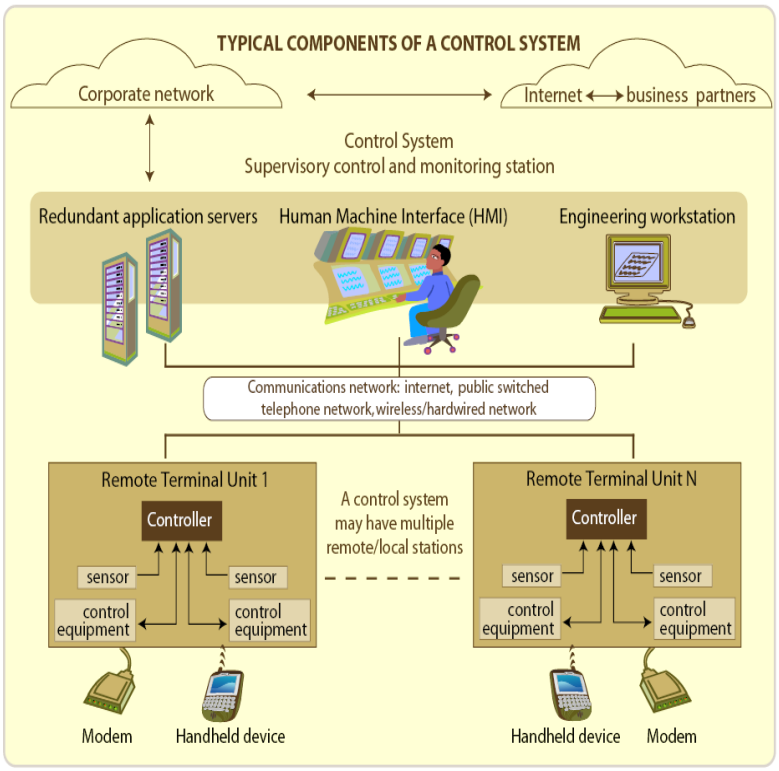
JRC Scientific and Technical Reports

Towards Standardisation Measures to Support the Security of Control and Real-Time Systems for Energy Critical Infrastructures

Alberto Stefanini , Marcelo Masera



EUR 23538 EN - 2008

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the IPSC is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: TP 210 I-21020 Ispra (VA)
E-mail: marcelo.masera@jrc.ec.europa.eu
Tel.: +39.0332.789238
Fax: +39.0332.789576
http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 48180
EUR 23538 EN
ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

Towards Standardisation Measures to Support the Security of Control and Real-Time Systems for Energy Critical Infrastructures

Alberto Stefanini*, Marcelo Masera
Institute for the Protection and Security of the Citizen
Joint Research Centre of the European Commission

*Contract Agent, November 2005 – November 2008

Table of Contents

Abstract

This report outlines the context for control and real time systems vulnerability in the energy sector, their role in energy critical infrastructures and their emerging vulnerabilities as they were put in light by some recent episodes. Then it provides a survey on the current efforts to set up reference frameworks addressing the broad issue of supervisory and control systems security. It discusses the role of standards and outlines the reference approaches in that respect. The current attitude of Europe towards the issue of control systems security is discussed and compared with the US situation, based on a stakeholder consultation, and gaps and challenges are outlined. A set of recommendations for policy measures to address the issue is given.

1 Introduction

Networked computers reside at the heart of critical infrastructures and systems on which people rely, such as the power grid, the oil & gas infrastructure and power, oil and chemical process plants. Today, many of these systems are far too vulnerable to cyber attacks that can inhibit their operation, corrupt valuable data, or expose business private information. These vulnerabilities occur in a landscape where industrial systems are highly connected and highly interdependent, within regions and countries and also among countries. Liberalisation of markets, cross-border links, corporate consolidation, industry rationalization, efficient business practices such as just-in-time manufacturing and population concentration in urban areas have all contributed to this situation.

Pressure to ensure cyber security of control and communication systems is very strong in the US, where there is a pungent push from the US government and an influential awareness by the main stakeholders, resulting for instance in the implementation of national facilities where to test the security of control and communication components.

Until now EU industry awareness and readiness have lagged behind, although the feeling that the issue is becoming crucial is now growing. However, few investments are actually made to update and improve security of existing applications, to the effect that EU manufacturers and operators currently need to resort to US cyber security facilities to test their products and services.

Security of the information and communication technologies (ICT) employed in process control systems is a relatively new issue that has emerged in the last few years. It has acquired a critical role for the reliability of power systems especially, with the increment of their interconnectivity (within the production installations, between production and business, and among companies) and the pervasive use of ICT solutions [Stefanini et al., 2005]. Most of the technologies used for control systems have shifted towards the adoption of hardware and software components used in general-purpose computation and communication (e.g. operating systems, TCP/IP protocols, etc.). While taking advantage of the technical possibilities provided by the new ICT, energy systems have inherited dangerous vulnerabilities. In addition, the economic benefits deriving from the adoption of standardized technologies accelerate the implementation of control systems and related communications without any guarantee of secure operation.

Vulnerabilities due to design and technology flaws may be exploited by malicious antagonist actors, who can gain access to the systems through external and internal connections. These threats menace industry in the whole energy industrial spectrum, as their control systems are based on similar technologies and are deployed using analogous architectures. Standards might help in the protection of control systems in different ways:

- Helping in setting a common conceptual basis between all stakeholders: operators, vendors, certifiers, authorities, etc.

- Supporting all engineering processes: from specification to procurement, and from operation to maintenance.
- Fostering the development of a market for security products and services, with verifiable levels of assurance.

However, there is a time gap between the availability of standards and their application. The current efforts to consider security in supervisory and control systems standards are too recent for being sure about their effectiveness. In the meantime the energy sector will continue deploying control systems. This opens a negative window of opportunity of several years for cyber attacks and failures.

There is therefore the risk that standards will arrive too late: when some important accidents will have happened, and when non-standard and incompatible solutions will be in use. Furthermore, as information and communication systems are at the core of the interconnections among the different actors of the energy sector, the delay in the availability of effective standards is by itself another vulnerability: the near future will see a great window of opportunity for incidents related to intentional exploitation of this vulnerability.

This report provides an overview of the context where supervisory and control systems are used, critical networked infrastructure, by making specific reference to power systems. Operation of the power infrastructure substantially depends so tightly on its information and control system (ICS) that any major failure of the ICS may cause extensive service disruption and even massive energy supply interruptions (as for instance wide-ranging power blackouts). Chapter 2 provides a view of the ICS in this context and analyses their crucial role for system operation. Several recent episodes are reported that confirm that ICS are both critical and vulnerable. Chapter 3 discusses the role of standards addressing the broad issue of supervisory and control systems security, provides a survey on the current efforts to achieve such standards and outlines the reference approaches in that respect. The current attitude of Europe towards the issue of control systems security is discussed in chapter 4 and compared with the US situation, based on a stakeholder consultation, and gaps and challenges are outlined. Finally, in chapter 5 a set of recommendations for policy measures to address the issue is given.

2 SCADA vulnerability: context outline

As discussed by Gheorghe, Masera et al. [2006] networked infrastructures, and in particular the power systems, have been fundamentally changed by the way they are controlled and monitored. One of the main factors behind this evolution is the pervasive and intensive use of information and communication systems.

The application of electronic technologies to power systems began as soon as those technologies were available, because they appeared as an effective means for implementing control and protection mechanisms. The massive incorporation of digital solutions has deeply changed the same functionality of power systems. From the late 90s on, companies and national infrastructures become fully digitalized. Taking as an example the evolution of the electricity systems in Europe, it is possible to appreciate how their unbundling and interconnectedness wouldn't have been possible without the parallel application of ICS. Within each country, the application of the regulations over the infrastructure depends on the flow of information between actors: be it the application of connectivity rules or tariffs, electricity and information go together. Data flows grow profusely between the industrial and the business sides of companies. Energy markets function on line. The vast interconnection among national grids is not just accompanied but enabled by ICS. Sensors and actuators can be reached through a variety of communication means. On the other hand, the pervasiveness of information allows new functions across systems.

The use of ICS has two sides: on the one side it provides new means for improving the operational and monitoring capabilities, but on the other it opens dangerous opportunities to cyber threats. Industrial

automation and control systems operate in a complex business environment. Organizations are increasingly sharing information with the industrial community, and partners in one business venture may be competitors in another venture. However, because industrial automation and control systems equipment connects directly to a process, loss of trade secrets and interruption in the flow of information are not the only consequences of a security breach. The potential loss of production, environmental damage, regulatory violation, and compromise to operational safety are far more serious consequences. In addition, safety and environmental effects may have ramifications beyond the targeted company; it may grievously damage the infrastructure of the host region or nation.

External threats are not the only concern; knowledgeable insiders with malicious intent or even an innocent unintended act can pose serious security risk. Additionally, industrial automation and control systems are often integrated with other business systems. Modifying or testing operational systems has led to unintended electronic effects on system operations. Personnel from outside the control systems area increasingly perform security testing on the systems, exacerbating the number and consequence of these effects. Combining all these factors, it is easy to see that the probability of someone gaining unauthorized access to an industrial process is not minor.

Although technology changes and electronic communications with partners may be good for business, they increase the potential risk of compromising security. As the threats to businesses increase, so does the need for security. Also, network-shaped, highly distributed infrastructures have to take into consideration a greater diversity of threats than single systems. For instance, in addition to local technical faults, human errors and natural disasters, one has to add systemic failures emerging from the composite topological and organisational structure of the infrastructure. Moreover, as typically infrastructural networks are geographically distributed, natural forces might affect them due to the accumulation of dispersed events; and due to the relevance of infrastructures to national security, deliberate attacks take a new and important significance. For instance, threats against the power system are also growing from the point of view of its adequacy: demand is always growing, and, although this growth may be forecast, it cannot be anytime easily faced, also because the public often contrasts construction of new power generating plants and transmission lines. Interconnections among national power systems have been developed in the past 50 years so as to ensure mutual assistance between national subsystems by allowing exchanges between these systems. Today's market development with its high level of cross-border exchanges was out of the scope of the original system design. Transactions increase, following electrical system liberalisation, and this involves operating the whole infrastructure closer to security limits. To emphasise this evolving mismatch, Gheorghe, Masera et al. [2006] argue that this discrepancy between the physical infrastructure and the requirements put to its operation has brought the system in a condition of "evolutionary unsuitability".

2.1 Current Industrial Control Systems and their vulnerabilities

Industrial control systems have evolved from individual, isolated computers with proprietary operating systems and networks to interconnected systems and applications employing widely used and well understood "open systems" technology (i.e., operating systems and protocols). As stated in ISA [2007] '*these systems are now being integrated with enterprise systems and other business applications through site and corporate communication networks. This integrated architecture provides significant business benefits including:*

- *Increased visibility of the production process and the manufacturing system from the business level (work in process, equipment status, production schedules)*
- *More direct access to enterprise information, enabling a more responsive manufacturing enterprise*
- *Common interfaces that reduce overall support costs and permit remote support of production processes'*

Concerning power production, integration also allows establish direct links among the production environment the market and the regulators thus allowing power plant management to quickly adapt to market fluctuations and environmental conditions.

However, integration and openness brings about more security risks: the increase in malicious attacks on business systems is an unremitting trend... While industrial control systems are moving toward COTS and are interconnecting wih business networks. they become potentially susceptible to the same software attacks. Also, the dramatic increase in 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 that have to contribute to common security issues. Collaboration ranges from sharing of information about vulnerabilities, to cooperation in emergency situations. Nowadays there is evidence that cyber criminals and cyber terrorists have more resources and knowledge to attack industrial automation and control systems. Potential consequences of these attacks have broadened as more systems are interconnected, within and among companies. According to ISA [2007] '*this shift requires more structured guidelines and procedures to define electronic security applicable to industrial automation and control systems, as well as the respective connectivity to other systems'*.

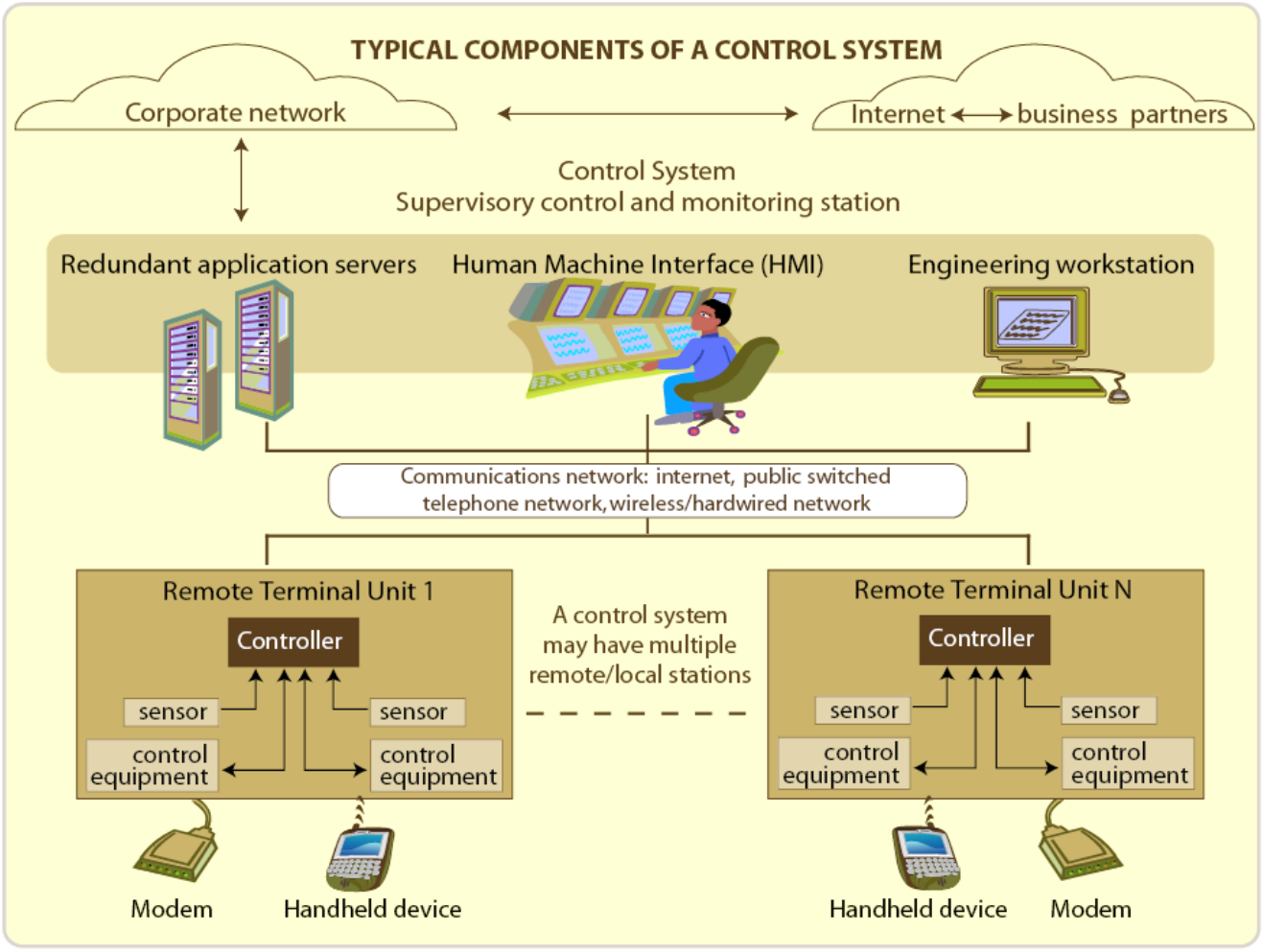


Figure 1 - Industrial Control System

2.2 Potential Impact of Control Systems vulnerability

Supervisory Control and Data Acquisition systems (SCADA for short)[1] are used all over the continuous process sectors to control critical networked infrastructures like the power grid, the oil & gas infrastructure, and large and complex plants, e.g. power, oil and chemicals. Similar systems are also employed to control discrete manufacturing processes, e.g. automotive, aircraft etc. The impact of disruption of several such systems and processes on the society may be paramount, as shown by a number of recent accidents. For instance, crucial economic and social functions depend on the security, adequacy, and quality of electricity supply. Overall the vulnerability of the European electrical infrastructure appears to be growing due to several factors [Eurelectric 2004]:

- demand is always growing, and, although this growth may be forecast, it cannot be easily faced anytime;
- after liberalisation, electricity transactions increased and became more hectic, so as to force operators to operate the whole infrastructure closer to capacity limits;
- critical infrastructures become highly interconnected with other networked systems and the potential for devastating effects on vital services can create attractive targets for malicious activity, including terrorism.

The impact of a major failure or a well targeted and successful attack on the electrical system (physical as well as presumed cyber attack) could be a major regional or national blackout possibly with cross-border ramifications. In recent years, both Europe and America have experienced a significant number of major blackouts, namely:

- August 14, 2003 – North East blackout over the US and Canada;
- August 28, 2003 - Southern London distribution;
- September 23, 2003 - Danish/Swedish blackout;
- September 28, 2003 - Italian electricity transport grid collapse;
- Nov. 4, 2006 - A serious incident on the continental European electricity network lead to massive service disruption in many portions of the EU grid.

Inadequacy and/or malfunction of communication and control equipment played a major role in all these events, and contributed to highlight the criticality of such systems [Stefanini et al., 2005]. Based on known facts and publicly available investigation reports, these blackouts were not caused by malicious attacks but nevertheless the current international scene calls for increased vigilance for the malicious risk factor. In fact, malicious attacks caused significant damage in other outstanding process plants, e.g.:

- The pipeline rupture occurred on June 10, 1999, which released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington [NTSB, 2002]. Subsequent ignition of the gasoline caused three deads and many injuries. The investigation by the US National Transportation Safety Board pointed out as a main cause of the event the poor performance and security of the operating company's supervisory control and data acquisition system.
- The infection of the Slammer worm in ICT systems of the Davis-Besse nuclear plant, January 2003 [Security Focus, 2003]. The worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for

[1] Although the acronym SCADA is extensively used in most process control sectors, power generation usually prefers to denote supervisory control and monitoring stations as EMS – Energy Management Systems.

nearly five hours, despite a belief by plant personnel that the network was protected by a firewall.

- The case of the disgruntled employee of an Australian sewer control plant, March 2000 who decided to seek revenge after being turned down for reemployment, and caused spillage of 264,000 gallons of sewage into waterways [Pipeline & Gas Journal, 2007].

Such events increased considerably since 2000. Although most of them are not reported for secrecy reasons, the rate of known facts appeared to exponentially increase in the period 2000-2006. Vulnerabilities due to design and technology flaws may be exploited by malicious antagonist actors, who can gain access to the systems through external and internal connections. The Denial of Service attacks against Estonia during April 2007 have shown the extent of the damage that organised cyber warfare may inflict on the global economy [Wikipedia 2007].

These threats menace industry in the whole industrial process spectrum, as their supervisory control and data acquisition systems are based on similar technologies and are deployed using analogous architectures.

Specifically concerning power systems, three recent episodes are especially worth reporting:

- Researchers at the Idaho's National Laboratory launched an experimental cyber attack and caused a generator to self-destruct, alarming the federal government and electrical industry about what might happen if such an attack were carried out on a larger scale. The experiment confirms that large electric systems are vulnerable to cyber attacks [CNN 2007]. This article outlines the potential social and economic impact of large and well orchestrated cyber attacks against critical infrastructures and argues that their effect could last for long time, e.g. up to 2-3 months.
- In a rare public warning to the power and utility industry, a CIA analyst said that cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities [Washington Post, 2008a]. The CIA analyst was speaking at a trade Conference in New Orleans attended by representatives of US and international security officials from the government and from power, oil and gas companies. The speaker reported that the CIA suspects the attackers to have profited on inside knowledge. Comments on the press outline that seldom the CIA goes public, unless threats are very large, and that cyber crime had a huge increase, especially against infrastructure networks.
- A nuclear power plant in Georgia was forced into an emergency shutdown for 48 hours after a software update was installed. The incident occurred on March 7, 2008 on the Hatch nuclear power plant near Baxley, Georgia. [Washington Post, 2008b]. The trouble started after a software update was installed on a computer operating on the plant's business network. The computer was used to monitor chemical and diagnostic data from one of the plant control systems, and the software update was to synchronize data on both systems. When the updated computer rebooted, it reset data on the control system, causing safety systems to interpret the lack of data as a drop in water reservoirs of the plant cooling system.

Figure 2 - A staged cyber attack against a power generator, March 2007 (from http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html)

3 Standardisation efforts

3.1 Main organizations concerned

CEN (European Committee for Standardization)

CEN was founded in 1961 by the national standards bodies in the European Economic Community and EFTA countries. Now CEN is contributing to the objectives of the European Union and the European Economic Area with voluntary technical standards which promote free trade, the safety of workers and consumers, interoperability of networks, environmental protection, exploitation of research and development programmes, and public procurement.

FERC – The US Federal Energy Regulatory Commission

FERC regulates and oversees the US energy industries in the economic, environmental, and safety interests of the American public. By mid 2003, FERC proposed adoption of new reliability standards for cyber security in the bulk power system. In January 2008 FERC approved eight new mandatory reliability guidelines focusing on cyber security proposed by NERC.

ISO (International Organization for Standardization)

ISO is a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented

worldwide. Hence in most cases ISO standards set a reference framework across a wide range of industrial and business sectors, like the ISO 15408, the Common Criteria.

ISA—Instrumentation, Systems and Automation Society (ISA)

ISA is an organization of engineers, technicians, and others who work in the field of instrumentation, measurement, and control of industrial processes. ISA has formed Standards and Practices Committee SP 99 with the express intent of developing guidance to help stakeholders provide secure Manufacturing and Control Systems that are not vulnerable to electronic or network based intrusion and failures. ISA committee membership is encouraged to provide representative expertise from the user, supplier, and academic communities.

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology is a US federal technology agency that develops and promotes measurement, standards, and technology. The Process Control Security Requirements Forum (PCSRF) was developed by NIST with the goal of sharing information in this area and developing standards that will provide secure Manufacturing and Control Systems. It provides another means of information sharing and a group to work with that is interested in developing standards.

North American Electric Reliability Council (NERC)

The North American Electric Reliability Corporation's mission is to ensure the reliability of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards and monitors users, owners, and operators for preparedness. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. NERC provides several industry information sharing services and programs for the Electric Utility Industry. In their Critical Infrastructure protection programme they proposed a first cybersecurity standard with minim requirements (Standard 1200) and then developed a more detailed standard (CIP-002-1 through CIP-009-1 Cyber Security Standards - formerly 1300), together with a set of security guidelines for the power sector that covers both physical and cyber aspects.

Chemical Industry Data Exchange (CIDX)

CIDX is a trade association whose mission is to improve ease and speed of electronic business between chemical companies and their trading partners. CIDX has recently formed a business unit devoted to the subject of cyber security in the Chemical industry. This group will promote education, adoption of standards, and technology development.

Institute of Electrical and Electronics Engineers (IEEE)

IEEE is the world's leading professional association for the advancement of technology. The IEEE name was originally an acronym for the Institute of Electrical and Electronics Engineers. Today, the organization's scope of interest has expanded into so many related fields, that it is simply referred to by the letters IEEE. Several societies of IEEE deal with subjects relevant for the security of SCADA systems: among them Power Engineering Society (PES), Computer Society, and Instrumentation and Measurement.

Several committees specifically address cyber security: for instance the PES Substation Committee, with the working group Working Group C3 - Electric Network Control Systems Standards.

International Electrotechnical Commission (IEC)

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts.

The IEC Technical Committee 57 prepares international standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA, distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. Within TC 57, Working Group 15 (Telecontrol) is addressing specifically cyber security of control centers and substation communications.

The IEC technical Committee 65 prepares international standards for systems and elements used for industrial-process measurement and control concerning continuous and batch processes. Recently, within IEC TC65, a specific working group - WG 10 - was established (October 2005) to address system security in a holistic way.

International Council on Large Electric Systems (CIGRE')

CIGRE' is a worldwide organisation covering technical, economic, environmental, organisational and regulatory aspects of electric power systems. Among its aims, they endeavour to synthesize state-of-the-art and world practices. Among their Study Committees, SC D2 deals with the Information and the Telecommunication systems required for operational and business activities. In particular, the Advisory Group D2.02 looks at Information systems and Internet, and it has formed a new Joint Working Group D2/B3/C2.01 "Security for Information Systems and Intranets in Electric Power Systems" (with B3 Substations, and C2 System Operation and Control). This working group has published a set of relevant reports [Dondossola and Lamquet, 2006].

Department of Energy National SCADA Test Bed Program

The US Department of Energy's has recognized the need for a National Laboratory-based SCADA test bed. Both Sandia National Laboratory and the Idaho National Engineering and Environmental Laboratory are involved in developing this national test bed with industry participation. The test bed will focus on identifying SCADA and process control system security vulnerabilities and then developing and validating solutions to improve the resilience of USA's critical infrastructures. The Test Bed program is now a Department of Homeland Security (DHS) unit. An overview of the US Test bed program is presented in Appendix 1 together with other related initiatives.

Process Control System Cyber Security Forum (PCSF)

This subscription forum was established to meet the complex, growing, and increasingly urgent security threats and vulnerabilities of process control systems. It is sponsored by the National Institute of Standards (NIST) and by the Department of Homeland Security. The forum brings together infrastructure industries, process control system vendors, services providers, government and regulatory stakeholders charged with protecting critical infrastructures and other industries reliant on networked process control systems. The forum relies on a collaborative, information-sharing environment to develop and share security solutions.

The PCSF roles in Manufacturing and Control Systems security include:

- Develop Protection Profiles for security features that new equipment will be built with
- Future solutions for new equipment and system installations
- System certification through independent testing, including security considerations in the specification, procurement, and assurance areas of the industrial process control systems life cycle
- Testbed to validate standards and to develop performance and conformance test methods.

3.2 General purpose applicable standards

ISO/IEC 27001(Information technology -- Security techniques -- Information security management systems – Requirements) is an information security management system standard published in October 2005, and it is part of a growing family of ISO/IEC standards, the ISO/IEC 27000 series. It is intended to be used in conjunction with ISO/IEC 27002, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement an information security management system in accordance with the best practice advice in ISO/IEC 27002 are likely simultaneously to meet the requirements of ISO/IEC 27001, but certification is entirely optional. The ISO 27000 series follows and is closely linked to ISO 17799, the Code of practice for information security management, and to ISO 15408, the Common Criteria.

ISO 17799, derived from the British Standard 7799 and produced by the ISO/IEC Joint Technical Committee 1, Subcommittee SC 27, in December 2000, provided a starting point for developing organization specific guidance arrangements. It is a *comprehensive set of controls comprising best practices in information security,* and comprises a code of practice and a specification for an information security management system. A corporation applying it will have to perform a risk assessment, prepare its security resources, and prepare the needed elements for certification and compliance. These will include the corporate security policy, and the functional and assurance requirements that have to be implemented. The standard provides a generic list of these requirements at a high level, independently from specific technologies. A fundamental point is the provision of appropriate security policies. A policy should set the direction for action and the commitment of the company to information security. Remaining at the management level, the application of this standard to industrial installations, mainly one with potential critical consequences, seem to merit a review, or at least a complement with particular considerations on, for instance, timing issues related to control applications. Security measures should be built into every system from the moment they are conceived. Security includes not only encryption, but also authentication, role-based access control, prevention of denial of services, monitoring and audit functions for the information infrastructure, and last, but by no means least, security policies that enforce and supplement the security measures [Cleveland, 2005].

The ISO 27001 essentially replaces the BS7799-2 standard, by enhancing its content and harmonizing with other standards (a scheme has been introduced by various certification bodies for conversion from BS7799 certification to ISO27001 certification). The objective of the ISO 27001 is to *"provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System"*. Its adoption is a strategic decision, because it involves a *"process which is influenced by the needs and objectives, the security requirements, …the size and structure of the organization"*. The standard defines its process approach as *"The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management"*. The ISO 27002 is the rename of the ISO 17799, and is a *code of practice for information security.* It outlines the hundreds of controls and control mechanisms which may be implemented subject to guidance provided within ISO 27001.

The ISO/IEC 15408, the Common Criteria for Information Technology Security Evaluation, is an international standard for computer security. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner, through. a framework where computer system users can specify their security requirements, vendors can implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. The Common Criteria were the result of long developments in the USA, Canada and European countries (the Netherlands, France, Germany, United Kingdom), and were aimed at supporting the specification of products with security requirements. First published in 1996, their second version was adopted by ISO as standard 15408 in 1998. The requirements to be defined are functional requirements, those related to desired security behaviours, and assurance requirements, which are the basis for gaining

confidence that the claimed security measures are effective and implemented correctly. The standard gives the possibility to select among seven evaluation assurance levels, which can be used for grouping components, or provide retrofit compatibility with existing products (first 4 levels), or develop specialised components.

This standard supports purchasers of products in the definition and formulation of the requirements they necessitate; vendors or developers in the specification of their products, and third party evaluators in the verification and validation of products. In this way, the whole procurement process is assisted with common terminology and procedures.

It is understandable that several approaches to the security of industrial control have taken the Common Criteria as reference. However it should be considered that this standard, although technically important, has not been heavily applied in the real world. Verifying technical products against a standard that comprises functional and assurance procedures is very costly. Some significant criticisms are that those evaluations do not seem to add value while entail notable costs, that they do not impact noteworthy on the reduction of vulnerabilities, that the engineering efforts could be better employed in other technical tasks related to security.

3.3 Industrial Control Initiatives

In the ISA the committee SP99 looks after Manufacturing and Control system *security* [Webb, 2002]. Their comprehensive approach [ISA 2005] includes:

- models, definitions and terminology;
- the analysis of risks and vulnerability;
- security programs;
- security requirements and controls.

So far ISA ISA99 published its Part 1 standard [ISA 2007] and is working on the Part 2 and Part 4 standards. There is of course no guarantee that the adopted terminology and methodology, although coherent and efficacious in their context, will not enter into conflict with other initiatives, namely:

- recently the NIST has issued an even broader approach, the NIST 800-53 [NIST 2007a], within their *Industrial Control System Security Project* and the concerned community is divided upon the respective merits of these two approaches.
- The IEC has produced two standards concerning process safety, the IEC 61508 and 61511. Further to these standards, the IEC Committee SC 65 A "Industrial-Process Measurement and Control - System Aspects" is striving to address the problem of functional safety in a systematic and general way. Also, the IEC recognized that internetworking has increased the exposure of automation systems to cyber attacks and established in October 2005 a specific working group (WG 10) within TC65 to specifically address system security

While TC 65 addresses system security in a general perspective, another working group of the IEC, TC 57, is targeting amendments to existing protocols for data communication in the power sector in view of strengthening their security. In this same perspective, IEEE has been producing some standards, such P1547 for “Interconnecting distributed resources with Electric Power Systems”, 1525 for substation automation, and 1379 for substation IED communication. The IEEE Substations Committee has the task force C0 TF1 that deals with Substation Data Security. An open question remains on the multiplicity of efforts for a sector that needs promptly answers.

The American Petroleum Institute has been working on cyber security guidelines documents and API 1164 is the first (published in 2004) dealing with SCADA security best practice. Its goal is to provide an easy to follow and rapid guide to industrial companies mainly in the pipeline sector – but their applicability is broader. There are no plans for third party certification or requirements on self-

certification. Although incomplete and not very sophisticated from the security viewpoint (for instance in the consideration of authentication and access control, links to security policies, etc.), it provides ready applicable and sound recommendations. It is therefore a straightforward, practical and undemanding effort that, if applied by industry, can have immediate effects. As a provisional action while waiting for more thorough measures, it is a lesson to learn by the European electric power sector.

The American Gas Association (AGA) initiated quite early some initiatives in the context of infrastructure security. Already in 1988 they had the first discussion in the use of encryption protocols to protect the gas sector communications and the SCADA systems. The first technical proposals by the Gas Technology Institute (GTI) received scarce attention, due to the lack of awareness on the risks. Only after the September 11th 2001 events there was some consciousness that specific safeguards were required. The work is conducted by a dedicated working group that has delivered the standard report AGA 12 "Cryptographic Protection of SCADA Communications" (Draft 4), issued in November 2004. Although the work is limited to the encryption of communications, the working group pointed to the beginning to generic results targeting several industries: gas, electric, water, wastewater and pipeline real-time control systems. It should be considered that encryption is a valuable solution, but it is first needed to understand the problem: the security risks.

In view of the specific scope of this report, the rest of this chapter especially focuses on the ISA and NIST approaches having general relevance, discusses the respective merits and compares them with the aforementioned efforts of the IEC within TC 65. We also focus on some more specific approaches undertaken in the power sector, namely the NERC 1200 and 1300 cyber security standards and the current status of efforts within IEC Technical Committee TC 57 (Power Systems Management and Associated Information Exchange) among others. A conclusive section will try to give a summary view of these efforts and address the issue of their convergence.

3.3.1 The ISA 99 Multipart Series of Standards

ISA has formed the Standards and Practices Committee SP 99 with the intent of developing guidance to help stakeholders provide *secure* Manufacturing and Control Systems and the express goal of achieving a uniform approach in the field of instrumentation. For ISA, Manufacturing and Control Systems include, but are not limited to:

- Hardware and software systems such as Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA), networked electronic sensing, and monitoring and diagnostic systems.
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.
- Basic Process Control System (BPCS), Safety Instrumented System (SIS), and associated systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces.

Hence the standard under development that will be issued in the coming years will have a multi-industry focus. So far, SP99 has planned a comprehensive approach including four parts [ISA 2005]:

ISA 99.00.01 - Security for Industrial Automation and Control: Concepts, Terminology and Models

This standard describes the basic concepts and models related to cyber security. Subsequent parts will address the application of these concepts and models in areas such as security program definition and minimum security requirements. In this standard, terms such as "enterprise," "controls," "process control," "security," and "manufacturing" are used in their most general sense and are held to be applicable to a broad sector of industries.

ISA 99.00.02 – Establishing an Industrial Automation and Control Systems Security Program

The purpose of Part 2 is to provide guidance for developing a program for the security of industrial automation and control systems. It also provides detailed guidance on process activities and key elements for the establishment of a cyber security management system.

ISA 99.00.03 – Operating an Industrial Automation and Control Systems Security Program

Part 3 addresses how to operate a security program after it is designed and implemented. This includes the definition and application of metrics to measure program effectiveness.

ISA 99.00.04 – Specific Security Requirements for Industrial Automation and Control Systems

Part 4 defines the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a security point of view. Based on these characteristics, the standard establishes the security requirements that are unique to this class of systems.

So far ISA ISA99 published its Part 1 standard [ISA 2007] and is working on the Part 2 standard in the ISA 99 series, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*. Also underway is work to develop the Part 4 standard, *Technical Requirements for Industrial Automation and Control Systems.*

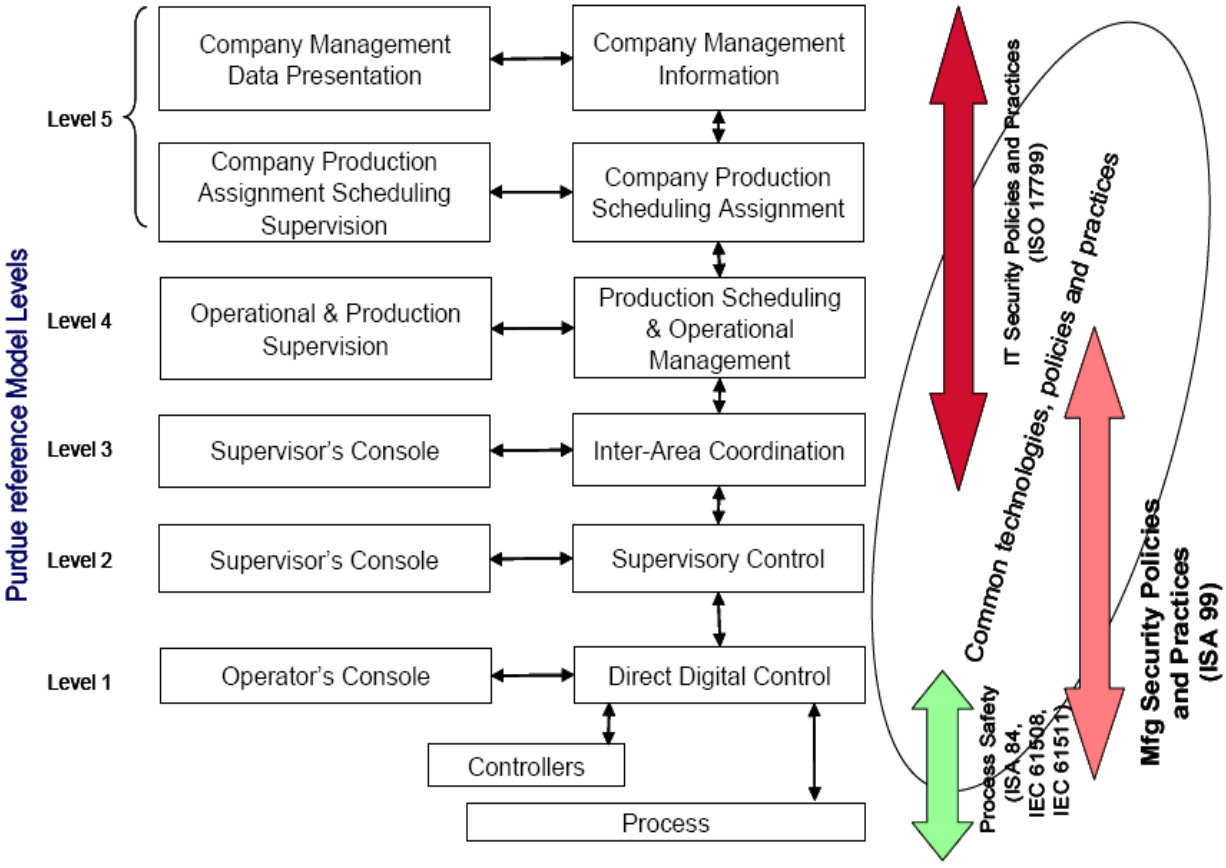


Figure 3 – Scope of ISA 99 (from ANSI/ISA-99.00.01-2007, Security for Industrial Automation and Control Systems: Concepts, Terminology and Models)

Remarkably, ISA 99 tried to position itself with respect to the overall scope of security in Industrial Automation, see figure above. While ISO 1799 mostly covers overall business and organizational issues, included IT security policies, ISA 99 is focusing on Industrial Automation and concerns mostly manufacturing security policies and practices, while the IEC 61508 and 61511 overviewed in [4.3]

below also concern Industrial Automation but basically focus on process safety. This latter appears to have more focused scope than security, because it involves the lower levels of process control only (direct digital control & operation) while security also involves process coordination and supervision.

3.3.2 The NIST 800-53 Approach to Industrial Cyber Security

The NIST 800 Series is a generic approach to computer *security*. Within this approach, The *Industrial Control System (ICS) Security Project* (http://csrc.nist.gov/groups/SMA/fisma/ics/index.html) especially addresses security of industrial controls systems. To some extent this project has an even broader objective than the ISA SP 99, although its constituency appears more specific. In fact, its goal is to establish an overall security program for industrial Information Systems by establishing a series of *security controls* [NIST 2007a], [NIST 2007b] that embrace the whole life cycle of the system:

1. well-defined system-level security requirements and security specifications;
2. well-designed information technology products;
3. sound systems/security engineering principles and practices to effectively integrate information technology products into the information system;
4. appropriate methods for product/system testing and evaluation; and
5. comprehensive system security planning and life cycle management

There is a lively debate among the concerned experts, whether the NIST series is divergent or not from the ISA 99 and whether those approaches can be harmonized. On Nov. 20, 2007, ControlGlobal.com, the online resource of the US Control magazine (http://www.controlglobal.com/unfettered/?p=24) reports this response by the renowned US expert Joe Weiss to a question by the Hon. Michael T. McCaul of the US Congress concerning this issue:

'Although the developmental processes were different for NIST 800-53 and the ISA 99 standards, the results are harmonious. There has been a significant amount of cross-pollination of people between the NIST and ISA standards which will provide for a seamless transition between the standards. Both ISA and NIST address multiple industries and have similar content in those areas where the development is essentially complete. It should be noted that neither ISA nor NIST include the exceptions and exclusions found in the NERC CIP cyber security standards. Specifically, NIST SP 800-53 security controls address the management, operational, and technical safeguards, countermeasures, and/or compensating measures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. ISA 99 Part 2 covers the management and operational requirements NIST will be performing a mapping between ISA 99 Part 2 and the NIST SP 800-53 management and operational security controls. ISA 99 Part 4 will cover the technical requirements. NIST has provided SP 800-53 to the ISA 99 Part 4 Working Group for consideration in the development of the Part 4 standard'

On the Digital Bond web site, a US control system security research and consulting practice, (http://www.digitalbond.com/) Dale Peterson expressed on Nov 21, 2007 a less diplomatic view on the issue:
'*SP800-53 exists and ISA SP99 Part 4, which will eventually include all of the normative technical controls, is at least two years away. Work is just beginning on SP99 Part 4, and the Working Group is trying to reach consensus on approach and structure of the document. It may or may not look at all like SP800-53. SP800-53 is being used as one of many reference documents by the group, and there has been discussions at the end of the effort to develop a chart that maps requirements to this and other standards including NERC CIP.'*

Concerning specifically the NIST approach, the same source also comments:

'NIST SP800-53 is a very good document, but we should not put a halo on it. SP800-53 was used to audit Federal control systems, and it had some major problems. This is why NIST has written draft

Industrial Control System (ICS) Supplemental Guidance *for about 25 of the controls. The guidance essentially says this control may not be technically feasible for an ICS. So some of the rigor that proponents of SP800-53 like is in fact being reduced.'*

3.3.3 The IEC/EN 61508 and 61511 standard

Although conceived for industrial process control instrumentation, this standard encompasses generic methodologies which may be applied to the functional safety of other control sectors where specific methodologies are not available (e.g. home applications). While functional safety addresses the negative impact (i.e. the damage) procured by a plant/equipment on the surrounding environment, security addresses primarily the damages that the surrounding environment may cause to the plant [Ciapessoni and Cortina, 2006].

IEC 61508 specifically addresses planning and management criteria for electrical, electronic, and programmable electrical and electronic devices (E/E/PE) for *safety* related applications. This standard also encompasses risk analysis in all possible situations, requirement specification and allocation of emergency functions and their integrity level, planning, operation and maintenance of safety related systems in order to guarantee their functionality and reliability.

The basic concepts introduced by the IEC/EN 61508 are the Safety Life Cycle and the Safety Integrity Level (SIL). The standard introduces four discrete SIL values for growing integrity levels corresponding to given failure ranges in two operating conditions of the considered safety function, low (i.e. less than once per year) where the average failure probability per demand is specified and high (or continuous), where the average failure probability per hour is specified.

The evaluation of the appropriate SIL for each safety function, and hence to the chain of components for implementing that function, is a difficult task because it requires specialized knowledge and skills, as well as acquaintance with the application of rigorous security planning methodologies. On this respect the IEC/EN 61508 only provides generic criteria, leaving to sector specific standards the selection of appropriate SIL values for each type of application.

Due to its broad and complex application range, the IEC/EN 61508 encompasses seven parts. The former three parts define the safety and risk evaluation cycle and the way to implement safety related functions. The latter four provide a glossary of terms and specific application examples, concerning SIL evaluation and the design, operation and maintenance criteria to achieve appropriate hardware and software reliability.

The IEC Technical Committee SC 65 A "Industrial-Process Measurement and Control - System Aspects" who is in charge of control systems standards in general has faced the problem of functional safety in a systematic and general way, developing the series of standards IEC 61508 [IEC/EN 61508], also acknowledged by the CENELEC as EN 61508. This set of standards covers the whole of industrial process instrumentation, and has become a common reference in several industrial sectors (industrial process control, buildings, etc.). Based on the IEC 61508 the aforementioned Committee SC 65 A also elaborated a more specific standard for process control, the IEC 68511, later acknowledged by the CENELEC as the EN 68511. This is the industrial process standard, encompassing specific sectors, namely chemicals, paper production and (non-nuclear) power generation. It provides detailed prescriptions for the design and operation of process control Safety Instrumented Systems (SIS). While the general 61508 standard is mostly oriented to SIS suppliers, the IEC/EN 61511 is mostly for designers, integrators and SIS end-users.

Furthermore, in the frame of TC 65, but with more general relevance for the whole committee, IEC considered that the increasing degree of internetworking of formerly isolated automation systems increases the exposure of such systems to attack and that standard IT security has inappropriate protection goals and strategies for automation systems, where timely response may be critical to the industrial security and then to the safety. Hence within TC65 a specific working group - WG 10 - was

established in October 2005. (Ref. http://www.iec.ch/cgi-bin/procgi.pl/ www/ iecwww.p?wwwlang=e&wwwprog=dirwg.p&progdb=db1&ctnum=2931).

The goal of WG 10 is to address system security in a holistic way, by preparing a standard to:

1. specify generic scenarios for non-physical external and internal access of industrial process measurement and control systems
2. establish requirements for securing these scenarios against cyber-attack.

Therefore this IEC Standard will address the topic of securing access to and within industrial systems, particularly where more widely available IT-based security techniques are inappropriate.

3.3.4 The IEC/TC65/WG10 work about Security for Industrial Process Measurement and Control

WG10 is developing the IEC 61443 standard about *security* for Industrial Process Measurement and Control. This standard - up circulated in draft form only to the concerned IEC working groups - is being created to become the reference point for the industrial cyber security, and establish requirements for securing access to industrial process measurement and control networks and devices on those networks. It defines security levels for industrial process measurement and control systems, based on risk assessment, provides guidance for that risk assessment and specifies requirements for securing such systems against cyber-attack. Some of those requirements involve mechanisms to secure the transmission of messages among participants within a distributed automation network, and the transmission of messages to and from such networks when connecting with other networks within an enterprise, or to the Internet.

Other security issues addressed include the protection of programs and data, the verification of identity of humans and devices, and the establishment and enforcement of permissions that determine the permitted scope of actions of identified humans, devices and programs. While such security issues are not the primary focus of this standard, they are nevertheless an essential adjunct to security access within automation systems.

The IEC/WG10 is considering almost all relevant security standards (ISO/IEC 7498, ISO/IEC 9797, ISO/IEC 9798, ISO/IEC 10118, ISO/IEC 10164, ISO/IEC 10181, ISO/IEC 11770, ISO/IEC 13335, ISO/IEC 14888, ISO/IEC 15408, ISO/IEC 17999, ISO/IEC 18014), and the efforts of other security working groups (ISO/IEC JTC1/SC27, IEEE, ISA S 99 and SP100) and has established liaison with IEC/TC 57, IEC/SC 65A, ISO/IEC JTC1/SC27 to make possible the development of a complete and adequate industrial security approach.

In summary, the standard will provide guidance for:

- automation system designers
- manufacturers (vendors) of devices, subsystems, and systems
- integrators of subsystems and systems
- end users (responsible for plant operation)

Major goals include communications security of control systems and their points of interconnection to other systems, interoperability of security mechanisms, and management and operational issues. The standard also takes into consideration the need for:

- graceful migration/evolution for existing systems
- fail-over modes that are process safe, including response to denial of service (e.g. autonomous operation)
- reliability/availability of the secured communications service
- scalability (esp. down to small, low cost, low risk systems)

- separation of security, safety and automation requirements as much as possible

Recently, WG 10 is devoting efforts to the identification of appropriate security assessment methodology and protection architectures for control systems and safety instrumented systems.

3.3.5 Power Sector Specific Standards

The necessity for the consideration of information and network *security* in the electric power sector standards was acknowledged in the late 90's only. The proprietary and isolated nature of the ICS equipment up to those years seemed to require no special provision [UCTE, 2003].

The International Council on Large Electric Systems (CIGRE') convened in 2003 the Joint Working Group D2/B3/C3-01, with participation of the Study Committees D2 (Information Systems and Telecommunication), B3 (Substations) and C3 (System Environmental Performance). Its objective is explicitly the security of the ICS of the electric power systems [CIGRE 2001, CIGRE 2004]. The working group is producing a series of papers that will undoubtedly serve for raising awareness in the sector. The papers have been published in the journal Electra [CIGRE, 2005]. The intention is to present a series of reflections and suggestions of immediate actions that could help in bettering the level of ICS security ad the development of proper security policies.

In North America, the NERC has organised a Cyber Security Urgent Action, resulting in some guidelines, compliance audits, and activities such as workshops for raising awareness. In 1998 the USA's Department of Energy assigned to NERC the role of co-ordinator of critical infrastructure protection activities reference point for the electric power sector, including cyber security. It was created the CIPC (Critical Infrastructure Protection Committee) that develops and maintains capabilities to respond to security threats and incidents, and supports the production of standards and guidelines. In June 2002, NERC issued the "Security Guidelines for the Electricity Sector" that cover physical and cyber security, along with emergency plans and business continuity. The approaches and practices recommended are generic, and no indications of particular methodologies are given. In any case, the guidelines are useful for disseminating common requirements and could act as a basis for further developments.

After 9/11, the Federal Energy Regulatory Commission, which oversees the power industry in the US, delegated responsibility for maintaining and complying with reliability standards to NERC, by making it officially the US Electric Reliability Organization (ERO) in charge of the development and enforcement of such mandatory reliability standards. Hence NERC issued security guidelines such as the NERC 1300 (including a compliance matrix): the provision of fines for not complying to such guidelines is a consequence of an overall strategy of the Federal Energy Regulatory Commission where NERC was established as the US ERO to all effects.

Further to the Sector Guidelines, NERC's Cyber Security Urgent Action was set with the purpose to reduce the risks from any compromise of critical cyber assets. A first standard (known as Urgent Action Cyber Security Standard 1200) was issued in August 2003. It is applicable to control centres only and aimed at self-certification. The Draft 2 of the last Cyber Security Standards proposed by the NERC Action (CIP-002-1 through CIP-009-1, formerly known as Urgent Action Cyber Security Standard 1300) was issued in August 2003. It applies to control centres, power plants – except nuclear– and substations and lists several tasks that are deemed essential for cyber security, ranging from security management controls, to the identification and definition of critical assets, controls, personnel, and functions such as training, systems security management, incident response and recovery plans.

But it doesn't consider control system protocols. The standard presents detailed metrics. Its importance resides more in its specification of basic requirements and measures, and the definition of compliance monitoring processes, levels on on-compliance and sanctions. This is a language easily understandable by industry and demonstrates a significant commitment. This type of approach, although its results will always be far from comprehensive, gives an important indication to all players

in industry and regulatory bodies: the recommendation we can derive is that the problem is serious, basic solutions are urgently needed, compliance and enforcement are a must.

The IEC Technical Committee 57 "Power Systems Management and Associated Information Exchange" develops and maintains International Standards for power systems control equipment and systems including EMS (Energy Management Systems), SCADA (Supervisory Control And Data Acquisition), distribution automation, teleprotection, and associated information exchange for real-time and non-real-time information, used in the planning, operation and maintenance of power systems. TC 57 recognized since 1997 that security would be necessary for power systems control equipment and systems. It therefore first established a temporary group (AdHoc WG06) to study the issues of security. In May 2003 this group issued the Technical Report TR62210 [IEC 2003] discussing the security aspects related to the computerised supervision, control, metering and protection in electrical utilities. One of the recommendations was to form a Working Group to develop security standards for the IEC TC57 protocols and their derivatives. Therefore, IEC TC57 WG15 was formed in 1999, and has undertaken this work.

The WG15 title is "Power system control and associated communications - Data and communication security" and its scope and purpose are to *"Undertake the development of standards for security of the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series; undertake the development of standards and/or technical reports on end-to-end security issues"* [Cleveland 2005]. As discussed, the security approach of WG 15 was initially set up by Technical Report TR62210 in July 2003 [IEC 2003].

The scope of the work of WG15 is to develop standards that increase the informational security assurance aspects of the protocols specified within TC57 [Cleveland 2005]. This work is to be published by the IEC as IEC 62351, Parts 1-7, titled:

- IEC 62351-1: Data and Communication Security – Introduction
- IEC 62351-2: Data and Communication Security – Glossary of Terms
- IEC 62351-3: Data and Communication Security – Profiles Including TCP/IP
- IEC 62351-4: Data and Communication Security – Profiles Including MMS
- IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and
- Derivatives (i.e. DNP 3.0)
- IEC 62351-6: Data and Communication Security – Security for IEC 61850 Profiles
- IEC 62351-7: Data and Communication Security – Security Through Network and System Management

So far the IEC/TS 62351-1 which provides an Introduction to the remaining parts of the series was published (May 2007).

3.4 Summary of current status

This chapter has provided a survey on the current efforts to set up reference frameworks addressing the issue of SCADA cyber security. In particular, we have discussed the main efforts characterizing the instrumentation area, where the most recent and most complete ones appear to come from the ISA (S 99) and the NIST (800-53) and the ones concerning the power sector specifically: these include the NERC guidelines and the efforts by two technical groups of the IEC, TC-65 and TC-57. Worth remarking again that in the US the Process Control Systems Forum is trying to aggregate information about current initiatives, to identify consensus across industrial sectors, and to promote a common understanding of security requirements.

As discussed, there is a lively debate in the industrial community about the principal differences among the NIST 800-53 and the S 99. The NIST 800-53 security controls appear to have a broader scope than the ISA: they address the whole life cycle of the industrial automation system, included the management, operational, and technical safeguards/measures to protect the confidentiality, integrity, and availability of the system and its information. The ISA 99 (Part 2) covers the management and operational requirements of the system. As some US experts have pointed out existing limitations of the NIST 800-53, NIST is striving to provide a mapping in between the two approaches. In summary, the NIST 800-53 strength is that it is comprehensive and ready, while completion of the S 99 is at least two years away. On the other hand, the constituency of the SP 99 appears far broader – hence the chances of the S 99 to become the reference standard for ICS appear stronger.

US companies predominate in the constituency of most of the key efforts mentioned in this chapter. This is justified in view of the mentioned strong push given by the US government on the issue, and the maturity of awareness among the concerned US stakeholders, especially in the power sector. The IEC TC 65 and 57 are a remarkable exception to this overall landscape, because EU stakeholders are fairly well represented, if not predominant. In the attempt to set up a CEN Focus Group on the issue of SCADA security, we summarized the respective roles of these two Committees as follows: *'There are many initiatives going on in the international area regarding security aspects of SCADA systems that respond to the clear and concrete industrial needs. These initiatives are carried out by several organizations, most significantly IEC. Here, two existing technical committees appear specifically relevant:*

- *IEC TC 65 addressing standardization of SCADA cyber security in the broad landscape of the process sector;*
- *IEC TC 57 addressing implementation of cyber security features within existing communication protocols for the electricity sector.*

This latter, although partly encompassing SCADA, extends beyond to embrace the requirements of innovative measurement systems like wide-area measurement. This is indicative of the need to cover control and communication systems.'

The experts consulted to set up the said CEN Focus Group on SCADA security agreed that Current standardization efforts appear to be converging towards a common terminology. The PCSF has established a common vocabulary and all current efforts, including IEC, CIGRE', ISA and AGA, are now converging towards that common set of definitions. Within ISA, Committee SP-99 appears to be leading this effort, while the other main effort is currently provided by the IEC TC 65.

4 The current state of the matter in Europe

As anticipated in the previous chapter, over 2006 we tried to sum up the current state of standardisation efforts[2], based on a questionnaire, to the aim of performing a survey of the existing guidelines, norms and standards at the national & EU/global level, so as to eventually indicate needs for further guidelines, norms and standards at the European level. The questionnaire was mainly focused on the protection against external deliberate disruptions, e.g. terrorist attacks, organised crime, information warfare.

After a first set of replies, summarised in [Stefanini et al., 2006], we further deepened with a few experts in the sector. All consulted people are involved in one or more Committees to discuss cyber

[2] Most of this effort was performed in the framework of CEN/BT/WG 161/EG on Energy Supply. WG 161 is a working group organized by CEN on Protection and Security of the Citizen. WG 161 committed to an Expert Group an investigation on security standards in the Energy sector. In that context an investigation on standards for control systems security was also performed.

security oriented standards (for control systems in general, e.g. SP 99 and/or power sector specific, e.g. IEC TC 65 and 57). They were asked three sets of questions:

1. Is there a need for a common conceptual and terminological basis? Are the current standardisation efforts converging towards an interoperable solution, or the plethora of efforts is diverging, to the effect of having a Babel of standards?
2. As current efforts are in the main quite recent, what is the degree of penetration of these standards in the current industry practice in Europe? Which measures appear more appropriate to encourage penetration of these practices in the EU industry? Which could be the obstacles to this?
3. Which is the relative position of Europe with respect to USA, and what actions might be required at the European level? While many industry sectors - electricity, oil, gas - in the US are issuing guidelines and have set up a common platform (the Process Control Systems Forum), international committees where EU industry is represented seem to carry out more dispersed efforts, to the effect that EU industry awareness and readiness may lag behind.

In the following we provide a brief summary of the replies received.

Question 1: Is there a need for a common conceptual and terminological basis?

- Current standardization efforts concerning SCADA security are converging. The IEC TC 65 – WG 10 is leading this effort, while the other main effort is currently provided by ISA SP-99, but it is likely that they will limit themselves in the future to issuing guidelines, leaving proper standardisation to the IEC TC 65 – WG 10. The time range to achieve a comprehensive cyber security standard about SCADA should be 3-5 years.
- The PCSF has established a common vocabulary and all current efforts, including IEC, CIGRE', ISA and AGA, are now converging towards that common set of definitions.
- Divergence of some efforts (most remarkably TC 57) can be explained by the different - more peculiar - scope and mission. These two factors account for most of the differences a particular standard will add – e.g., in form of a qualifying language to a definition - to place particular emphasis on their scope of work. Specifically, WG 15 of TC 57 has a unique problem, in that they have to amend for cyber security specific communication protocols established quite long time ago, by 1995-96, and have to adapt to the original vision and terminology of the foundational documents.[3] In conclusion, TC 57 is looking to more specific issues, peculiar of the electric power system sector. And cyber security requirements for some Transmission & Distribution equipment (e.g. Wide Area Monitoring and Protection) are far more stringent than the ones regarding SCADA in general.

Question 2: Degree of penetration of these standards in the current industry practice in Europe

- Penetration of security related standards was quite limited in Europe until now because Europe considerably invested in security in the past. However the feeling that the issue is becoming crucial is growing in the EU. Probably other sectors than electricity (e.g. chemicals) may feel strongly the issue of SCADA security, because their investment in security was less in the past.
- Specifically concerning cyber security of SCADA we cannot say that such standards exist yet. There are a lot of standardisation efforts, but the result is not a Babel of standards, but a lack of standards, because the same few experts are involved in all initiatives and thus have

[3] Manufacturers are a unifying force, because they are looking to scalable solutions that may apply to any enterprise worldwide. They do not want to develop a product for the US market only. The same is true for asset owners with a little different point of view. They also want a comprehensive and scalable solution that can be deployed throughout the enterprise. They do not want "stove pipe" solutions that do not have a common approach for managing, maintaining and operating the security mechanisms. From their point of view, stove pipe solutions are not cost effective. This a goal, but in practice very difficult to achieve because an organization can establish corporate policies, but organizational units within the enterprise need to modify those policies to carry out their mission and responsibilities effectively. Balancing this diversity is where the majority of their effort is expended.

nowhere the time to actually produce something. Another problem is that academics, government representatives, security consultants/vendors and automation stakeholders (vendors, plant owners) have diverging interests and stall each other. Unusable, unrealistic standards and requirements (e.g. certification), cost, further dispersion of efforts through creation of even more working groups look to be obstacles.

- No standards, thus no usage, but all vendors and many users are trying to accommodate what emerges as best practice security. An appropriate measure to encourage penetration of these practices is government funding for automation users and automation vendors to promote investments into more secure systems.
- On the utility side, while some best practice exist and now is requested as part of new system deployment, few investments are actually made to update and improve security of existing applications. In summary, electric companies in the EU may not follow security guidelines now but will comply to standards when they will exist.
- There is a shortage of skilled IT security engineers in the utility environment (as opposed to other domains where IT may have even broader impact). Large training programs should be deployed to improve security awareness of these technicians.

Question 3: Relative position of Europe with respect to USA

- While many industry sectors - electricity, oil, gas - in the US are issuing guidelines and have set up a common platform (the Process Control Systems Forum), international committees where EU industry is represented seem to carry out more dispersed efforts, to the effect that EU industry awareness and readiness may lag behind. US organisations like NERC, NIST and ISA took the lead of standardization efforts. The overall motivation why this started with the US is their unique geopolitical position with the related exceptional threats over the last decade. Regarding the approach - guidelines versus standards - while in the EU in general, when a standard is issued, national legislations subsume it, hence stakeholders also comply, this is not quite so in the US - so that more specific guidelines, issued by sector organisations, need to be issued to enforce measures. Although earlier awareness in the US is also due to an objective lack of security due to less investment in security than Europe in the past, at least as far as the power sector is concerned, now Europe is behind. Funding for security R&D in European automation industry looks an appropriate reply.
- The American DOE initiative, and the US Process Control Forum that follows, should be broadly disseminated in Europe, to raise awareness in all stakeholders on the vulnerability of the various IT applications used in the utility industry.

5 Conclusions and recommendations: needs for Europe

The following main conclusions can be drawn from the overview on current efforts presented in chapter 3 and the discussion on the needs for Europe summarised in chapter 4:

- Current standardization efforts appear to converge, especially related to terminology, but at a slow pace. The IEC, where Europe is predominant, harbours two Technical Committees somewhat concerned with control systems security. Progress is hindered by conflicting needs and interests among the stakeholders involved in those efforts. By the time being, the only available standard is the NIST 800-53, but its tiny constituency makes unlikely its wider adoption even in the US. On the contrary, the S 99 appears a good candidate to becoming the reference standard for cyber security of industrial automation and control, but its completion is at least two years away.
- By the time being, the market for industrial control is still segmented. Market needs in the EU differ from North America. While pressure to ensure cyber security of control systems is very

strong in the US (where there is a pungent push from the US government and an influential awareness by the main stakeholders), this is not the case in Europe yet: there is less awareness about cyber security risks and a lack of expertise among technicians in the process control sector. A large majority of European stakeholders do not fully perceive the extent of the cyber threat to their systems yet, and in most cases they are not aware of the potential damage that cyber attack may impart, hence the potential impact of such threat on their business. Summarizing, security of Industrial Control systems in Europe is currently hindered with respect to other markets because there is no substantial business driver for security measures in Europe yet, while such a market was created and established in North America because critical infrastructure security remained a high priority in the US political agenda since the Clinton era, and eventually became a perceived threat for all stakeholders after 9/11.

- In Europe, the high cost of security must be justified: this predicament applies to most industrial security measures, SCADA cyber security included. By consequence, manufacturers' current offers in the EU and the US markets are differentiated. Responding to US market needs, SCADA manufacturers include security packages in their current offer on that market; while the European market does not demand for such packages yet. The cost of such security packages is considerable, and may add over 15% on the overall control equipment cost. Manufacturers are forced to hold a different market approach in Europe with respect to North America: while security is a business for them in the North American market, it is likely to be a pure cost in Europe, as they have nonetheless to embed in their systems security features they have no interest to publicize, because they would meet a deaf ear by their European customers. Manufacturers might be a driving force to encourage ICS and SCADA cyber security because they have an interest to hold a single product line.
- Europe lacks facilities where to test equipment resilience against cyber attacks, while the US and Canada have such facilities in place since years (see Appendix 1). These facilities played a substantial role in improving awareness in the control system community in the US, by their outreach activities and their training and education programmes. Concerning awareness raising, the role of the PCSF is also praised by most experts. As the current PCSF coverage is almost all American, they recommend disseminating the PCSF experience in Europe. The PCSF may act as a model for a European Focus Group on process control security.

From the above, the following main recommendations can be drawn:

- Encourage convergence of most prominent generic approaches to standardisation. IEC led efforts within TC 57 and TC 65 should strive to achieve a generic approach together with ISA S 99. On the technical side, a comparison among those approaches and the NIST 800-53 (which is the only complete one available so far) should take priority. On the political side, clarification of the conflicting needs and interests among stakeholders should take priority.

- There is lack of basic data on SCADA vulnerabilities among stakeholders. There is a need to establish standards for exchange and communication of security relevant information among stakeholders. The Commission should encourage the establishment of a permanent communication structure on ICS security relevant information among stakeholders.

- The Process Control Security Forum was a substantial instrument both to exchange ICS security information and to achieve clarification of the conflicting needs, interests and viewpoints in the North American stakeholders community. Liaison with the US PCSF should be encouraged, and its experience imported in Europe. The Commission should encourage the European stakeholders community to establish a permanent workshop on security of industrial control systems along the PCSF model.

- Cyber security testbeds continue to be key instruments for security information exchange, awareness raising and dissemination of best practice among the North American stakeholder

community The US DoE Test Bed programme and the DHS have been substantial to the establishment of such testbeds in the US and Canada. The Commission should encourage the establishment of European reference cyber security testing platforms.

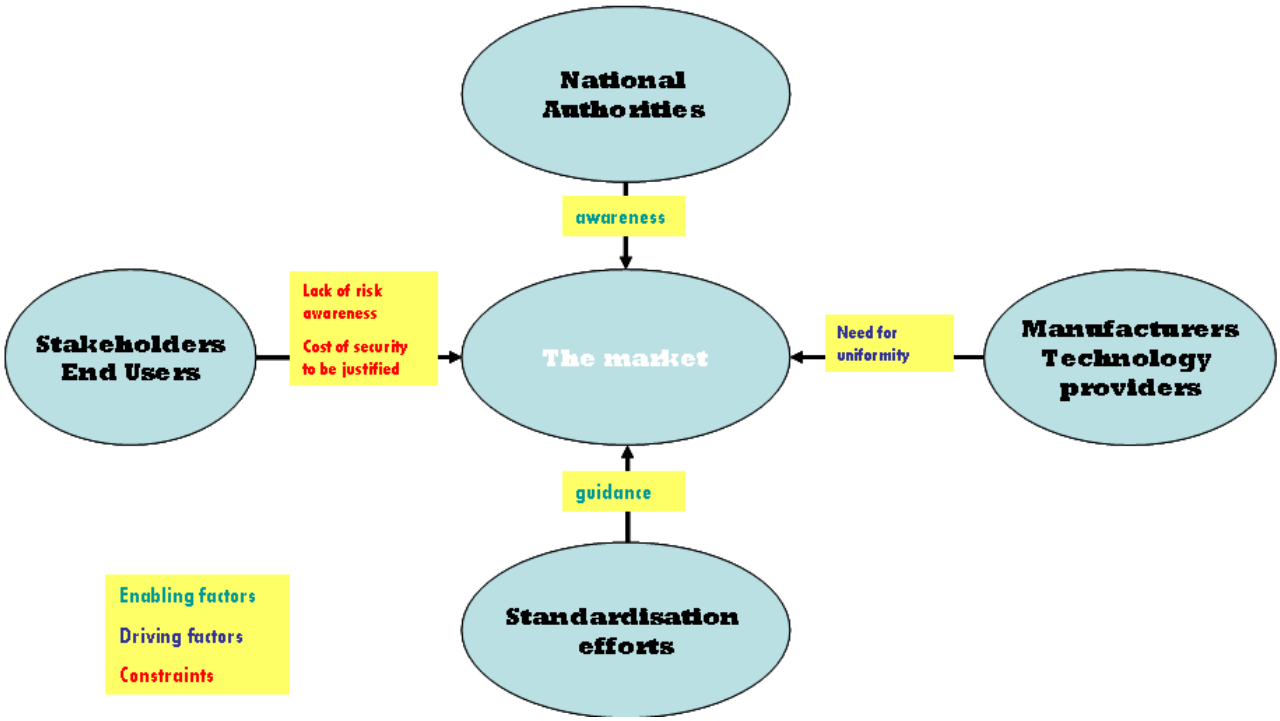


Figure 4 – The EU market for ICS security

Acknowledgement

The authors would like to thank Enzo Tieghi and Joe Weiss for the advice given on early drafts of this paper.

References

[CIGRE, 2001] *System Protection Schemes in Power Networks*, CIGRE' Task Force 38.02.19June 2001.

[CIGRE, 2004] *Managing information security in an electric utility*, Joint Working Group D2-B3-C2.01, Electra, n. 216, October 2004.

[CIGRE, 2005] *Cybersecurity considerations in Power System Operations*, Joint Working Group D2-B3-C2.01, Electra, n. 218, February 2005.

[Ciapessoni and Cortina 2006] *La sicurezza funzionale nel sistema elettrico di potenza:stato della normativa tecnica applicabile*, E. Ciapessoni and R.Cortina, Gennaio Febbraio 2006 – 1 Rivista AEIT, "Sicurezza dei Sistemi"

[Cleveland, 2005] *IEC TC57 Security Standards for the Power System's Information Infrastructure – Beyond Simple Encryption*, Frances Cleveland, October 2005, https://www.pcsforum.org/library/index.php?mode=file_details&fid=105

[CNN 2007] *Staged cyber attack reveals vulnerability in power grid*, CNN com edition 2007, http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html

[DOE, 2005] *A Summary of Control Security Standards Activities in the Energy Sector*, Department of Energy Office of Electricity Delivery and Energy Reliability, USA, October 2005.

[Dondossola et al., 2004)] *Emerging standards and methodological issues for the security analysis of the Power System information infrastructures*, G. Dondossola, M. Masera and O. Lamquet, CRIS 2004 Conference: Securing critical infrastructures, Grenoble 25-27 October, 2004.

[Dondossola and Lamquet, 2006] *Cyber risk assessment in the electric power industry*, G. Dondossola, O. Lamquet, Electra, no. 224, February 2006.

[Eurelectric 2004] *Power Outages in 2003*, Task Force Power Outages, Eurelectric report 2004-181-0007, June 2004

[IEC 2003] *Power system control and associated communications – Data and communication security*, Technical Report TR 62210, May 2003. Available in: http://www.standardsdirect.org/standards/standards4/StandardsCatalogue24_view_26054.html/

[Gheorghe, Masera et al., 2006] *Critical Infrastructures at Risk. Securing the European Electric Power System.* Gheorghe, A.V., Masera, M., Weijnen, M., De Vries, L.J. (2006). Springer V., ISBN: 1-4020-4306-6

[IEC/EN 61508] *Functional safety of electrical/ electronic/programmable electronic safety-related systems*, 2003

[ISA 2005] *Guide to the ISA-99 Standards Manufacturing and Control Systems Security Revision 4*, ISA SP-99 Committee, November 2005, available in http://www.isa.org/

[ISA 2007] ANSI/ISA-99.00.01-2007, *Security for Industrial Automation and Control Systems: Concepts, Terminology and Models*, available in http://www.isa.org/Template.cfm?Section=Shop_ISA&Template=/Ecommerce/ProductDisplay.cfm&Productid=9661

[NIST 2007a] NIST Special Publication 800-53, Revision 2, *Recommended Security Controls for Federal Information Systems*, R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner and G. Rogers, December 2007. Available in http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

[NIST 2007b] NIST Special Publication 800-82, SECOND PUBLIC DRAFT, *Guide to Industrial Control Systems (ICS) Security*, K. Stouffer, J. Falco and K. Scarfone, September 2007, http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

[NTSB 2002] Pipeline Accident Report: *Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999*, National Transportation Safety Board NTSB/PAR-02/02 PB2002-916502 October 8, 2002.

[Pipeline & gas Journal 2007] *SCADA security protections are on the increase*, by Hugh Njemanze, Pipeline & Gas Journal, Feb,2007. http://www.arcsight.com/articles/ArcSight_SCADA_Security_Protections.pdf.

[Security Focus, 2003] *Slammer worm crashed Ohio nuke plant network* by *Kevin Poulsen*, SecurityFocus, August 2003. http://www.securityfocus.com/news/6767

[Stefanini et al., 2005] *Electric System vulnerabilities: the crucial role of information & communication technologies in recent blackouts*, A. Stefanini, A. Servida And S. Puppin, ELECTRA n. 232, December 2005

[Stefanini et al., 2006] *A Survey On Existing SCADA Security Standards*, A. Stefanini, E. Ciapessoni and M. Masera, Convegno Annuale ANIPLA, Sept. 2006

[UCTE, 2003] *UCTE Operation Handbook – Policy 3, Appendix 1*, http://www.ucte.org/ohb/cur_status.asp

[Washington Post, 2008a] *Hackers Have Attacked Foreign Utilities, CIA Analyst Says*, E. Nakashima and S. Mufson, Washington Post, January 19, 2008; Page A04

[Washington Post, 2008b] *Cyber Incident Blamed for Nuclear Power Plant Shutdown*, Brian Krebs, Thursday, June 5, 2008.

[Webb, 2002] *Manufacturing And Control Systems Security - Isa Sp99 History, Status, And How It Can Help You*, Robert C. Webb, October 22, 2002 – Chicago ISA 2002 Conference, ISA SP 99 Standards Committee Meeting

[Wikipedia 2007] *Cyber warfare – known attacks*, see: http://en.wikipedia.org/wiki/Cyber-warfare

Related Links

- ISO 15408. Common Criteria for Information Technology Security Evaluation http://www.iso15408.net/
- National Strategy to Secure Cyberspace http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf
- Instrument Society of America -- http://www.isa.org
- Critical Infrastructure Protection: Cyber Security of Industrial Control Systems http://www.mel.nist.gov/proj/cip.htm
- Process Control Security Requirements Forum (PCSRF) -- http://www.isd.mel.nist.gov/projects/processcontrol/
- Process Control Systems Forum -- http://www.pcsforum.org
- National Infrastructure Assurance Partnership (NIST and NSA) -- http://niap.nist.gov/

- Computer Security Resource Center -- http://csrc.nist.gov/
- CIAO - Critical Infrastructure Assurance Office
- The Twenty Most Critical Internet Security Vulnerabilities http://www.sans.org/top20.htm
- North American Electric Reliability Council (NERC) -- www.nerc.com/cip.html
- Critical Infrastructure Protection Advisory Group (CIPAG)
  http://www.nerc.com/~filez/cipfiles.html
- Federal Energy Regulatory Commission (FERC)
- NOPR on Standard Market Design
  http://www.ferc.gov/Electric/RTO/Mrkt-Strct-comments/discussion_paper.htm
- Department of Energy (DOE). 21 steps to secure your SCADA network
  http://oea.dis.anl.gov/home.htm
- Oil and Natural Gas - National Petroleum Council
  https://www.pcis.org/getDocument.cfm?urlLibraryDocID=30
- Chemicals - US Chemical Sector Cyber Security Information Sharing Forum
  https://www.pcis.org/getDocument.cfm?urlLibraryDocID=37
- Water—The Association of Metropolitan Water Agencies
  https://www.pcis.org/getDocument.cfm?urlLibraryDocID=27
- Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions
  http://www.selinc.com/techpprs/6118.pdf
- The Common Criteria ISO/IEC 15408—The Insight, Some Thoughts, Questions, and Issues --
  http://www.niser.org.my/resources/common_criteria.pdf
- FBI Infragard
  http://www.infragard.net/
- Dept of Homeland Security
  http://www.dhs.gov/
- Information Sharing and Analysis Centers Operations Center public home page
  https://www.it-isac.org/
- Water & Wastewater Information Sharing and Analysis Center
  http://www.waterisac.org/
- International organization for standardization (ISO) -- www.iso.org
- International Electrotechnical Commission (IEC) -- www.iec.ch
- European Committee for Electrotechnical Standardization (CENELEC) -- www.cenelec.org

Appendix 1 - The main SCADA Test beds in the US and Canada

US Department of Energy: The National SCADA TEST Bed

http://www.oe.energy.gov/randd/487.htm

Supervisory Control and Data Acquisition (SCADA) systems and distributed control systems (DCS) are computerized control systems that support the efficient production and distribution of electric, oil, and gas. If unprotected, they are vulnerable to malicious cyber attacks that could produce catastrophic disruptions to our critical national infrastructures. The National SCADA Test Bed is a DOE multi-laboratory program that addresses the security challenges of control systems in the energy sector through:

- control systems testing, research and development;
- advanced technology development;
- control systems requirements development; and
- industry outreach.

The National SCADA Test Bed is jointly managed and executed by Idaho National Laboratory (INL) and Sandia National Laboratories (SNL). Other partners include the Pacific Northwest National Laboratory, Argonne National Laboratory, the National Institute of Standards and Technology, and contractors.

US Department of Homeland Security: The Control Systems Security Program (CSSP)

http://www.us-cert.gov/control_systems/

The Control Systems Security Center is funded by the Department of Homeland Security and is working with industry, universities, national laboratories, and government agencies to identify and develop solutions to protect vital infrastructures from a cyber attack. The Center provides a centralized location for vulnerability assessments, tool development, research, and incident response. To reduce control system risks within and across all critical infrastructure sectors, the National Cyber Security Division of the Department of Homeland Security established the Control Systems Security Program to coordinate efforts among federal, state, local, and tribal governments, as well as control systems owners, operators and vendors. The Control Systems Security Program 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.

The goal of the CSSP is to guide a cohesive effort between government and industry to reduce the risk to critical infrastructure control systems. To lead this effort, the CSSP executes a strategy composed of two interrelated objectives, on both national and international fronts, and works with other government entities and the control systems community to improve the security posture of our nation’s control systems.

The CSSP provides guidance to the control systems community through a variety of mechanisms and activities.

- Maintaining a technical support center to conduct assessments of commercially available control systems and components.

- Enhancing industry practices for securing control systems against cyber attacks by providing assessment tools, implementation guidelines, and recommended practices.
- Performing outreach activities and improving awareness in the control system community through training and education.
- Providing informational products to assist vendors and owners/operators in designing,
- procuring, installing, and operating controls systems to mitigate risks.
- Providing strategic recommendations to the research and development community for development and testing of next-generation secure control systems.
- Assisting national and international standards organizations in developing control systems cyber security standards.

Process Control System Forum

https://www.pcsforum.org/

The PCSF mission is to accelerate the design, development, and deployment of more secure control and legacy systems. It leverages and unifies the experience, capabilities, and contributions of international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community through meetings, Interest Groups, and Working Groups, to develop and adopt common architectures, protocols, and practices. The Forum is uniquely positioned to:

- Aggregate information about current organizations, their efforts, directions, and work product from across multiple sectors to increase visibility and reduce redundancy.
- Identify consensus cross-industry and cross-functional issues that require resolution, and determine a path and effort that is owned, traceable, and produces generally acceptable solutions.
- Cross-connect decision-makers from industry, government, vendors, and academia, in ways that promote increased understanding of requirements and opportunities for collaboration.
- Impact a broad portion of the control system community through procedures, methods, guidelines, best practices, and other resources, issued through organizations that participate in the PCSF.

The PCSF is an open, collaborative, voluntary forum of international stakeholders from government; academia; industry users, owner/operators, and systems integrators; and the vendor community. The list of companies represented through the Forum participants is a constantly growing example of the variety and quality of collaborative input. As of September 5, 2007 PCSF participants include representatives from over 410 organizations worldwide.

Sandia National Laboratories

http://www.sandia.gov/mission/homeland/programs/cyber/prevent.html

Sandia helps protect cyber systems with tools to identify and harden vulnerabilities in existing systems. Supervisory control and data acquisition (SCADA) systems are key to the smooth and secure operation of many of our critical infrastructure elements. The Center for SCADA Security helps sponsors harden their systems by providing engineering best practices, industry standards, vulnerability assessments, and testbeds.

The Information Operations Red Team and Assessments (IORTA) and its Information Design Assurance Red Team (IDART) offer independent assessments of information, communications and

critical infrastructures throughout their lifecycles, focusing on the malevolent intent of adversaries. These assessments lead to blueprints for bolstering security and mitigating damage.

Tools developed by Sandia to enhance network security include:

- An invisible router that employs traffic routing countermeasures to protect sensitive networks
- Intelligent secure agents that automatically raise or lower a network's security profile based on cumulative information detected
- Distributed security with threshold cryptograph that enables cyber systems to withstand some malicious node behavior without compromising the entire network

Idaho National Laboratory

http://www.inl.gov/nationalsecurity/capabilities/security/

Comprehensive computer and cyber security programs are an essential element for today's personnel computers as well as for the digital control systems that operate our nation's infrastructure systems such as transportation and telecommunication systems and facilities such as chemical and water treatment plants. Leveraging the Laboratory's more than 50 years of experience in developing, operating, and maintaining complex control systems for nuclear reactors and other infrastructure systems, the INL created a Critical Infrastructure Test Range complete with full-scale infrastructure systems, remote and secure testing grounds, and an expert staff to aid the utility and control systems industry in developing tools and solutions to improve cyber security.

In 2004, the departments of Energy and Homeland Security established two multi-year programs at INL to protect the nation's infrastructures against attacks from hackers, virus writers, disgruntled employees, terrorist organizations and nation states. The National Supervisory Control and Data Acquisition (SCADA) Test Bed is funded by the Department of Energy and works in collaboration with Sandia National Laboratory to systematically analyze, test, and improve cyber security features in the control systems that operate the nation's electric power grid. SCADA systems are also commonly found in the water and oil and gas industry. The Control Systems Security Center is funded by the Department of Homeland Security and is working with industry, universities, national laboratories, and government agencies to identify and develop solutions to protect vital infrastructures from a cyber attack. The Center provides a centralized location for vulnerability assessments, tool development, research, and incident response.

Pacific Northwest National laboratory - The Critical Infrastructure Protection Analysis Laboratory

http://homeland-security.pnl.gov/cipal.stm

Understanding the risk posed by these vulnerabilities is the driving force behind the Pacific Northwest National Laboratory's research facility that serves as a safe test-bed for evaluating existing technology, research and development, and independent verification and validation of cyber systems. The CIPAL - Critical Infrastructure Protection Analysis Laboratory is a state-of-the-art facility to help the user identify and address vulnerabilities in computer systems, embedded electronic devices and networks. CIPAL provides a completely isolated network for simulated attacks where researchers, engineers and users of critical infrastructure protection-related technologies can address the vulnerabilities related to computers or networks and other aspects of information assurance. Performing such work in an isolated network is necessary to preclude harming real-world applications. Research within CIPAL focuses on:

- Vulnerability Simulation
- Plug and Play
- Vulnerability Assessment
- Information Assurance
- Information Operations
- Software Agents
- Advanced Intrusion
- Detection Sensors
- Secure Software
- Engineering Processes
- Supervisory Control & Data Acquisition (SCADA)
- Vulnerability Assessment
- Critical Infrastructure Modeling.

BCIT – British Columbia Institute of Technology

http://www.bcit.ca/appliedresearch/security/

Research conducted at the BCIT Internet Engineering Lab and the Industrial Instrumentation Process Lab (the activity seems to have stopped in 2003) aims to determine the risks and create solutions for protecting industrial systems from both internal interference and outside intrusion (i.e. Internet hackers). Topics included:

- Understanding possible effects of cyber attacks on SCADA and process systems and the risk they pose to the economy, the environment and the safety of the public
- How traditional IT systems differ from industrial control systems in terms of architectural design, security requirements and risk management
- Analysis of SCADA protocols for potential security vulnerabilities
- Development of protocol and device security test harnesses
- Development of new techniques and technologies for protecting critical industrial networks

As a pioneer in Cyber-Security Engineering for Critical Infrastructure research, BCIT offers a full range of security services for industrial and governmental clients. These are based on our current research programs and include:

- Controller security vulnerability testing
- Vulnerability and risk assessments
- Security policy development
- Security architecture and technology development
- Policy and regulatory compliance audits
- Penetration testing and ethical hacking
- Incident response planning

- Onsite industrial cyber security training
- Security instructional multimedia training
- Industrial security incident database subscriptions

Vulnerability and risk assessments

An understanding of risks and vulnerabilities is the crucial first step to securing SCADA and process systems. BCIT can provide on-site assessments based on a number of cyber security vulnerability assessment methodologies (VAM), including both scenario and asset based techniques. We can also provide guidance in the development of methodologies tailored to your needs specific industry or site.

Controller security/vulnerability testing

Research has uncovered a number of serious security vulnerabilities in the control platforms used in critical infrastructures, such oil refining and power generation. If you are equipment vendor who needs to test your product prior to market release or a user who wants to be aware of system vulnerabilities prior to deployment, BCIT will conduct a series of systematic cyber vulnerability tests against any networked device used in process operations including:

- SCADA Remote Terminal Units
- SCADA Masters
- Programmable logic controllers
- Distributed control systems
- Emergency shutdown systems
- Human Machine Interfaces
- Intelligent Electronic Devices

Industrial security incident database

The BCIT Industrial Security Incident Database (ISID) is an initiative designed to track incidents of a cyber security nature that directly affect industrial control systems and processes. This includes events such as accidental impacts, external hacks, DoS attacks, etc. Data is collected by through research into publicly known incidents (such as the Australian Sewage Spill) and private reporting. Each incident is rated according to reliability and impact along with a number of important variables. At the present time there are approximately 120 incidents in the database and it is growing by about 10 incidents per quarter.

European Commission

EUR 23538 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Towards Standardisation Measures to Support the Security of Control and Real-Time Systems for Energy Critical Infrastructures
Alberto Stefanini, Marcelo Masera
Luxembourg: Office for Official Publications of the European Communities
2008 – 38 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593

Abstract

This report outlines the context for control and real time systems vulnerability in the energy sector, their role in energy critical infrastructures and their emerging vulnerabilities as they were put in light by some recent episodes. Then it provides a survey on the current efforts to set up reference frameworks addressing the broad issue of control systems security. It discusses the role of standards and outlines the reference approaches in that respect. The current attitude of Europe towards the issue of control systems security is discussed and compared with the US situation, based on a stakeholder consultation, and gaps and challenges are outlined. A set of recommendations for policy measures to address the issue is given.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.