.
- Discovery functionality to facilitate the creation of the initial whitelist.
- Fingerprinting techniques to distinguish the same application in different machines.
- Centralized management
- Different lists for different roles or uses.
- Vendor signature integration, to perform whitelisting updates by a trusted source.

An alternative approach is the one called Application Blacklisting, in which just a set of applications are disallowed. This benefits productiveness for end users, as they have greater control, but are, by far, less secure as administrators have to determine risky applications in advanced. There are also ways to determine if an application is secure or not by heuristic methods, assigning risks to different parameters such as provider, or predetermined file location.

Therefore, these solutions can be helpful in supervisory control computers as well as in field devices, where the patching processes are tedious and require careful planning and where applications and processes running are quite static. For more information on application whitelisting please have a look at (64).

1.5.6.3 Data Loss Prevention (DLP)

Data Loss (or Leak) Prevention (or Protection) technologies are used to control the use and flow of sensitive data across a network. They are very intrusive techniques as state-of-the-art solutions take into account:

- Data in use: The information being worked on in every station by monitoring the endpoints.
- Data in motion: By monitoring network traffic and checking for confidential data
- Data at rest: using discovery and data mining techniques to scan all repositories and identifying the resources in which the information is located.

They are not very popular in ICS networks as they are more oriented to scenarios in which the value rests on the information itself (such as credit card numbers) than to real-time Control Systems. However, where they might become useful is in the data exploitation process from historical and other business information processing applications and servers. This solution could help avoiding attacks such as Night Dragon, which is presented in this report in section 1.2.1.

1.6 Known Good Practices, Standards and Policies

In the following section we will provide an overview of the most relevant guidelines, standards and policies that are currently available or under development regarding ICS security. It is important to highlight that we consider the following definitions:

- **Guidelines:** recommended security good practices, technical reports on specific topics and any worksheet supporting activities such as risk analysis self-assessment, security requirements definition for ICS components, ICS components assessment from a security perspective, etc.
- **Standards:** documents intended for defining new security mechanisms or frameworks focusing on interoperability or certification aspects.
- **Policies/regulations:** industrial mandates or governmental mandates for ICS operators, manufacturers, integrators, etc. Official supporting/guiding documents to comply with this regulation fall under this category.

There are a good number of guidelines, standards and regulations currently addressing different aspects of cyber security on ICS. During the desktop research phase, 35 different documents were studied: 24 guidelines, 9 standards and 3 regulatory documents. However, it is worth highlighting that many of them are generic, meaning that they focus on security aspects affecting ICS from a general perspective. However, there are also many documents

focusing on the Energy Sector, including here oil, gas and electricity subsectors. Moreover, inside the Energy sector, it is the electricity subsector which presents by far the largest number of guidelines, standards and regulatory documents. It seems that the Energy sector and specially the electricity sector have been very active in addressing the cyber security risks affecting their ICS. At the same time, other sectors like transportation (e.g. railway transportation or airports), water supply (e.g. water distribution and waste water), or agriculture (e.g. food production) might be seen as not very active in this field.

It is also interesting to see that most of these documents are in a final state, even though there are important initiatives that are still in a draft version; this is the case of the ANSI/ISA 99 and of IEC 62443 standards. Additionally, there have been many new publications or updates in the last three years (2009, onwards). Actually, 18 of the 35 identified documents were published during 2009, 2010 or 2011 which shows the increasing relevance of this subject. While there are many documents coming from the United States of America or from international organizations such as IEEE, ISO, etc. it is also remarkable that many countries in Europe have defined their own guidelines or even industrial mandates. Some of the most active countries are the United Kingdom, Germany, and Norway.

There are important efforts regarding the improvement and standardisation of the security of SCADA and DCS communications. For instance, the IEC 62351 focuses on the security of many important protocols of the Energy sector such as IEC 60870-5 (DNP3, IEC101, IEC104), or IEC 60870 (TASSE.2/ICCP). Another example is the IEEE 1711, published early this year, which defines a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of serial links.

Several guidelines provide advice based on industrial security good practices for relevant issues specific to ICS. This is the case for CPNI Good Practice Guide series on process control and SCADA security which focuses on aspects like cyber security assessments of ICS, configuring and managing remote access for ICS, or firewall deployment for SCADA and process control networks.

A very important aspect of cyber security is to establish inside the company an Information Security Management System (ISMS). With regards to this, there are several documents that have been studied which guide operators on how to include industrial control systems into their ISMS. For example, the international standards IEC 62443 and ANSI/ISA 99 address this issue but unfortunately are not yet in their final versions. Other documents that help operators develop such an ISMS system are API 1164 or a combination of the famous ISO 27000 framework with NIST 800-53 rev. 3 or NIST SP 800-82 guidelines. These last two documents address specific security controls for ICS, provide enhancements to classic ones, and also supplemental guidance for those controls that can be applied in an almost straightforward manner. There are multiple other guidelines that have been analysed which deal with specific controls for ICS operators that could also be used as a reference for including ICS inside the company's ISMS.

Finally, there is a very useful set of documentation which addresses the set of security requirements and characteristics that new ICS components should include to comply with critical infrastructure protection programmes. Some of them are based on the famous ISO/IEC 15408 standard ("Common Criteria"), which is a framework in which computer systems functional and assurance requirements can be defined and tested, and which is also presented in this section. These kinds of requirements are very useful since they allow operators to ask vendors for specific security functions in their products, as well as to consider appropriate criteria when making purchasing decisions. For instance, the IEEE 1686-2007 defines the functions and features to be provided in substation IEDs to accommodate CIP programmes. Another example could be the "WIB Security Requirements for Vendors" mandate, which specifies requirements and gives recommendations for IT security to be fulfilled by vendors of process control and automation systems.

2 References

1. **National Institute of Standards and Technology (NIST).** *NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology. 2011.

2. **Boyer, Stuart A.** *SCADA: Supervisory Control and Data Acquisition.* Iliad Development Inc., ISA. 2010.

3. **Institute of Electrical and Electronics Engineers (IEEE).** *IEEE Standard C37.1-1994: Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control.* Institute of Electrical and Electronics Engineers. 1994.

4. **United States General Accounting Office (GAO).** *Critical infrastructure protection. Challenges and Efforts to Secure Control Systems.* United States General Accounting Office. 2004.

5. **Bailey, David and Wright, Edwin.** *Practical SCADA for Industry.* s.l. : Newnes, 2003.

6. **West, Andrew.** SCADA Communication protocols. [Online] http://www.powertrans.com.au/articles/new pdfs/SCADA PROTOCOLS.pdf.

7. **Department of Energy (DoE).** Hands-on Control Systems Cyber Security Training of National SCADA Test Bed. [Online] 2008. http://www.inl.gov/scada/training/d/8hr_intermediate_handson_hstb.pdf.

8. **Boyer, Stuart A.** *SCADA Supervisory and Data Acquisition.* 2004.

9. **International Society of Automation (ISA).** ISA99 Committee - Home. [Online] http://isa99.isa.org/ISA99 Wiki/Home.aspx.

10. *Identifying, understanding, and analyzing Critical Infrastructure Interdependencies.* **Rinaldi, Steven M., Peerenboom, James P. and Kelly, Terrence K.** 2001, IEEE Control Systems Magazine.

11. **American National Standard (ANSI).** *ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models.* International Society of Automation (ISA). 2007.

12. **Tsang, Rose.** *Cyberthreats, Vulnerabilities and Attacks on SCADA networks.* 2009.

13. **Falliere, Nicolas, Murchu, Liam O and Chien, Eric.** *W32.Stuxnet Dossier.* Symantec. 2011.

14. **Centre for the Protection of National Infrastructure (CPNI).** *Cyber security assessments of industrial control systems.* Centre for the Protection of National Infrastructure. 2011.

15. **IBM Global Services.** *A Strategic Approach to Protecting SCADA and Process Control Systems.* 2007.

16. **Centre for the Protection of National Infrastructure (CPNI).** *Firewall deployment for scada and process control networks.* Centre for the Protection of National Infrastructure. 2005.

17. —. *Process control and SCADA security. Guide 5. Manage third party risk.* Centre for the Protection of National Infrastructure.

18. —. *Process control and SCADA security. Guide 7. Establish ongoing governance.* Centre for the Protection of National Infrastructure.

19. **International Electrotechnical Commission (IEC).** *IEC TS 62351-1: Power systems management and associated information exchange – Data and communications security. Part 1: Communication network and system security – Introduction to security issues.* International Electrotechnical Commission. 2007.

20. **Department of Homeland Security (DHS).** DHS officials: Stuxnet can morph into new threat. [Online] 2011. http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat.

21. **McAfee.** Global Energy Cyberattacks: "Night Dragon". [Online] 2011. http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.

22. **Gartner.** Assessing the Security Risks of Cloud Computing. *Gartner.* [Online] 2008. http://www.gartner.com/DisplayDocument?id=685308.

23. **Swedish Civil Contingencies Agency (MSB).** *Guide to Increased Security in Industrial Control Systems.* Swedish Civil Contingencies Agency. 2010.

24. **American Gas Association (AGA).** *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 1 Background, policies and test plan.* American Gas Association. 2006.

25. —. *AGA Report No. 12, Cryptographic Protection of SCADA Communications. Part 2 Performance Test Plan.* American Gas Association. 2006.

26. **International Electrotechnical Commission (IEC).** *IEC TS 62351-7: Power systems management and associated information exchange – Data and communications security. Part 7: Network and system management (NSM) data object models.* International Electrotechnical Commission. 2010.

27. **Centre for the Protection of National Infrastructure (CPNI).** *Configuring & managing remote access for industrial control systems.* Centre for the Protection of National Infrastructure. 2011.

28. **DigitalBond.** DigitalBond. *ICS Security Tool Mail List.* [Online] http://www.digitalbond.com/tools/ics-security-tool-mail-list.

29. **National Institute of Standards and Technology (NIST).** *NIST SP 800-53: Information Security.* National Institute of Standards and Technology. 2009.

30. **North American Electric Reliability Corporation (NERC).** *CIP-003-4: Cyber Security — Security Management Controls.* North American Electric Reliability Corporation. 2011.

31. **Commission of the European communities.** *Communication from the commission to the council and the European parliament. Prevention, preparedness and response to terrorist attacks COM(2004) 698 final.* 2004.

32. —. *Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM(2004) 702 final.* 2004.

33. —. *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.* 2005.

34. —. *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.* 2006.

35. —. *Communication from the commission to the council, the European parliament, the European economic and social commitee and the commitee of the regions. A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment' COM(2006) 251.* 2006.

36. *Council decision on a Critical Infrastructure Warning Information Network (CIWIN) COM(2008) 676».* **Commission of the European communities.** 2008.

37. **Commission of the European communities.** *Council directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* 2008.

38. —. *Communication from the commission to the European parliament. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.* 2009.

39. —. *Communication from the commission to the European parliament, the European economic and social commitee and the commitee of the regions. Achievements and next steps: towards global cyber-security.* 2011.

40. **Suter, Manuel and Brunner, Elgin M.** *International CIIP Handbook 2008 / 2009.* 2008.

41. **European Network and Informations Security Agency (ENISA).** *EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection.* [Online] 2010. http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1.

42. **IRRIIS Project.** Homepage of the IRRIIS project. [Online] 2006. http://www.irriis.org.

43. **CRUTIAL Project.** CRitical Utility InfrastructurAL resilience. [Online] 2006. http://crutial.rse-web.it.

44. **CI2RCO Project.** Critical information infrastructure research coordination. [Online] 2008. http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=79305.

45. **ESCoRTS Project.** Security of Control and Real Time Systems. [Online] 2008. http://www.escortsproject.eu.

46. **INSPIRE Project.** INcreasing Security and Protection through Infrastructure REsilience. [Online] 2008. http://www.inspire-strep.eu.

47. **VIKING Project.** Vital Infrastructure, Networks, Information and Control Systems Management. [Online] 2008. http://www.vikingproject.eu.

48. **The White House.** Executive Order 13231. [Online] 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

49. **Jeff Trandahl, Clerk.** USA Patriot Act (H.R. 3162). [Online] 2001. http://epic.org/privacy/terrorism/hr3162.html.

50. **Department of Homeland Security (DHS).** Homeland Security Presidential Directive-7. [Online] 2003. http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1.

51. **Stouffer, K. A., Falco, J. A. and Scarfone, K. A.** *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC).* s.l. : National Institute of Standards and Technology, 2011.

52. **Department of Homeland Security (DHS).** *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency.* Department of Homeland Security. 2009.

53. **The White House.** National Strategy for Information Sharing. [Online] 2007. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html.

54. **United States Computer Emergency Readiness Team (US-CERT).** US-CERT: United States Compueter Emergency readiness Team. [Online] http://www.us-cert.gov.

55. —. Control Systems Security Program: Industrial Control Systems Cyber Emergency Response Team. [Online] http://www.us-cert.gov/control_systems/ics-cert/.

56. —. Control Systems Security Program: Industrial Control Systems Joint Working Group. [Online] http://www.us-cert.gov/control_systems/icsjwg/index.html.

57. **Huntington, Guy.** *NERC CIP's and identity management.* Huntington Ventures Ltd. 2009.

58. **American Petroleum Institute (API) energy.** *API Standard 1164. Pipeline SCADA Security.* American Petroleum Institute. 2009.

59. **Institute of Electrical and Electronics Engineers (IEEE).** *Transmission & Distribution Exposition & Conference 2008 IEEE PES : powering toward the future.* Institute of Electrical and Electronics Engineers. 2008.

60. **United States Nuclear Regulatory Commission.** *Regulatory Guide 5.71: Cyber security programs for nuclear facilities.* 2010.

61. **Web application Security Consortium.** Web Application Firewall Evaluation Criteria. [Online] 2009. http://projects.webappsec.org/w/page/13246985/Web Application Firewall Evaluation Criteria.

62. **Masica, Ken.** *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.* 2007.

63. —. *Securing WLANs using 802.11i. Draft. Recommended Practice.* 2007.

64. **Ginter, Andrew.** *An Analysis of Whitelisting Security Solutions and Their Applicability in Control Systems.* 2010.

65. **North American Electric Reliability Corporation (NERC).** *CIP-001-1a: Sabotage Reporting.* North American Electric Reliability Corporation. 2010.

66. **National Institute of Standards and Technology (NIST).** *NISTIR 7176: System Protection Profile - Industrial Control Systems.* Decisive Analytics. 2004.

67. **North American Electric Reliability Corporation (NERC).** *CIP-004-4: Cyber Security — Personnel and Training.* North American Electric Reliability Corporation. 2011.

68. —. *CIP-005-4: Cyber Security — Electronic Security Perimeter(s).* North American Electric Reliability Corporation. 2011.

69. —. *CIP-006-4: Cyber Security — Physical Security.* North American Electric Reliability Corporation. 2011.

70. —. *CIP-007-4: Cyber Security — Systems Security Management.* North American Electric Reliability Corporation. 2011.

71. —. *CIP-008-4: Cyber Security — Incident Reporting and Response Planning.* North American Electric Reliability Corporation. 2011.

72. —. *CIP-009-4: Cyber Security — Recovery Plans for Critical Cyber Assets.* North American Electric Reliability Corporation (NERC). 2011.

73. —. *Categorizing Cyber Systems. An Approach Based on BES Reliability Functions. Cyber Security Standards Drafting Team for Project 2008-06 Cyber Security Order 706.* 2009.

74. *Security of Industrial Control Systems, What to Look For.* **Zwan, Erwin van der.** 2010, ISACA Journal Online.

75. **Weiss, Joseph.** *Protecting Industrial Control Systems from Electronic Threats.* s.l. : Momentum Press, 2010.

76. **Smith, Steven S.** *The SCADA Security Challenge: The Race Is On.* 2006.

77. **International Organization for Standardization (ISO), International Electrotechnical Commission (IEC).** *Information technology — Security techniques — Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission. 2005.

78. **Holstein, Dennis Cease, Li, Haiyu L and Meneses, Albertin,.** *The Impact of Implementing Cyber Security Requirements using IEC 61850.* 2010.

79. **Holstein, Dennis K.** *P1711 "The state of closure".* s.l. : PES/PSSC Working Group C6, 2008.

80. **Goméz, J. Antonio.** *III Curso de verano AMETIC-UPM 2011 hacia un mundo digital: las e-TIC motor de los cambios sociales, económicos y culturales.* 2011.

81. **Glöckler, Oszvald.** IAEA Coordinated Research Project (CRP) on Cybersecurity of Digital I&C Systems in NPPs. [Online] 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/meetings/2011-05-TWG-NPPIC/Day-3.Thursday/TWG-CyberSec-O.Glockler-2011.pdf.

82. **Ericsson, Göran.** *Managing Information Security in an Electric Utility.* Cigré Joint Working Group (JWG) D2/B3/C2-01.

83. **Berkeley III, Alfred R. and Wallace, Mike.** *A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council.* s.l. : National Infrastructure Advisory Council, 2010.

84. **Asad, Mohammad.** Challenges of SCADA. [Online] http://www.ceia.seecs.nust.edu.pk/pdfs/Challenges_of_SCADA.pdf.

85. **Amin, Saurabh, Sastry, Shankar and Cárdenas, Alvaro A.** *Research Challenges for the Security of Control Systems.* 2008.

86. **ZigBee.** ZigBee Home Automation Overview. [Online] http://www.zigbee.org/Standards/ZigBeeHomeAutomation/Overview.aspx.

87. **The 451 Group.** *The adversary: APTs and adaptive persistent adversaries.* 2010.

88. **SANS.** The 2011 Asia Pacific SCADA and Process Control Summit - Event-At-A-Glance. [Online] 2011. http://www.sans.org/sydney-scada-2011.

89. **ESCoRTS Project.** *Survey on existing methods, guidelines and procedures.* 2009.

90. **American Petroleum Institute (API) energy.** *Security Guidelines for the Petroleum Industry.* American Petroleum Institute. 2005.

91. **Technical Support Working Group (TSWG).** *Securing Your SCADA and Industrial Control Systems.* Departmet of Homeland Security. 2005.

92. **SANS.** SCADA Security Advanced Training. [Online] 1989. http://www.sans.org/security-training/scada-security-advanced-training-1457-mid.

93. **Water Sector Coordinating Council Cyber Security Working Group.** Roadmap to Secure Control Systems in the Water Sector. 2008.

94. **Department of Homeland Security (DHS).** Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. 2009.

95. **International Instruments Users' Association (WIB).** *Process control domain - Security requirements for vendors.* EWE (EI, WIB, EXERA). 2010.

96. **Centre for the Protection of National Infrastructure (CPNI).** *Process control and SCADA security. Guide 6. Engage projects.* Centre for the Protection of National Infrastructure.

97. —. *Process control and SCADA security. Guide 4. Improve awareness and skills.* Centre for the Protection of National Infrastructure.

98. —. *Process control and SCADA security. Guide 3. Establish response capabilities.* Centre for the Protection of National Infrastructure.

99. —. *Process control and SCADA security. Guide 2. Implement secure architecture.* Centre for the Protection of National Infrastructure.

100. —. *Process control and SCADA security. Guide 1. Understand the business risk.* Centre for the Protection of National Infrastructure.

101. —. *Process control and SCADA security.* Centre for the Protection of National Infrastructure.

102. **Norwegian Oil Industry Association (OLF).** *OLF Guideline No.110: Implementation of information security in PCSS/ICT systems during the engineering, procurement and commissioning phases.* Norwegian Oil Industry Association. 2006.

103. **National Institute of Standards and Technology (NIST).** *NISTIR 7628: Guidelines for Smart Grid Cyber Security.* Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

104. **Centre for the Protection of Critial Infrastructure (CPNI).** Meridian Process Control Security Information Exchange (MPCSIE). [Online] http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie.

105. **Meridian.** Meridian. [Online] http://www.meridian2007.org.

106. **International Society of Automation (ISA).** LISTSERV 15.5 - ISA67-16WG5. [Online] http://www.isa-online.org/cgi-bin/wa.exe?A0=ISA67-16WG5.

107. **INTERSECTION Project.** INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks (INTERSECTION). [Online] 2008. http://www.intersection-project.eu.

108. **Norwegian Oil Industry Association (OLF).** *Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems.* Norwegian Oil Industry Association. 2009.

109. **International Federation for Information Processing (IFIP).** IFIP WG 1.7 Home Page. [Online] http://www.dsi.unive.it/~focardi/IFIPWG1_7.

110. **Institute of Electrical and Electronics Engineers (IEEE).** *IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities.* 2007.

111. —. IEEE Power & Energy Society. [Online] http://www.ieee-pes.org.

112. **International Electrotechnical Commission (IEC).** *IEC TS 62351-6: Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850.* International Electrotechnical Commission. 2007.

113. —. *IEC TS 62351-5: Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives.* International Electrotechnical Commission. 2009.

114. —. *IEC TS 62351-4: Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS.* International Electrotechnical Commission. 2007.

115. —. *IEC TS 62351-3: Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP.* International Electrotechnical Commission. 2007.

116. —. *IEC TS 62351-2: Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms.* International Electrotechnical Commission. 2008.

117. —. *IEC 61850-7-2: Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI).* International Electrotechnical Commission. 2010.

118. **international Atomic Energy Agency (IAEA).** IAEA Technical Meeting on Newly Arising Threats in Cybersecurity of Nuclear Facilities. [Online] 2011. http://www.iaea.org/NuclearPower/Downloads/Engineering/files/InfoSheet-CybersecurityTM-May-2011.pdf.

119. **National Infrastructure Security Coordination Centre (NISCC).** *Good Practice Guide Process Control and SCADA Security.* PA Consulting Group. 2006.

120. —. *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* British Columbia Institute of Technology (BCIT). 2005.

121. —. *Firewall deployment for scada and process control networks. good practice guide.* National Infrastructure Security Coordination Centre. 2005.

122. **eSEC.** eSEC. *Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza.* [Online] http://www.idi.aetic.es/esec.

123. **Department of Energy (DoE).** *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities.* Department of Energy. 2002.

124. **Department of Homeland Security (DHS).** *Cyber storm III Final Report.* Department of Homeland Security Office of Cybersecurity and Communications National Cyber Security Division. 2011.

125. **Centre for the Protection of Critical Infrastructure (CPNI).** CPNI. [Online] http://www.cpni.gov.uk/advice/infosec/business-systems/scada.

126. **Interstate Natural Gas Association of America (INGAA).** *Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry.* Interstate Natural Gas Association of America. 2011.

127. **North American Electric Reliability Corporation (NERC).** *CIP-002-4: Cyber Security — Critical Cyber Asset Identification.* North American Electric Reliability Corporation. 2011.

128. **Department of Homeland Security (DHS).** *Catalog of Control Systems Security: Recommendations for Standards Developers.* 2009.

129. **American National Standard (ANSI).** *ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems.* International Society of Automation (ISA). 2007.

130. —. *ANSI/ISA–99.02.01–2009 Security for Industrial Automation and Control Systems. Part 2: Establishing an Industrial Automation and Control Systems Security Program.* International Society of Automation (ISA). 2009.

131. **Department of Energy (DoE).** *21 Steps to Improve Cyber Security of SCADA Networks.* Department of Energy.

132. **Institute of Electrical and Electronics Engineers (IEEE).** *WGC1 - Application of Computer-Based Systems.* http://standards.ieee.org/develop/wg/WGC1.html.

133. —. *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

134. —. *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

135. —. IEEE PES Computer and Analytical Methods SubCommittee. [Online] 2000. http://ewh.ieee.org/cmte/psace/CAMS_taskforce.html.

136. **Norwegian Oil Industry Association (OLF).** *OLF Guideline No. 104: Information Security Baseline Requirements for Process.* Norwegian Oil Industry Association. 2006.

137. **International Federation of Automatic Control (IFAC).** TC 3.1. Computers for Control — IFAC TC Websites. [Online] http://tc.ifac-control.org/3/1.

138. —. TC 6.3. Power Plants and Power Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/6/3.

139. —. Working Group 3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/5/4/working-groups/copy2_of_working-group-1-decentralized-control-of-large-scale-systems.

140. **International Federation for Information Processing (IFIP).** IFIP TC 8 International Workshop on Information Systems Security Research. [Online] http://ifip.byu.edu.

141. —. IFIP Technical Committees. [Online] http://ifiptc.org/?tc=tc11.

142. **Department of Energy (DoE).** Cybersecurity for Energy Delivery Systems Peer Review. [Online] 2010. http://events.energetics.com/CSEDSPeerReview2010.

143. —. Control Systems Security Publications Library. [Online] http://energy.gov/oe/control-systems-security-publications-library.

144. **Open Smart Grid.** Open Smart Grid. [Online] http://osgug.ucaiug.org/default.aspx.

145. **Smart Grid Interoperability Panel (SGIP).** SGIP Cyber Security Working Group (SGIP CSWG). [Online] http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG.

146. **Theriault, Marlene and Heney, William.** *Oracle Security.* First Edition. s.l. : O'Reilly, 1998. p. 446. 1-56592-450-9.

147. **Rijksoverheid.** Scenario's Nationale Risicobeoordeling 2008/2009. [Online] 2009. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/21/scenario-s-nationale-risicobeoordeling-2008-2009.html.

148. **Energiened.** Energiened Documentation. [Online] http://www.energiened.nl/Content/Publications/Publications.aspx.

3 Abbreviations

ACC	American Chemistry Council
AD	Active Directory
AGA	American Gas Association
AMETIC	Multi-Sector Partnership Of Companies In The Electronics, Information And Communications Technology, Telecommunications And Digital Content
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programming Interface
API	American Petroleum Institute
ARECI	Availability And Robustness Of Electronic Communication Infrastructures
ARP	Address Resolution Protocol
AV	Anti-Virus
BDEW	Bundesverband Der Energie Und Wasserwirtschaft
BGW	Bundesverband Der Deutschen Gas Und Wasserwirtschaft
BW	Band Width
CA	Certified Authority
CC	Common Criteria
CCTV	Closed-Circuit Television
CEN	European Committee For Standardization
CENELEC	European Committee For Electrotechnical Standardization
CERT	Computer Emergency Response Team
CFR	Code Of Federal Regulations
CI	Critical Infrastructure
CI2RCO	Critical Information Infrastructure Research Coordination
CIFS	Common Internet File System
CIGRE	Conseil International Des Grands Réseaux Électriques
CII	Critical Information Infrastructures
CIIP	Critical Information Infrastructures Protection
CIKR	Critical Infrastructure And Key Resources
CIP	Critical Infrastructures Protection
CIWIN	Critical Infrastructure Warning Information Network
CNPIC	Centro Nacional Para La Protección De Infraestructuras Críticas
COTS	Commercial Off-The-Shelf
CPNI	Centre For The Protection Of National Infrastructures
CRP	Coordinated Research Project
CRUTIAL	Critical Utility Infrastructural Resilience
CSSP	Control Systems Security Program
DCS	Distributed Control Systems
DD	Data Diode
DDOS	Distributed Denial-Of-Service Attack
DHS	Department Of Homeland Security

DLP	Data Loss (Or Leak) Prevention (Or Protection)
DLP	Data-Leakage Prevention
DMZ	Demilitarized Zone
DNP	Distributed Network Protocol
DNS	Domain Name Server
DOE	Department Of Energy
DOS	Denial Of Service
DPI	Deep Packet Inspection
DSO	Distribution System Operator
EC	European Commission
ECI	European Critical Infrastructure
ELECTRA	Electrical, Electronics And Communications Trade Association.
ENISA	European Network And Information Security Agency
EO	Executive Orders
EPA	Environmental Protection Agency
EPCIP	European Programme For Critical Infrastructures Protection
ERA	European Research Area
ESCORTS	Security Of Control And Real Time Systems
E-SCSIE	European Scada And Control Systems Information Exchange
EU	European Union
EXERA	Association Des Exploitants D'equipements De Mesure, De Régulation Et D'automatisme
FDAD	Full Digital Arts Display
FIPS	Federal Information Processing Standard
FP	Framework Programme
FTP	File Transfer Protocol
GIPIC	Grupo De Trabajo Informal Sobre Protección De Infraestructuras Críticas
GP	Good Practices
GPS	Global Position System
GUI	Graphical User Interface
HIPS	Host Intrusion Prevention System
HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
HW	Hardware
I&C	Instrumentation And Control
IAEA	International Atomic Energy Agency
IAM	Identity And Access Management
IAONA	Industrial Automation Open Networking Association
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control Systems
ICSJWG	Industrial Control Systems Joint Working Group
ICT	Information And Communications Technology
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IFAC	International Federation Of Automatic Control.
IFIP	International Federation For Information Processing
IMG-S	Integrated Management Group For Security
INL	Idaho National Laboratory
INSPIRE	Increasing Security And Protection Through Infrastructure Resilience
INTER-SECTION	Infrastructure For Heterogeneous, Resilient, Secure, Complex, Tightly Inter-Operating Networks
IO	Input/Output
IPS	Intrusion Protection System
IPSEC	Internet Protocol Security
IRBC	Ict Readiness For Business Continuity Program
IRIIS	Integrated Risk Reduction Of Information-Based Infrastructure Systems
ISA	Instrumentation, Systems And Automation Society
ISACA	Information Systems Audit And Control Association
ISBR	Information Security Baseline Requirements
ISMS	Information Security Management System
ISO	International Organization For Standardization
IST	Information Society Technologies
IT	Information Technologies
JHA	Justice And Home Affairs
KF	Key Finding
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPDE	Low Density Polyethyl
MAC	Media Access Control
MCM	Maintenance Cryptographic Modules
MIT	Middleware Improved Technology
MSB	Swedish Civil Contingencies Agency
MTU	Master Terminal Unit
NAC	Network Access Control
NBA	Network Behaviour Analysis
NBA	Network Behaviour Analysis
NCI	National Critical Infrastructure
NCS	Norwegian Continental Shelf
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NHO	Norwegian Business And Industry
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan

NIS	Network And Information Security
NISCC	National Infrastructure Security Co-Ordination Centre
NIST	National Institute For Standard And Technologies
NISTIR	National Institute Of Standards And Technology Interagency Report
NRC	Nuclear Regulatory Commission
NRG	Nuclear Regulatory Guide
NSAC	National Security Advice Centre
OLF	Norwegian Oil Industry Association
OPC	Ole For Process Control
OS	Operating System
OSG	Open Smart Grid
OSI	Open System Interconnection
OTP	One Time Password
PCCIP	Presidential Commission On Critical Infrastructure Protection
PCD	Process Control Domains
PCN	Process Control Networks
PCS	Process Control System
PCSRF	Process Control Security Requirements Forum
PDCA	Plan, Do, Check, Act
PDD	Presidential Decision Directive
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PP	Protection Profiles
PPP	Public Private Partnerships
QOS	Quality Of Service
R&D	Research And Development
RAT	Remote Administration Tools
RF	Radio Frequency
RSS	Really Simple Syndication
RTU	Remote Terminal Units
SANS	System Administration, Networking, And Security Institute
SCADA	Supervisory Control And Data Acquisition
SEM	Security Event Manager
SEMA	Swedish Emergency Management Agency
SIEM	Security Information And Event Management
SIM	Security Information Management
SIMCIP	Simulation For Critical Infrastructure Protection
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier

SSL	Secure Sockets Lay
SSP	Sector-Specific Plan
ST	Security Targets
SW	Software
TCG	Trusted Computing Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TISP	The Infrastructure Security Partnership
TKIP	Temporal Key Integrity Protocol
TOE	Target Of Evaluation
TR	Technical Report
TSWG	Technical Support Working Group
UDP	User Datagram Protocol
UK	United Kingdom
USA	United States Of America
VDI	The Association Of German Engineers
VDN	Verband Der Netzbetreiber
VIKING	Vital Infrastructure, Networks, Information And Control Systems Management
VPN	Virtual Private Network
VRE	Verband Der Verbundunternehmen Und Regionalen Energieversorger In Deutschland
WAF	Web Application Firewall
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIB	International Instruments Users' Association
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web