enisa
European Network and Information Security Agency

Protecting Industrial Control Systems

Annex IV. ICS Security Related Initiatives

[Deliverable – 2011-12-09]

About ENISA

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

Contact details

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

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

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

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

Contents

1. ICS Security Related Initiatives

The aim of this section is to highlight a number of security initiatives and organisations that are important to ICS protection. These initiatives have been classified according to their geographical origin and type. Furthermore, their mission/objectives and primary activities related to ICS security are also described.

What follows is a brief explanation on some of the key fields that will be used for the classification of the initiatives/organisations which are presented in this chapter:

- **Name:** Name of the Group.
- **Type:** Type of organisation/initiative (see below).
- **Line of action:** The activities the group is related to (i.e. policy, standards, information sharing, dissemination and awareness, economic or financial, technical, training and education, R&D).
- **Participants:** Stakeholder types which participate in the organisation/initiative (i.e. ICS manufacturers, ICS security tools and services providers, Operators, Public bodies, Standardisation bodies, Academia and research).
- **Mission/Objectives:** Purpose of the group.
- **Results:** Standards, Good Practices, Regulations, Technical Reports, Technical Solutions, etc.
- **Comments:** Additional information about the organisation/initiative.
- **Site:** The reference URL for the initiative being described.

The values of the “Type” field can be one of the following:

- **International agency:** An association of public bodies from different countries, which support its members, seeks to achieve common goals and collaborates with other similar agencies and even non-member countries.
- **Industry association:** An association that supports and protects the rights of a particular industry and the people who work in that industry, and which seeks to achieve the common goals of its members. There may be a public entity within these associations, but it does not have a leading role.
- **Public Private Partnership:** A government service or private business venture which is funded and operated through a partnership of government and one or more private sector companies.
- **Public body:** An organization whose work is part of the process of government, but is not a government department.

- **Regular private organisation:** An organisation which is privately run and does not rely on money from the government and funds from charities. They get make their own money by providing a service at a cost.
- **Professional association:** Also called a professional body, professional organization, or professional society. A professional association is usually a non-profit organization seeking to represent a particular profession, the interests of individuals engaged in that profession, and the public interest.
- **Specialized event:** Workshops, forums, conferences or summits focusing on ICS security and CIP.
- **R&D project:** A collaborative project, involving research and development activities which results are worth-mentioning in the area of ICS security.
- **Online resource:** A specialised website, blog, e-forum, online group, and similar resources.
- **Other:** When an initiative or an organisation does not match with any of the previously defined types, it will be classified with this value.

1.1 International

Name	CIGRE, JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems
Type	Industry association
Line of action	Organizational and Policy, Standards, Economic or Financial, Technical
Participants	All stakeholders
Mission/Objectives	CIGRE (International Council on Large Electric Systems) is one of the leading worldwide Organizations on Electric Power Systems, covering their technical, economic, environmental, organisational and regulatory aspects. A permanent, non-governmental and non-profit International Association, based in France, CIGRE was founded in 1921 and aims to: • To facilitate the exchange of information between engineering personnel and specialists in all countries and to develop knowledge in power systems. • Add value to the knowledge and information exchanged by synthesizing state-of-the-art world practices. • Make managers, decision-makers and regulators aware of the synthesis of CIGRE's work, in the area of electric power.
Activities related to ICS security	The D2 study Committee is focused on Information Systems and Telecommunications, and its security. It publishes a journal called ELECTRA CIGRE's Bilingual bimonthly Journal for Power System Professionals and some of its articles are related to security in ICS environments. i.e.: “The Impact of Implementing Cyber Security Requirements using IEC 61850” (Holstein, Li, & Meneses, 2010).
Results	Technical Reports

Comments	CIGRÉ is based in France
URL	www.cigre.org

Name	IAEA
Type	International agency
Line of action	Dissemination and Awareness, Standards, Technical
Participants	Public bodies
Mission/Objectives	Its Member States assist in planning and using nuclear science and technology for various peaceful purposes, including the generation of electricity. The objectives of this organisation are: • To develop nuclear safety standards. • To verify through its inspection system that States comply with their commitments, under the Non-Proliferation Treaty and other non-proliferation agreements, in order to use nuclear material and facilities only for peaceful purposes.
Activities related to ICS security	The IAEA organises several events and participates in several projects in which they try to acquire knowledge on security applications in ICS environments such as nuclear power plants. Some examples are: • IAEA Coordinated Research Project (CRP) on Cyber security of Digital I&C Systems in NPPs (Glöckler, 2011) • IAEA Technical Meeting on Newly Arising Threats in cyber security of Nuclear Facilities (Iinternational Atomic Energy Agency (IAEA), 2011).
Results	Standards, guides, training resources, technical meetings and associated material
Comments	International Atomic Energy Agency
URL	www.iaea.org

Name	IEC
Type	International agency
Line of action	Standards, Technical
Participants	Standardization bodies
Mission/Objectives	The International Electrotechnical Commission (IEC) is the world's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies. EC provides a platform to companies, industries and governments for meeting, discussing and developing the International Standards they require. All IEC International Standards are fully consensus-based and represent the needs of key stakeholders of every nation participating in IEC work. Every member country, no matter how large or small, has one vote and a say in what goes into an IEC International Standard.
Activities related to ICS security	The IEC develops a lot of standards and technical reports, alone or in collaboration with other organizations like ISO, on security and other technical aspects. IEC has several groups working for the implementation of security measures in ICS environments. The following points highlight the most important ones: • IEC TC27: this technology committee works in data and communication security. • ISO/IEC JTC 1/SC 27: in charge of the standardization of generic methods and techniques for IT security. • IEC TC 65: this technology committee works in systems and elements used for industrial-process measurement and

	control concerning continuous and batch processes. Some of the most relevant documents on ICS security of IEC are: • IEC 62351, Data and communication security • IEC 62210, Power system control and associated communications. Data and communication security • IEC 62443, Security for industrial process measurement and control: network and system security For more information on these documents and other important IEC documents related to ICS security, please refer to Annex III.
Results	Standards, technical reports
Comments	International electro technical commission
URL	www.iec.ch

Name	IEEE
Type	Professional association
Line of action	Standards
Participants	All stakeholders
Mission/Objectives	IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities. In this way, the IEEE develops standards and technical reports on security and other technical-related aspects.
Activities related to ICS security	The IEEE is divided into several technical committees. One of the most important is the standardization technical committee. This Committee includes several work groups that are devoted to defining security measures for ICS environments. Some of the most important workgroups are: • IEEE WGC1 - Application of Computer-Based Systems: This group has been responsible for the document "1686-2007 IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities Active Standard" (Institute of Electrical and Electronics Engineers (IEEE)). • IEEE WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: This group has been in charge of the document "1711-2010 IEEE Trial-Use Standards for a Cryptographic Protocol for Cyber Security of Substation Serial Links" (Institute of Electrical and Electronics Engineers (IEEE)). • IEEE E7.1402 - Physical Security of Electric Power Substations: Responsible for the treatment of all matters related to the secure operation of electrical substations with respect to outside intrusions into the substation (Institute of Electrical

	and Electronics Engineers (IEEE)). Another technical committee which makes studies on the security of ICS environments is the IEEE Power & Energy Society (Institute of Electrical and Electronics Engineers (IEEE)). This technical committee comprises several technical workgroups devoted to security problems in ICS. It is worth highlighting workgroup IEES PSACE CAMS (Power System Analysis, Computing, and Economics) (Computing and Analytical Methods Subcommittee). The focus of the workgroup is the cyber security of electric power infrastructures (Institute of Electrical and Electronics Engineers (IEEE), 2000). Finally, we would highlight the following IEEE standard documents on ICS security, which are explained in detail in Annex III: • IEEE 1686-2007, Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities • IEEE 1402, Guide for Electric Power Substation Physical and Electronic Security • IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security Substation Serial Links
Results	Standards, technical reports, conferences, educational and training activities
Comments	Institute of Electrical and Electronics Engineers
URL	www.ieee.org

Name	IFAC
Type	International agency
Line of action	Technical, dissemination and awareness, information sharing.
Participants	Public bodies
Mission/Objectives	The International Federation of Automatic Control, founded in September 1957, is a multinational federation of National Member Organizations (NMOs), each one representing the engineering and scientific societies concerned with automatic control in its own country. The aims of the International Federation of Automatic Control (IFAC) are to promote the science and technology of control in the broadest sense in all systems, whether, for example, engineering, physical, biological, social or economic, in both theory and application. IFAC is also concerned with the impact of control technology on society.
Activities related to ICS security	IFAC includes several technical committees concerned about security in critical infrastructures. Some of these are: • IFAC TC3.1: Computer for control (International Federation of Automatic Control (IFAC)). • IFAC TC5.4 WG3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems (International Federation of Automatic Control (IFAC)). • IFAC TC6.3: Power plants and power system. Control of constraints and security of control aspect (International Federation of Automatic Control (IFAC)).
Tb Results	Technical reports
Comments	IFAC stands for International Federation of Automatic Control.
URL	www.ifac-control.org

Name	IFIP
Type	Professional association
Line of action	Technical
Participants	All stakeholders
Mission/Objectives	It is a non-governmental, not-for-profit cluster organisation of national learned societies working in the field of information processing.
Activities related to ICS security	The International Federation for Information Processing (IFIP) is comprised of several technical committees, which at the same time include different Working Groups (WGs), which focus their efforts on viewing security from different points of view. There are WGs engaged in the analysis of safe practices, others in the implementation of these measures and even one in the review of the state of the art of security in the information process. Some important Working Groups are: • IFIP TC1 WG 1.7 Theoretical Foundations of Security Analysis and Design: The main research topics relevant to the workgroup include a formal definition and a verification of the various aspects of security: confidentiality, integrity, authentication and availability; new theoretically-based techniques for the formal analysis and design of cryptographic protocols and their manifold applications (e.g., electronic commerce); formal analysis and design for prevention of denial of service (International Federation for Information Processing (IFIP)). • IFIP TC8/TC11 WG8.11/WG11.13 Information Systems Security Research**:** The aim of the workgroup is the creation, dissemination, and preservation of well-formed research about information systems security (International Federation for Information Processing (IFIP)).

	• IFIP TC11 WG11.10 Critical Infrastructure Protection: The principal aim of IFIP WG 11.10 is to weave science, technology and policy in developing and implementing sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors (International Federation for Information Processing (IFIP)).
Results	Technical reports, technical solutions, forums/congresses (e.g. WCC), etc.
Comments	IFIP stands for International Federation for Information Processing
URL	www.ifip.org

Name	ISACA
Type	Professional association
Line of action	Dissemination and Awareness
Participants	All stakeholders
Mission/Objectives	ISACA is a worldwide association of IS professionals dedicated to the audit, control, and security of information systems. As an independent, non-profit, global association, ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. It provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT, Val IT and Risk IT governance frameworks and the CISA, CISM, CGEIT and CRISC certifications are respected ISACA brands and used by these professionals for the benefit of their enterprises.
Activities related to ICS security	Some articles about ICS security like “Security of Industrial Control Systems” (Zwan, 2010), as well as some books such as “Systems from Electronic Threats” (Weiss, 2010).
Results	Certification, international conferences, journals, IS auditing and control standards.
Comments	
URL	www.isaca.org

Name	ISA
Type	Professional association
Line of action	Dissemination and awareness, standards, and education and training
Participants	All Stakeholders
Mission/Objectives	The International Society of Automation is a leading, global, non-profit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities. ISA's mission is to become the standard for automation globally by certifying industry professionals; providing education and training; publishing books and technical articles; hosting conferences and exhibitions for automation professionals; and developing standards for industry. Some of the ISA objectives are to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance.
Activities related to ICS security	The ISA is involved in the development of standards and technical reports about ICS security. For instance, there is the ISA99 committee specific on ICS security. The ISA99 Committee addresses industrial automation and control systems whose compromise could result in any or all of the following situations: • endangerment of public or employee safety

	• loss of public confidence • violation of regulatory requirements • loss of proprietary or confidential information • economic loss • impact on national security The ISA99 Committee establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance (International Society of Automation (ISA)). Additionally, the ISA67 16WG5 is in charge of organizing the cyber security for the nuclear power industry (International Society of Automation (ISA)).
Results	Standards, technical reports, good practices, events
Comments	It is not necessary to be a member of ISA in order to be a member of an ISA99 committee
URL	www.isa.org

Name	MERIDIAN Conference
Type	Specialised event
Line of action	Dissemination and Awareness, Organizational and Policy
Participants	Public bodies
Mission/Objectives	The Meridian process aims to provide Governments worldwide with a means by which they can discuss how to work together at the policy level on critical information infrastructure protection (CIIP). An annual conference and interim activities is held each year to help build trust and establish international relations within the membership to facilitate sharing of experiences and good practices on CIIP from around the world. Participation in the Meridian process is open to all countries and aimed at senior government policy-makers. The Meridian process is founded on the G8 principles that provide a basic framework for understanding and implementing CIIP measures. As new challenges of connectivity and dependencies arise beyond national borders, Meridian enables Governments to explore the benefits and opportunities of cooperation with the private sector, and exchange of information and good practices in CIIP between governments internationally. Tools to raise awareness and share information include the CIIP Directory to facilitate intergovernmental contacts and the Traffic Light Protocol to facilitate distribution of information.
Activities related to ICS security	One of the key topics of MERIDIAN conference is the security issues in ICS environments. In addition to the lectures the MERIDIAN conference has a newsletter, which regularly publishes articles about security in ICS environments (Meridian). It is important to highlight that during EU Sweden's Presidency some

	of the activities included setting up the permanent Meridian Website and establishing the Meridian Process Control Security Information Exchange (MPCSIE). MPCSIE is a workgroup which has recently been established by the international governmental ICT-policy discussion group Meridian (Centre for the Protection of Critial Infrastructure (CPNI)).
Results	Good practices, regulations, conferences
Comments	Annual conference (2011-Qatar)
URL	www.meridian2007.org

Name	SANS
Type	Regular private organisation
Line of action	Dissemination and awareness, training and education, R&D, technical.
Participants	N/A
Mission/Objectives	The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community. SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Centre.
Activities related to ICS security	SANS counts with a complete collection of ICS security courses, like for instance “SCADA Security Advanced Training” (SANS, 1989). SANS also organises a series of conferences dissemination of security issues in ICS, like for instance “The 2011 Asia Pacific SCADA and Process Control Summit” (SANS, 2011).
Results	Certifications, conferences, research articles, technical reports.

1.1.1 **Comments**	
URL	www.sans.org

Name	UCA International Users Group
Type	Industry association
Line of action	Organizational and Policy, Standards, Information sharing.
Participants	Manufacturers, Integrators, Security tools and services providers, Operators.
Mission/Objectives	The UCA International Users Group is a not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The Users Group does not write standards, however works closely with those bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange). The UCAIug as well as its member groups (CIMug, Open Smart Grid, and IEC61850) draws its membership from utility user and supplier companies. The mission of the UCA International Users Group is to enable integration through the deployment of open standards by providing a forum in which the various stakeholders in the energy and utility industry can work cooperatively together as members of a common organization to: • Influence, select, and/or endorse open and public standards appropriate to the energy and utility market based upon the needs of the membership. • Specify, develop and/or accredit product/system-testing programs that facilitate the field interoperability of products and systems based upon these standards. • Implement educational and promotional activities that increase awareness and deployment of these standards in the energy and utility industry.

	• Influence and promote the adoption of standards and technologies specific to the ever-increasing Smart Grid initiatives worldwide.
Activities related to ICS security	UCAIug works in security and in other aspects through its member groups. For instance, the Open Smart Grid sub-technical committee is responsible for developing security guidelines, recommendations, and good practices for AMI system elements. This group fosters enhanced functionality, lower costs and speed market adoption of Advanced Metering networks and Demand Response solutions through the development of an open standards-based information/data model, reference design & interoperability guidelines (Open Smart Grid).
Results	Standards, guidelines.
Comments	UCA International Users Group
URL	www.ucaiug.org

Name	TCG
Type	Industry association
Line of action	Standards, Dissemination and Awareness, Technical.
Participants	Manufacturers, Integrators, Security tools and services providers.
Mission/Objectives	The Trusted Computing Group (TCG) is an international industry standards group. The TCG develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and the implementation by the industry.
Activities related to ICS security	The Trusted Computing Group (TCG) is incorporated as a not-for-profit industry standards organization focused on developing, defining, and promoting open standards for trusted computing that will benefit end users.
Results	Standards, Technical reports.
Comments	Trusted Computing Group
URL	www.trustedcomputinggroup.org

Name	Zigbee Alliance
Type	Industry association
Line of action	Standard, Technical
Participants	Manufacturers, Integrators, Operators.
Mission/Objectives	The ZigBee Alliance is a non-profit industry consortium of leading semiconductor manufacturers, technology providers, OEMs and end-users worldwide. Members aim at defining a global specification for interoperable, cost-effective, low-power wireless applications based on the IEEE 802.15.4 standard. Current membership is about 200 and includes both heavyweights (such as Siemens and Texas Instruments) and small start-ups.

	The goal of the ZigBee Alliance is to create an open specification defining mesh and tree network topologies with interoperable application profiles for wireless control systems. Its focus is clearly on standards-based, low-cost, low-power, and low-data rates applications. Means to certify products are also within the scope of the ZigBee Alliance.
Activities related to ICS security	Zigbee Alliance is working on a communication method based on wireless technology. Low cost and low power have done Zigbee an ideal protocol in industrial automation. The Zigbee Alliance works on the definition of the security mechanism implemented in the protocol definition.
Results	Standards
Comments	
URL	www.zigbee.org

1.2 Europe

Name	Seventh Framework Programme
Type	Other (European R&D Programme)
Line of action	Organizational and Policy, Standards, Dissemination and Awareness, Economic or Financial, Technical.
Participants	All stakeholders
Mission/Objectives	The main objective of this research programme is that Europe becomes the "most dynamic competitive knowledge-based economy in the world".
Activities related to ICS security	There are some projects within FP7 that are related to ICS security. The following sets out a number of them: • **Escort Program:** It aims at disseminating good practice on security of Supervisory Control and Data Acquisition (SCADA) systems (ESCoRTS Project, 2008). • **INSPIRE:** The INSPIRE project aims at identifying techniques to enhance the reliability of communications over unreliable and/or insecure links (WAN, wireless), so that critical control loops become possible over a WAN (INSPIRE Project, 2008). • **INTERSECTION** (**In**frastructure for he**te**rogeneous, **R**esilient, **SE**cure, **C**omplex, **and Tightly I**nter-**O**perating **N**etworks): aims to enhance the European potential in the field of security by assuring the protection of heterogeneous networks and infrastructures, this project develops security measures for communications satellite (INTERSECTION Project, 2008). • **VIKING (*Vital Infrastructure, Networks, Information and Control Systems Management*):** VIKING aims to investigate the vulnerability of SCADA systems and the cost of cyber attacks on society, propose and test strategies and technologies to mitigate these weaknesses and increase the awareness for the importance of critical infrastructures and

	the need to protect them (VIKING Project, 2008).
Results	Technical reports, good practices
Comments	FP7 is the short version for Seventh Framework Programme
URL	http://cordis.europa.eu/fp7/home_en.html

Name	EPCIP
Type	Other (European Programme for Critical Infrastructure Protection)
Line of action	Technical
Participants	All stakeholders
Mission/Objectives	To improve the protection of critical infrastructure in the European Union (EU). This is achieved by implementing specific legislation and by developing an appropriate plan.
Activities related to ICS security	The ECPIP action plan has three main work streams: • The first relates to the strategic aspects of EPCIP and the development of measures horizontally applicable to all CIP work; • The second concerns the protection of European critical infrastructures and aims to reduce their vulnerability; • The third is a national framework to assist EU countries in the protection of their NCIs.
Results	Regulations
Comments	EPCIP stands for European Programme for Critical Infrastructure Protection
URL	http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

Name	Action plan on CIIP
Type	Other
Line of action	Organisational and Policy, Dissemination and awareness, Information sharing, Technical, Economic or financial.
Participants	Public bodies, Manufacturers, Integrators, Operators, Security tools and services providers.
Mission/Objectives	In order to enhance the security and resilience of CIIs, this integrated EU action plan was devised by the European Commission to complement and add value to existing national programmes as well as to the existing bilateral and multilateral cooperation schemes between Member States. This action plan was firstly introduced in COM(2009)149 and consisted of five main pillars: • Preparedness and prevention: to ensure preparedness at all levels. • Detection and response: to provide adequate early warning mechanisms. • Mitigation and recovery: to reinforce EU defence mechanisms for CII. • International cooperation: to promote EU priorities internationally. • Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures. **Preparedness and prevention:** *Baseline of capabilities and services for pan-European cooperation*. The Commission invites Member States and concerned stakeholders to: define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation; make sure National/Governmental CERTs act as the key component of national capability for preparedness, information

	sharing, coordination and response. *European Public Private Partnership for Resilience (EP3R)*. The Commission will foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. *European Forum for information sharing between Member States (EFMS)*. The Commission will establish a European Forum for Member States to share information and good policy practices on security and resilience of CIIs. **Detection and response:** *European Information Sharing and Alert System (EISAS).* The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. **Mitigation and recovery:** *National contingency planning and exercises.* The Commission invites Member States to develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. *Pan-European exercises on large-scale network security incidents.* The Commission will financially support the development of pan-European exercises on Internet security incidents, which may also constitute the operational platform for pan-European participation in international

	network security incidents exercises, like the US Cyber Storm. *Reinforced cooperation between National/Governmental CERTs*. The Commission invites Member States to strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC.29. **International cooperation:** *Internet resilience and stability.* Three complementary activities are envisaged: A Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet; the definition of guidelines for the resilience and stability of the Internet, focusing inter alia on regional remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data; work o na roadmap to promote principles and guidelines at the global level. *Global exercises on recovery and mitigation of large scale Internet incidents.* The Commission invites European stakeholders to reflect on a practical way to extend at the global level the exercises being conducted under the mitigation and recovery pillar, building upon regional contingency plans and capabilities. **Criteria for European Critical Infrastructures in the ICT sector:** *ICT sector specific criteria.* By building on the initial activity carried out in 2008, the Commission will continue to develop, in cooperation with

	Member States and all relevant stakeholders, the criteria for identifying European critical infrastructures for the ICT sector.
Activities related to ICS security	The EP3R, the EFMS and EISAS can be interesting platforms for any future action plan on ICS security at the European level.
Results	Policies.
Comments	
URL	http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

Name	EU-US Working Group (EU-US WG) on Cyber-security and Cybercrime
Type	Other
Line of action	Information sharing, dissemination and awareness, training and education, organisational and policy.
Participants	Public bodies
Mission/Objectives	The EU-US Working Group (EU-US WG) on Cyber-security and Cybercrime was established in the context of the EU-US summit of 20 November 2010 held in Lisbon to tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend. The EU-US WG will address a number of specific priority areas and will report progress within a year time after its establishment. The efforts include: • Expanding incident management response capabilities jointly and globally, through a cooperation programme culminating in a joint EU-US cyber-incident exercise by 2012. • A broad commitment to engage the private sector, sharing of good practices on collaboration with industry, and pursuing specific engagement on key issue areas such as fighting botnets, securing industrial control systems and smart grid (such as water treatment and power generation), and enhancing the resilience and stability of the Internet. • A programme of immediate joint awareness raising activities, sharing messages and models across the Atlantic, as well as a roadmap towards synchronised annual awareness efforts and a conference on child protection online in Silicon Valley by end 2011. • Continuing EU/US cooperation to remove child pornography from the Internet, including through work with domain-name registrars and registries. • Advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards

	and become parties.
Activities related to ICS security	With respect to ICS and Smart Grid security the proposed tasks include the stock taking and comparative analysis of existing initiatives, pilots, good practices and methods addressing ICT risks, privacy and security. The input from the EU side includes: • Activities at national level (NL, DE, UK, SE…) as well as at European level (Euro-SCSIE, possibly via Member States experts in the WG and during the stock taking of the ENISA studies on ICS and Smart Grids security) • Ongoing ENISA studies on Industrial control systems and Interdependencies of ICT sector to energy • Activities of the Expert Group on the Security and Resilience of Communication Networks and Information Systems for Smart Grids, composed of European public and private stakeholders and coordinated by DG INFSO. The input from the US side includes: • Experiences in international public-private coordination to mature acceptance of voluntary security standards. • Specific methodology and mechanisms to engage with the private sector to achieve cooperation and mutual engagement in public-private control system security coordination. The deliverables expected from this cooperation include: • Strategy for EU and US engagement on the control system/smart grid priority area; • Plan of Action for EU and US public private engagement on cyber security of industrial control systems and Smart grids; this will also draw on an analysis of existing coordination bodies for security of industrial control

	systems and highlighting best practices for voluntary participation developed within them.
Results	Good practices
Comments	
URL	http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/658&type=HTML

Name	EuroSCSIE
Type	Public Private Partnership
Line of action	Dissemination and Awareness, Technical.
Participants	Academia and R&D, Public bodies, Standardisation bodies
Mission/Objectives	The E-SCSIE aim is for European industry, government, and research to benefit from the ability to collaborate on a range of common issues, and to focus effort and share resource where appropriate. Its main focus is Information Sharing and the expectations are to raise the level of protection adopted across Europe's SCADA and Control Systems (SCADA/CS) Among its objectives, we highlight the following ones: • To define a European information exchange system for security-related information about SCADA and control systems. • To share and exchange information using the Traffic Light Protocol. • To cultivate a network of relevant government, industrial and research actors. • To establish the basis for a pan-European system for the exchange of security-related information concerning SCADA and control systems.
Activities related to ICS security	Some of the activities carried out by EuroSCSIE include: • Sharing of incidents and good practices • Questionnaire on Control System Cyber-Security (aimed at vendors) 2008/2009 • Standards and requirements (e.g. WIB Process Control Domain Security Requirements for Vendors) • Self Assessment tools (like the one from CPNI UK) • Smart Grids (e.g. Smart Grid Conference in Baarn - 2010)
Results	Information exchange, technical documents, guidelines
Comments	European SCADA and Control Systems Information Exchange

URL	sta.jrc.ec.europa.eu/index.php/competitive-projects-/21-scni/8-e-scsie

Name	IMG-S
Type	Industry association
Line of action	Dissemination and Awareness, Technical.
Participants	Manufacturers, Integrators, Academia and R&D,
Mission/Objectives	The IMG-S is working to define a long term view on the priorities for research in the security domain. The group is looking at technology research priorities at all levels embracing fundamental research, through mission capabilities and system integration. Short, medium and long-term priorities are to be addressed although the focus is primarily on EU funded security research within future financial perspectives (2013 and beyond)
Activities related to ICS security	The main objective is to complement and to improve the current capabilities of the surveillance systems over Europe by identifying technologies and components which could be integrated within an interoperable, reliable, cost effective global system of systems. IMG-S develops European road-map and technical recommendations and tools to enable future regulation on civil aircraft protection against MANPADS or Solution for ensuring end to end secure communications infrastructure and services of hybrid systems.
Results	Technical Reports
Comments	
URL	imgs.frascati.enea.it

Name	Sixth Framework Programme
Type	Other (European R&D programme).
Line of action	Organizational and Policy, Standards, Dissemination and Awareness, Economic or Financial, Technical.
Participants	All stakeholders
Mission/Objectives	The main objective is that Europe becomes the "most dynamic competitive knowledge-based economy in the world".
Activities related to ICS security	FP6 encompasses a number of projects related to security on ICS environments, here there are set out a number of them: • IRIIS: IRIIS developed MIT (Middleware Improved Technology) which, by supporting recovery actions and increasing service stability in case of critical situations, tried to enhance the security of large complex critical infrastructures. Additionally, a simulation environment was developed, SimCIP (Simulation for Critical Infrastructure Protection), which allowed for controlled experimentation with a special focus on CIs interdependencies. (IRRIIS Project, 2006). • CRUTIAL: Some of the main activities of CRUTIAL were the investigation of models and architectures that cope with the scenario of openness, heterogeneity and endured by electrical utilities infrastructures (CRUTIAL Project, 2006). • CI2RCO: The main objective of the CI2RCO project was to create and coordinate a European Taskforce to encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and to establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security (CI2RCO Project, 2008).
Results	Technical reports, good practices
Comments	FP6

URL	http://ec.europa.eu/research/fp6/index_en.cfm
Name	European Network for Cyber Security (ENCS), formerly known as Cyber-TEC.
Type	Public Private Partnership
Line of action	Technical, Education and training, information sharing, R&D
Participants	All stakeholders
Mission/Objectives	ENCS is an independent European public-private collaboration. Their Founding members are Alliander (Dutch DSO), City of The Hague, CPNI.NL, KEMA, KPN (Biggest Dutch Telecom provider), Radboud University Nijmegen and TNO. The idea of ENCS is that it contributes to the resilience of CI by connecting people and organizations, being an information and knowledge sharing catalyst and educating people to the highest management levels. The ENCS will not only focus on the technical, but also on physical and personnel security.
Activities related to ICS security	The ENCS is planned to constantly scan the international arena for relevant developments, innovating and creating new initiatives to enable others. Besides the public-private network of experts and organizations, the ENCS will offer four focus areas: • Research & Development • Test Bed • Information & Knowledge Sharing • Education & Training All four focus areas are interconnected, providing collaborative input and optimal synergy. The ENCS will focus primarily on the protection of smart grids and CI's Process Control Domains. These still present substantial cyber security issues and challenges. To address them, the ENCS will connect existing organisations as the

	European Commission, ENISA, Joint Research Centre and national public and private initiatives across Europe and beyond – collaboration with the DHS Control Systems' Security Program and Idaho National Labs are prime examples.
Results	Technical reports, courses, test bed, etc.
Comments	ENCS was formerly known as Cyber-TEC
URL	N/A

1.3 Germany

Name	BDEW
Type	Industry association
Line of action	Organizational and Policy, Economic or Financial, Technical.
Participants	Manufacturers, Integrators, Operators
Mission/Objectives	The German Association of Energy and Water Industries, BDEW, was founded in autumn 2007 to combine the competencies of four different associations, including: • Federal Association of German Gas and Water Industries (BGW) • Association of regional transmission companies and utilities in Germany (VRE), • Association of Network Operators (VDN) and • Electricity Association (VDEW). It is the central contact point for all questions about natural gas, electricity and district heating, water and sanitation.
Activities related to ICS security	Conducts activities (e.g. studies) related to natural gas, electricity and district heating, water and sanitation. Some of these activities are related to cyber security issues.
Results	Technical reports
Comments	BDEW stands for "Bundesverband der Energie- und Wasserwirtschaft"
URL	www.bdew.de

1.1.2 Name	*1.1.3* NAMUR
Type	Industry association
Line of action	Technical, Standards, Economic or financial, Information sharing
Participants	Manufacturers, Service providers, Operators, Academia

Mission/Objectives	The International User Association for Automation in Process Industries has the following main objectives:
	• Minimizing the costs for member companies arising from process control technology.
	• Enhancing the availability of process control technology.
	• Increasing plant safety.
	• Enabling the exchange of experience among its members and with manufacturers and other associations.
	The main activities carried out by NAMUR are:
	• Interpretation of guidelines, regulations and directives
	• Preparation of check lists as working aids
	• Setting of minimum requirements for equipment and systems
	• Identification of equipment and system development needs
	• Definition of best practice solutions
	• NAMUR member companies openly share information related to automation and process control technology. Experience is pooled for mutual benefit.
	• NAMUR maintains a constructive dialogue with other associations.
	• NAMUR supports national and international standardization through cooperation in the field of automation if this is to the advantage of member companies.
	• The results of NAMUR‘s work are published in:
	  ○ NAMUR recommendations and NAMUR worksheets
	  ○ Presentations at the Annual General Meeting
	  ○ Publications in technical journals

	○ Contributions to workshops and conferences NAMUR recommendations (NE) and NAMUR worksheets (NA) are documents prepared by NAMUR for its members and other interested companies and bodies. • NE usually define best practice procedures or requirements for devices, systems and services in the process industry and are therefore important documents also for manufacturing companies. • NA usually are designed as an aid for member companies in the form of checklists and instructions for practical use.
Activities related to ICS security	NAMUR WA2/AK2.8 (Working Area 2. Automation Systems for Processes and Plants/Working Group 8. Internet/Intranet) is responsible for the creation of "NAMUR NA 115 IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries"
Results	News, Technical reports (recommendations and work-sheets)
Comments	
URL	www.namur.de

Name	VGB
Type	Industry association
Line of action	Technical, Information sharing
Participants	Operators
Mission/Objectives	VGB was already founded as the federation of the owners of large boilers. During its course of 80 years VGB has set off a range of activities in own companies. These companies are dealing with: • training of power plant personnel, • research activities and • the production and distribution of media VGB represents the German power plant operators in the WANO (World Association of Nuclear Operators). VGB's technical committees on nuclear power plant engineering and operation and nuclear fuel cycle we are actively taking part in the world-wide exchange of experience as well as in the analysis of particular events in nuclear power plants. For this purpose, VGB is operating a reporting and evaluation centre (ZMA - Zentrale Melde- und Auswertestelle) to collect, evaluate and forward the occurrences of nuclear power plants.
Activities related to ICS security	They have made contributions to the security of ICS by publishing guidelines and instructions sheets, organising forums and training experts. One of the most important results is the VGB R175 guideline on IT security for generating plants
Results	Standard, technical reports, good practices, conferences
Comments	VGB means Verband der Großkraftwerks-Betreiber.

	As an international technical association for power and heat generation VGB is working - on European level - in close co-operation with EURELECTRIC, the umbrella association of the European electricity industry. Within the framework of a memorandum of understanding association agreement between EURELECTRIC and VGB, VGB's professional competence is integrated into the political/strategic work of EURELECTRIC in all questions regarding the generation of power and heat including issues of environmental protection.
URL	www.vgb.org

Name	VDI
Type	Professional association
Line of action	Technical, Dissemination and awareness, Information sharing, Standards
Participants	Operators
Mission/Objectives	The Association of German Engineers, VDI, is the largest technical and scientific association in Europe. The VDI has successfully expanded its activities, nationally and internationally, committing itself to foster and impart knowledge about technology related issues. As a financially independent, politically unaffiliated and non-profit organization the VDI is recognized as the representative of engineers both within the profession and in public. The VDI covers a wide range of technical topics and communicates this knowledge through studies, technical discussions and congresses or the VDI guidelines that create generally accepted technical rules. As an advisory partner the VDI engages in the relationship between technical and social developments. It focuses on the promotion of young talents and the support of upcoming engineers.
Activities related to ICS security	The most important work done by VDI is the VDI Guidelines which play a very important role as pioneers for international standardization. These guidelines are based on the latest technical developments are produced by the VDI's technical divisions. The VDI/VDE 2182 series are the most relevant guidelines in relation to ICS security.
Results	Studies, technical discussions and congresses, guidelines
Comments	VGB stands for "Verein Deutscher Ingenieure"

URL	http://www.vdi.de/

1.4 United Kingdom

Name	CPNI
Type	Public body
Line of action	Organizational and Policy, Standard, Technical
Participants	N/A
Mission/Objectives	CPNI was formed from the merger of the National Infrastructure Security Coordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC). NISCC provided advice and information on computer network defence and other information assurance issues. NSAC provided advice on physical security and personnel security issues. CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure. Through the delivery of this advice, they protect national security, by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.
Activities related to ICS security	CPNI has created several interesting guidelines on ICS security, such as "Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks" (National Infrastructure Security Coordination Centre (NISCC), 2005) and "Good Practice Guide - Process Control and SCADA Security, Overview, Parts 1 to 7" (Centre for the Protection of Critical Infrastructure (CPNI)).
Results	Technical reports, good practices
Comments	Centre for the Protection of National Infrastructure
URL	www.cpni.gov.uk

Name	Byres Security Blog
Type	Online resource
Line of action	Dissemination and Awareness, Technical
Participants	N/A
Mission/Objectives	• To avoid malicious and accidental network incidents with practical how-to suggestions. • To understand current security threats and what to do with them.
Activities related to ICS security	Byres security is a private company that develops technology to secure the ICS networks. Additionally, they create whitepapers, vulnerability advisories, educational videos, and technical presentations which are then published on this blog.
Results	Whitepapers, vulnerability advisories, educational videos, technical presentations, how-to suggestions.
Comments	
URL	www.tofinosecurity.com/blog

1.5 The Netherlands

Name	WIB
Type	Industry association
Line of action	Standards, Dissemination and Awareness, Technical.
Participants	Manufacturers and Integrators
Mission/Objectives	WIB provides process instrumentation, evaluation and assessment services for and on behalf of its industrial user member companies. WIB operates in close collaboration -through the 'SWE' federation- with 'sister' Associations, EXERA in France and SIREP/EI in the UK.
Activities related to ICS security	• WIB facilitates the exchange of experiences and expertise amongst end-users and with vendors of C&A. • WIB provides requirements, selection and application guidance through independent evaluation. • WIB has developed a “security requirements for vendors” report about the security capabilities the devices need (see section **Error! Reference source not found.**).
Results	Standards, technical reports, services
Comments	A co-operation agreement exists with the NAMUR organisation in Germany.
URL	www.wib.nl

Name	National Risk Assessment
Type	Other
Line of action	Standards, Dissemination and Awareness, Technical.
Participants	All stakeholders
Mission/Objectives	Under the command of security and justice Ministry of The Netherlands, this initiative is devoted to the protection of all critical infrastructures that are throughout the country. Its main activity includes the development of a series of guidelines and recommendations for national protection.
Activities related to ICS security	In the Dutch National Risk Assessment of 2009 a scenario was created on hacking SCADA-systems in the Energy sector (Rijksoverheid, 2009)
Results	Standards, technical reports, services
Comments	
URL	http://www.rijksoverheid.nl/

Name	CPNI.NL
Type	Public body
Line of action	Organizational and Policy, Standards, Technical
Participants	N/A
Mission/Objectives	CPNI.NL is a public private platform to protect national security. Its objective is to improve and extend information sharing between private industry and the Government when it comes to critical national infrastructure.
Activities related to ICS security	Under the umbrella of the CPNI.NL there are several on-going initiatives. The most relevant ones with respect to ICS security are the following: **Cybercrime Information Exchange (IE)**: This workgroup consists of 12 ISACs. An ISAC is a safe environment in which public and private parties exchange confidential and sensitive information about threats and best practices. The CPNI.NL takes part in each ISAC as a neutral party and facilitates the meetings. In the ISACs, critical infrastructures and government (KLPD, AIVD and GOVCERT.NL) share information about incidents, threats, vulnerabilities and good practices. The security of the Process Control Domain is a recurring topic in a lot of these ISACs (e.g. the Energy-ISAC, Water-ISAC, Airport-ISAC, Multinationals-ISAC, Nuclear-ISAC, PCS-Vendors-ISAC) and also the topic of intersectoral ISACs (e.g. Energy and Drinking Water). **National Roadmap to Secure Process Control Systems:** It is a set of activities to raise the level of resilience and security of PCS. The products of the roadmap are: • Building the network, national and international (e.g. meetings, conferences, PCS-vendors-ISAC, EuroSCSIE and MPCSIE)

	• Open source Intelligence with LinkedIn group PCS Roadmap NL as subgroup of "Samen tegen Cybercrime"(United against Cybercrime) and Twitter account (@PCS_Roadmap_NL) • PCS Security Benchmarks (Energy- and Water-ISAC) – Restricted, available at CPNI.NL • PCS Security Brochure for management • SCADA Security Best Practices for the Drinking Water sector • Exercise scenarios for the Process Control Domain (made by the Dutch Drinking Water companies) – Restricted, available through CPNI.NL • White papers (working now on 2 white papers: 'Threat Landscape ICS' and 'How to deal with Legacy Systems'. More will follow like one on 'How to deal with Removable Media') • Education & Training (e.g. 40 representatives of Dutch CI operators do the Red-Blue team training at INL in the US in the week of 10-14 October 2011).
Results	Information exchange, good practices, policies
Comments	
URL	www.cpni.nl

Name	Working Group Privacy and Security of Smart Grids of Netbeheer Nederland
Type	Industry association
Line of action	Technical
Participants	All stakeholders
Mission/Objectives	This initiative is the point of contact for matters affecting the energy market, such as environmental issues, free market performance and security of supply. EnergieNed is the forum in which energy producers consult each other on issues such as the environment and investment conditions, traders consult each other on the functioning of the wholesale market and the integration of European markets, and retailers discuss a wide range of topics varying from stimulation of energy saving to consumer protection.
Activities related to ICS security	This working group wrote the document 'Privacy and Security of the Advanced Metering Infrastructure' which can be found on (Energiened)
Results	Information exchange, good practices
Comments	This working group is very active on this topic on a European level.
URL	http://www.energiened.nl/

1.6 Norway

Name	OLF
Type	Industry association
Line of action	Technical
Participants	Manufacturers, Integrators, Operators
Mission/Objectives	OLF, the Norwegian Oil Industry Association is a professional body and employer's association for oil and supplier companies engaged in the field of exploration and production of oil and gas on the Norwegian Continental Shelf. OLF is a member of the Confederation of Norwegian Business and Industry (NHO). Its main goal is to look after the member companies joint interests towards government, employer organizations, other national and international institutions, organizations and society in general.
Activities related to ICS security	OLF has made some guidelines for ICS protection. The most remarkable guide is “Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems” (Norwegian Oil Industry Association (OLF), 2009). The objective of the guideline is to improve the overall information security of the offshore industry and thereby improving the safety and regularity of the operations on the Norwegian continental shelf.
Results	Environmental reports, guidelines
Comments	Norwegian Oil Industry Association
URL	www.olf.no/en

1.7 Spain

Name	AMETIC
Type	Industry association
Line of action	Organizational and Policy, Economic or Financial
Participants	Security tools and services providers and other companies of the ICT sector.
Mission/Objectives	AMETIC is the industry association of Information Technology and Electronics companies. Among its objectives it is worth mentioning the following ones: • To represent and defend its members. • To build, encourage and promote the information society and the development of eLife. • To cooperate with public and private bodies, both national and international in the Spanish ICT growing sector. • To achieve the goals which are good for the ICT sector. • To support areas of activity of its partners. • To foster collaboration and solidarity among. • To collaborate with associated companies to provide services and advice on the ICT sector.
Activities related to ICS security	This association organises a series of seminars where one of the main topics of discussion are critical infrastructures and industrial environments. Their areas of expertise are varied, but among them, we highlight ICS and home automation. For more information check (Goméz, 2011). This association has several initiatives related to cyber security, such as eSec, which promotes the creation of major research projects in cooperation, develops a new version of the Strategic Research Agenda, advises national managers in defining their

	national programmes and disseminates relevant information in the field of security Networking (eSEC).
Results	Technical reports
Comments	
URL	www.ametic.es/organizations.aspx

Name	CNPIC
Type	Public body
Line of action	Organisational and policy, Standards
Participants	N/A
Mission/Objectives	The National Centre for the Protection of Critical Infrastructure (CNPIC) is the leading and coordinating office for every activity related to the protection of critical infrastructure assigned to the Secretariat of State for Security of the Ministry of the Interior. Its main objective is to ensure efficient cooperation and advice businesses and operators, in order to improve the protection of the Spanish critical infrastructures that provide essential services to our society.
Activities related to ICS security	All exposed in Mission/Objectives. To be highlighted the Law and associated Royal Decree on Critical Infrastructures Protection.
Results	Regulatory policies
Comments	CNPIC stands for "Centro Nacional para la Protección de Infraestructuras Críticas"
URL	www.cnpic-es.es

Name	GIPIC
Type	Public Private Partnership
Line of action	Organizational and Policy, Technical
Participants	Public bodies, Security tools and services providers.
Mission/Objectives	The GIPIC aims to develop minimum content guidelines and best practices to guide and assist future operators in the preparation of Critical Security Plan (OSP) and Specific protection Plans (EPP) within the responsibilities and functions deriving from the Law 8 / 2011 of 28 April and the Royal Decree 704 / 2011, May 20, which are the Regulation on the protection of critical infrastructure.
Activities related to ICS security	See Mission/Objectives.
Results	Technical reports, Partnership
Comments	GIPIC stands for “Grupo de Trabajo Informal sobre Protección de Infraestructuras Críticas”
URL	https://gipic.isdefe.es

Name	Protect-IC
Type	R&D project
Line of action	Technical
Participants	Manufacturers, Security providers, Operators, Academia and R&D
Mission/Objectives	To develop new ICS specific security tools for critical infrastructures protection.
Activities related to ICS security	• Analysis and classification of vulnerabilities, threat modelling and auditing of ICS. • Research and development of secure architectures, robust and reliable systems for ICS. • Analysis and risk management in the field of critical infrastructures. • Study of techniques and creation of tools for forensic analysis in ICS.
Results	Technical reports
Comments	
URL	http://www.nics.uma.es/ProtectIC/

Name	Test bed Framework for Critical Infrastructure Protection Exercise (Cloud CERT),
Type	Other
Line of action	Organizational and Policy, Technical, Information sharing, Dissemination and awareness.
Participants	Public bodies, Security tools and services providers
Mission/Objectives	To promote the security culture and the intercommunication between CERTs.
Activities related to ICS security	The project aims to simulate a real environment of collaboration between CERTs in different EU member states, so as to join efforts and to promote coordination on critical infrastructure protection. In this way, it will be possible to achieve a greater exchange of knowledge to obtain the best results related to information security in facilities, networks, equipment and services whose interruption would have a major impact on health, safety, welfare of citizens, or operation of the authorities.
Results	Technical reports
Comments	
URL	www.inteco.es

Name	PESI
Type	Public Private Partnership
Line of action	Dissemination and Awareness, Organizational and Policy, Technical, R&D
Participants	Manufacturers, Integrators, Research & Academia
Mission/Objectives	The Spanish Technology Platform on Industrial Safety, set up in October 2005, **promotes Industrial Safety issues**, integrating all the agents interested on **research and technological developments.** At the same time, it also contributes to define its own necessities and ideas to improve the Strategic Research Agenda. The main objective is to develop a general view about Industrial Safety to promote and boost research activities, technological development and innovation to improve safety in industrial activities. The deployment areas are: • Product & Installation Safety • Occupational Safety & Health • Environmental Safety • Enterprise Security
Activities related to ICS security	PESI includes many activities related with ICS protection: • Promote industrial safety • Identify existing gaps in research. • Establish a coherent strategy and plan of action. • Develop a Strategic Research Agenda, setting their priorities. • Promote R&D for promoting Spanish competitiveness, in line with the European. • Help partners to develop R & D in the European Union. • Establish cooperative action to boost R & D at the regional and national levels. • Getting support from the European Commission and the Spanish government to finance R & D in industrial safety.

Results	Technical reports, guidelines and events.
Comments	
URL	http://www.pesi-seguridadindustrial.org/.

1.8 Sweden

Name	SEMA
Type	Public body
Line of action	Dissemination and Awareness
Participants	N/A
Mission/Objectives	The Swedish Emergency Management Agency co-ordinates the work to develop the preparedness of the Swedish society to manage serious crises. SEMA works together with municipalities, county councils and government authorities, as well as the business community and several organisations, to reduce the vulnerability of Society and to improve the capacity to handle emergencies.
Activities related to ICS security	The support that SEMA is able to provide in the event of a crisis may include advice and expert support within areas such as crisis communication and management methodology. SEMA should also assist the Government Offices with updated situation reports. To carry out this task, the authority has an established network of county administrative boards, central authorities and others that may be affected by or have knowledge of an emergency situation. SEMA also co-ordinates the planning, resource allocation, follow-up and evaluation of work within the area of crisis management. Furthermore, SEMA collects knowledge through horizon scanning, strategic analyses and research to develop society's emergency management.
Results	Technical reports
Comments	SEMA stands for Swedish Emergency Management Agency
URL	http://www.krisberedskapsmyndigheten.se

Name	The MSB Industrial Control System Security Program
Type	Other (Swedish ICS Security national programme)
Line of action	Dissemination and Awareness, Information sharing, Technical, Organisational and Policy
Participants	Public bodies and private sector
Mission/Objectives	The MSB develops, in collaboration with other stakeholders, the individual's and society's capacity to prevent, deal with and learn from emergencies and disasters. The agency operates via knowledge-building, support, education, training, regulation, supervision and its own operational work, to achieve increased safety and security at all levels of society – from the local to the global community. The MSB shall support and coordinate societal information security work, as well as analyse and assess global developments in this field. This includes providing advice and support in matters related to preventative work to other government authorities, the municipalities and the country councils, as well as the private sector and organisations. The MSB also reports to the government on conditions in the information security field that can give rise to a need for measures on different levels and within different areas of society. Furthermore, the MSB shall also be responsible for a Swedish national service tasked with supporting society in efforts to prevent and mange IT incidents. For this work the MSB shall (i) respond promptly when IT incidents occur by spreading information and where needed work with the coordination of measure, and partake in work to remedy or mitigate the incident's consequences; (ii) cooperate with authorities that have specific tasks in the field of information security, and; (iii) act as Sweden's point of contact for equivalent services in other countries, and develop cooperation and information exchanges with them.
Activities related to ICS security	The MSB's work on issues related to cyber security in industrial information and control systems is conducted within the framework of a multiannual national program – the MSB Industrial Control System Security Program. The aim of the program is to create an increased national capacity for the prevention and handling of IT related risks and threats against the IT systems that control vital societal services and critical infrastructure. The goal of the program is to develop private-public partnerships, to increase the technical

	capabilities and competence in the society, and to provide practical support to end users in order to increase the cyber security of industrial control systems. The program consists of four program areas: • Technical platform for collaboration – together with the Swedish Defence Research Agency (FOI), activities include e.g. technical studies, exercises, and training. • Awareness raising – activities include e.g. seminars and dissemination of best practices. • Information sharing and cooperation – activities include e.g. the national private-public information exchange forum FIDI-SC, and representation in the E-SCSIE and other international groups. The national cooperation also includes work through the Cooperation group for information security (SAMFI), which includes representatives from the Swedish Post and Telecom Agency; the Swedish National Police Board; the Swedish Armed Forces; the Swedish National Defence Radio Establishment; the Swedish Defence Material Administration, and the MSB. • Planning and program development – policy and strategy support, as well as cooperation with MSB R&D funding schemes.
Results	Information sharing and awareness, national platform for technical collaboration, exercises and training, guidance and good practice, policy and strategy support
Comments	• MSB is the Swedish Civil Contingencies Agency. • CERT-SE is Sweden's national Computer Emergency Response Team (CERT). Since 1 January 2011 CERT-SE has been a part of MSB.
URL	http://www.msb.se/scada

1.9 USA

Name	ACC
Type	Industry association
Line of action	Economic or Financial, Organisational and policy, dissemination and awareness.
Participants	Manufacturers, Integrators, Security tools and services providers, Operators.
Mission/Objectives	The American Chemistry Council's (ACC's) mission is to deliver business value through exceptional advocacy using best-in-class member performance, political engagement, communications and scientific research. We are committed to sustainable development by fostering progress in our economy, environment and society. ACC supports public policies that will drive creation of groundbreaking products that improve lives and our environment, enhance the economic vitality of communities and protect public health.
Activities related to ICS security	The ACC has organised several workshops to raise awareness about the importance of safety in industrial environments, especially in the chemical industry. They have also supported the Introduction of Senate Cyber security Legislation.
Results	Conferences, technical reports
Comments	ACC stands for American Chemistry Council
URL	www.americanchemistry.com

Name	AGA
Type	Industry association
Line of action	Organizational and Policy, Standards, Dissemination and Awareness, Technical.
Participants	Operators
Mission/Objectives	The American Gas Association represents companies delivering natural gas to customers to help meet their energy needs. AGA members are committed to delivering natural gas safely, reliably, cost-effectively and in an environmentally responsible way. AGA advocates the interests of its members and their customers, and provides information and services promoting efficient demand and supply growth, and operational excellence, in the safe, reliable and efficient delivery of natural gas. To further this mission, AGA: • Focuses on the advocacy of natural gas issues • Promotes growth in the efficient use of natural gas on behalf of natural gas utilities • Encourages, facilitates and assists members in sharing information designed to achieve operational excellence • Assists members in managing and responding to customer energy needs, regulatory trends, natural gas markets, capital markets and emerging technologies • Collects, analyzes and disseminates information on a timely basis to opinion leaders, policy makers and the public • Encourages the identification, development, commercialization, demonstration and regulatory acceptance of end-use technologies • Delivers measurable value to AGA members.
Activities related to ICS	AGA's most prominent contributions to ICS security are:

security	• Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry. • Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan (Interstate Natural Gas Association of America (INGAA), 2011).
Results	Technical reports, Standard
Comments	American Gas Association
URL	www.aga.org

Name	API
Type	Industry association
Line of action	Organizational and Policy, Standards, Dissemination and Awareness, Technical.
Participants	Manufacturers and Integrators, Security Tools and services providers, Operators
Mission/Objectives	The American Petroleum Institute (API) is the only national trade association that represents all aspects of America's oil and natural gas industry. Among its objectives, API: • Takes part in federal and state legislative and regulatory advocacy that is based on scientific research; technical legal and economic analysis; and public issues communication. • Provides an industry forum to develop consensus policies and collective action on issues impacting its members. • Works collaboratively with all industry oil and gas associations, and other organizations, to enhance industry unity and effectiveness in its advocacy.
Activities related to ICS security	API has developed the following security guidelines for industrial control systems: • API 1164, Pipeline SCADA Security • Security Guidelines for the Petroleum Industry (American Petroleum Institute (API) energy, 2005).
Results	Technical reports, Standards, Certification
Comments	American Petroleum Institute
URL	www.api.org

Name	DoE
Type	Public body
Line of action	Standards, Dissemination and Awareness, Technical
Participants	N/A
Mission/Objectives	The mission of the Energy Department is to ensure America's security and prosperity by addressing its energy, environmental and nuclear challenges through transformative science and technology solutions. Among its main objectives we highlight the following ones: • Catalyze the timely, material, and efficient transformation of the nation's energy system and secure U.S. leadership in clean energy technologies • Maintain a vibrant U.S. effort in science and engineering as a cornerstone of our economic prosperity with clear leadership in strategic areas. • Enhance nuclear security through defence, non-proliferation, and environmental efforts. • Establish an operational and adaptable framework that combines the best wisdom of all Department stakeholders to maximize mission success.
Activities related to ICS security	DoE has a cyber security department and they have organised conferences about cyber security (Department of Energy (DoE), 2010). The DoE also has a library with various publications on Control Security Systems, research articles, training materials and Vulnerability Reports and recommended practices (Department of Energy (DoE)). Among the most interesting publications it is worth highlighting the following ones:

	• 21 Steps to improve Cyber Security for SCADA systems • Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities
Results	Technical reports, conferences, training material, research articles.
Comments	Department of Energy
URL	www.energy.gov

Name	DHS
Type	Public body
Line of action	Standards, Dissemination and Awareness, Technical
Participants	N/A
Mission/Objectives	The mission of the Department of Homeland Security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. Among its objectives, we highlight the following ones: • Prevent terrorism and enhance security. • Secure and manage borders. • Enforce and administer immigration laws. • Safeguard and secure cyberspace. • Ensure resilience to disasters. • Mature and strengthen the DHS.
Activities related to ICS security	DHS carries out a very important work on de cyber security in all environments, included ICS. For instance, the DHS organises dissemination activities on the security of critical infrastructures (Department of Homeland Security (DHS), 2011), as well as training activities with guided learning based on practical exercises. The DHS also makes technical documents among which one can find ICS security recommendations (Berkeley III & Wallace, 2010). We highlight the following ones: • Cyber Security Assessments of Industrial Control Systems. A good practice guide (joint effort between the UK's CPNI and the DHS) • Configuring and managing remote access for industrial control systems. A good practice guide (joint effort between the UK's CPNI and the DHS)

	• Catalogue of Control Systems Security: Recommendation for Standards Developers • Securing you SCADA and Industrial Control Systems
Results	Technical reports
Comments	Department of Homeland Security
URL	www.dhs.gov

Name	NERC
Type	Public Private Partnership
Line of action	Standards, Dissemination and Awareness, Technical
Participants	Manufacturers and Integrators, Security Tools and services providers, Operators, Public bodies, Standardisation bodies
Mission/Objectives	The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk-power system. Among other activities, NERC: • Works with the industry to develop reliability standards • Enforces compliance with those reliability standards and assesses monetary and non-monetary penalties for noncompliance • Assesses future bulk power system reliability via annual summer, winter and 10-year forecasts • Analyzes system events • Promotes a culture of excellence by identifying areas for improvement and Examples of Excellence during regular "readiness" evaluations • Monitors the status of the bulk power system • Coordinates physical and cyber security needs • Identifies trends and potential reliability issues • Helps the industry train and educate system operators • Certifies system operators
Activities related to ICS security	NERC has developed the NER-CIP Standards, a nine documents series about security and cyber security aspects of the Bulk Electric System in the USA. Two new documents are being developed.

	Based on these documents, NERC provides specific guidelines and concept papers. This is the case of the "Categorization system based on Bulk Electric System Reliability Functions" (North American Electric Reliability Corporation (NERC), 2009).
Results	Technical reports, Regulatory documents
Comments	North American Electric Reliability Corporation
URL	www.nerc.com

Name	NIST
Type	Public body
Line of action	Organizational and Policy, Standards, Dissemination and Awareness, Economic or Financial, Technical
Participants	N/A
Mission/Objectives	NIST, an agency of the U.S. Department of Commerce, was founded in 1901 as the nation's first federal physical science research laboratory Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Activities related to ICS security	NIST is one of the most important standardisation organizations in the USA. They have developed several standards on ICS security. We highlight the following ones: • NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security. • NIST SP 800-53, Recommended Security Controls for Federal Information Systems. • Field Device Protection Profile for SCADA Systems in Medium Robustness Environments. • NISTIR 7176, System Protection Profile – Industrial Control Systems. NIST has also defined a security smart grid workgroup to develop an overall cyber security strategy for the Smart Grid. This overall strategy includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure (Smart Grid Interoperability Panel (SGIP)). This group

	has created the following document of interest: ○ NISTIR 7628, Guidelines for Smart Grid Cyber Security (National Institute of Standards and Technology (NIST), 2010).
Results	Technical reports, Standards, good practices
Comments	NIST stands for National Institute for Standards and Technology
URL	www.nist.gov

Name	Digital Bond- S4 workshop
Type	Specialised event
Line of action	Dissemination and Awareness, Technical.
Participants	Manufacturers and Integrators, Security Tools and services providers, Operators
Mission/Objectives	Digital Bond is a private company specialised in ICS security services. It provides consulting services, but also focuses on research, and it also offers a control system security portal with several resources: blog, SCADApedia, etc.
Activities related to ICS security	Digital Bond organises on a year basis the S4 workshop which targets key questions related with ICS security, like technical solutions, new devices, vulnerabilities, etc. It is mainly a technical conference for a technical audience.
Results	Technical solutions
Comments	S4 stands for SCADA Security Scientific Symposium
URL	www.digitalbond.com

Name	TISP
Type	Public Private Partnership
Line of action	Organizational and Policy, Technical
Participants	All stakeholders
Mission/Objectives	Eleven professional and technical organizations and federal agencies formed The Infrastructure Security Partnership (TISP) as a non-profit partnership to be a national asset facilitating dialogue on domestic infrastructure security and offering sources of technical support and sources for comment on public policy, related to the security of the nation's built environment. TISP activities provide opportunities to its members for partnering on projects, for peers to learn from one another, for sharing relevant information during key discussions, and to raise awareness among the decision makers and the general public. TISP activities include quarterly technical forums, roundtable discussions and workshops, and co-sponsored events.
Activities related to ICS security	ICS security is a key topic among the activities of TISP (see Mission/Objectives).
Results	Technical reports, guidelines, good practices
Comments	The Infrastructure Security Partnership
URL	www.tisp.org

Name	SCADA hacker
Type	Online resource
Line of action	Dissemination and Awareness, Technical.
Participants	Public access
Mission/Objectives	The goal of SCADAhacker is best broken down into two equally important pieces. First, to take something like information security and make it simple for those involved in industrial control systems to easily understand. Teach and present complexity over time, simply! Next, SCADAhacker aims at educating those who show a sincere desire to learn of the intricacies that make infosec complex. The net result is a more receptive readership that both understands the importance of infosec in protecting the automation systems that control our critical infrastructure, and knows the steps necessary to improving the overall security posture of the resulting solution. This encompasses the people that use the systems, the processes that are employed with these systems, and the security products that help provide defence-in-depth or DiD through various layers of protection from attacks that can originate from outside and inside the physical perimeter of the manufacturing facility under control of the system.
Activities related to ICS security	There are a good number of resources and services provided by SCADAhacker. However, we highlight the following ones: • Security services specifically related to SCADA systems, including: risk exposure analysis, security assessments, gap analysis, vulnerability assessments, penetration testing, and standards compliance. • Training services covering security awareness, SCADA

	security, security program development, SCADA exploitation and hardening. • A collection of tools used to build the ideal "Hackers Toolbox". • Dashboard of current trends and threats SCADA specific information like advisories, threats, vulnerability disclosure, white papers, and much more.
Results	Technical reports, training programs, Technical solutions
Comments	
URL	http://www.scadahacker.com/ http://scadahacker.blogspot.com/

1.10 Other web 2.0 initiatives

Name	SCADAsec
Type	Online resource
Line of action	Dissemination and Awareness, Technical
Participants	Public access
Mission/Objectives	This group forum is about security discussions, trends and overall discussions pertaining to 'critical infrastructure protection' and SCADA/control systems. To provide education and training awareness programs for both public and private sectors, as well as for the general public. Information, its availability, and its dissemination, are vital in securing our Nation's infrastructures.
Activities related to ICS security	See Mission/Objectives
Results	
Comments	A mailing list on ICS security.
URL	http://news.infracritical.com/mailman/listinfo/scadasec

Name	SCADA/Control System Security Professionals
Type	Online resource
Line of action	Technical
Participants	All stakeholders
Mission/Objectives	This group is for professionals who are responsible for securing and controlling SCADA/Control Systems, including those trying to meet NERC CIP compliance requirements. The group was started by CoreTrace Corporation who provide solutions in this industry.
Activities related to ICS security	All exposed in Mission/Objectives
Results	
Comments	LinkedIn group
URL	http://www.linkedin.com/groups?home=&gid=1629767

Name	Water Security
Type	Online resource
Line of action	Technical
Participants	All stakeholders
Mission/Objectives	This group was created for all those involved in securing water infrastructures against contamination and emergencies. The goal is to allow knowledge sharing, discussion of dilemmas and new methods with colleagues, post questions, promote your own water security/technology, and general communication about managing our water utilities. This group is part of a wider mission to share knowledge of the field and encourage higher security of water as a critical public resource.
Activities related to ICS security	Refer to Mission/Objectives and Results sections
Results	Among the topics for discussion, one can find the following ones: ○ Potential discussion topics ○ EPA regulation for Utilities ○ Water Crisis prevention and management techniques ○ Anti-terrorism intelligence ○ Water quality monitoring ○ Fast recovery from water crisis events
Comments	LinkedIn group
URL	http://www.linkedin.com/groups?home=&gid=2751785

Name	Cyber Security in Real-Time Systems:
Type	Online resource
Line of action	Technical
Participants	Security Tools and services providers
Mission/Objectives	This group consists of professional security consultants who have experience in Real-Time security threats
Activities related to ICS security	It is mainly a discussion forum, where experts hare their opinion on trending topics regarding cyber security in real-time systems.
Results	
Comments	LinkedIn group
URL	http://www.linkedin.com/groups?gid=3623430

2. References

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

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

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

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

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

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

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

Amin, S., Sastry, S., & Cárdenas, A. A. (2008). *Research Challenges for the Security of Control Systems.*

Asad, M. (n.d.). *Challenges of SCADA.* Retrieved 2011, from http://www.ceia.seecs.nust.edu.pk/pdfs/Challenges_of_SCADA.pdf

Bailey, D., & Wright, E. (2003). *Practical SCADA for Industry.* Newnes.

Berkeley III, A. R., & Wallace, M. (2010). *A Framework for Establishing Critical Infrastructure Resilience Goals. Final Report and Recommendations by the Council.* National Infrastructure Advisory Council.

Boyer, S. A. (2004). *SCADA Supervisory and Data Acquisition.* Retrieved 2011, from http://www.fer.unizg.hr/_download/repository/SCADA-Supervisory_And_Data_Acquisition.pdf

Boyer, S. A. (2010). *SCADA: Supervisory Control and Data Acquisition.* Iliad Development Inc., ISA.

Centre for the Protection of Critial Infrastructure (CPNI). (n.d.). *Meridian Process Control Security Information Exchange (MPCSIE)*. Retrieved 2011, from http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie

Centre for the Protection of Critical Infrastructure (CPNI). (n.d.). *CPNI*. Retrieved 2011, from http://www.cpni.gov.uk/advice/infosec/business-systems/scada

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

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

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

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 1. Understand the business risk.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 2. Implement secure architecture.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 3. Establish response capabilities.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 4. Improve awareness and skills.* Centre for the Protection of National Infrastructure.

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 5. Manage third party risk.* Centre for the Protection of National Infrastructure.

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

Centre for the Protection of National Infrastructure (CPNI). (n.d.). *Process control and SCADA security. Guide 7. Establish ongoing governance.* Centre for the Protection of National Infrastructure.

CI2RCO Project. (2008). *Critical information infrastructure research coordination*. Retrieved 2011, from http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=79305

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

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

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

Commission of the European communities. (2005). *Green paper. On a European programme for critical infrastructure protection COM(2005) 576 final.*

Commission of the European communities. (2006). *Communication from the commission on a European Programme for Critical Infrastructure Protection COM(2006) 786.*

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

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

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

Commission of the European communities. (2009). *Communication from the commission to the European parliament. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience.*

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

CRUTIAL Project. (2006). *CRitical Utility InfrastructurAL resilience*. Retrieved 2011, from http://crutial.rse-web.it

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

Department of Energy (DoE). (2008). *Hands-on Control Systems Cyber Security Training of National SCADA Test Bed.* Retrieved 2011, from http://www.inl.gov/scada/training/d/8hr_intermediate_handson_hstb.pdf

Department of Energy (DoE). (2010). *Cybersecurity for Energy Delivery Systems Peer Review.* Retrieved 2011, from http://events.energetics.com/CSEDSPeerReview2010

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

Department of Energy (DoE). (n.d.). *Control Systems Security Publications Library*. Retrieved 2011, from http://energy.gov/oe/control-systems-security-publications-library

Department of Homeland Security (DHS). (2003). *Homeland Security Presidential Directive-7.* Retrieved 2011, from http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1

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

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

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

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

Department of Homeland Security (DHS). (2011). *DHS officials: Stuxnet can morph into new threat.* Retrieved 2011, from http://www.homelandsecuritynewswire.com/dhs-officials-stuxnet-can-morph-new-threat

DigitalBond. (n.d.). *DigitalBond.* Retrieved 2011, from ICS Security Tool Mail List: http://www.digitalbond.com/tools/ics-security-tool-mail-list

Energiened. (n.d.). *Energiened Documentation*. Retrieved 2011, from http://www.energiened.nl/Content/Publications/Publications.aspx

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

ESCoRTS Project. (2008). *Security of Control and Real Time Systems*. Retrieved 2011, from http://www.escortsproject.eu

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

eSEC. (n.d.). *eSEC*. Retrieved from Plataforma Tecnológica Española de Tecnologías para Seguridad y Confianza: http://www.idi.aetic.es/esec

European Network and Informations Security Agency (ENISA). (2010). Retrieved 2011, from EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection: http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

Falliere, N., Murchu, L. O., & Chien, E. (2011). *W32.Stuxnet Dossier.* Symantec.

Gartner. (2008). *Assessing the Security Risks of Cloud Computing.* Retrieved 2011, from Gartner: http://www.gartner.com/DisplayDocument?id=685308

Ginter, A. (2010). *An Analysis of Whitelisting Security Solutions and Their Applicability in Control Systems.* Retrieved 2011

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

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

Holstein, D. C., Li, H. L., & Meneses, A. (2010). *The Impact of Implementing Cyber Security Requirements using IEC 61850.*

Holstein, D. K. (2008). *P1711 "The state of closure".* PES/PSSC Working Group C6.

Huntington, G. (2009). *NERC CIP's and identity management.* Huntington Ventures Ltd.

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

Iinternational Atomic Energy Agency (IAEA). (2011). *IAEA Technical Meeting on Newly Arising Threats in Cybersecurity of Nuclear Facilities.* Retrieved 2011, from http://www.iaea.org/NuclearPower/Downloads/Engineering/files/InfoSheet-CybersecurityTM-May-2011.pdf

INSPIRE Project. (2008). *INcreasing Security and Protection through Infrastructure REsilience*. Retrieved 2011, from http://www.inspire-strep.eu

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

Institute of Electrical and Electronics Engineers (IEEE). (2000). *IEEE PES Computer and Analytical Methods SubCommittee*. Retrieved 2011, from http://ewh.ieee.org/cmte/psace/CAMS_taskforce.html

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

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

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *E7.1402 - Physical Security of Electric Power Substations.* http://standards.ieee.org/develop/wg/E7_1402.html.

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *IEEE Power & Energy Society*. Retrieved 2011, from http://www.ieee-pes.org

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

Institute of Electrical and Electronics Engineers (IEEE). (n.d.). *WGC6 - Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.* http://standards.ieee.org/develop/wg/WGC6.html.

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

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

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

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

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

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

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

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

International Federation for Information Processing (IFIP). (n.d.). *IFIP TC 8 International Workshop on Information Systems Security Research*. Retrieved 2011, from http://ifip.byu.edu

International Federation for Information Processing (IFIP). (n.d.). *IFIP Technical Committees*. Retrieved 2011, from http://ifiptc.org/?tc=tc11

International Federation for Information Processing (IFIP). (n.d.). *IFIP WG 1.7 Home Page*. Retrieved 2011, from http://www.dsi.unive.it/~focardi/IFIPWG1_7

International Federation of Automatic Control (IFAC). (n.d.). *TC 3.1. Computers for Control — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/3/1

International Federation of Automatic Control (IFAC). (n.d.). *TC 6.3. Power Plants and Power Systems — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/6/3

International Federation of Automatic Control (IFAC). (n.d.). *Working Group 3: Intelligent Monitoring, Control and Security of Critical Infrastructure Systems — IFAC TC Websites*. Retrieved 2011, from http://tc.ifac-control.org/5/4/working-groups/copy2_of_working-group-1-decentralized-control-of-large-scale-systems

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

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

International Society of Automation (ISA). (n.d.). *ISA99 Committee - Home*. Retrieved 2011, from http://isa99.isa.org/ISA99 Wiki/Home.aspx

International Society of Automation (ISA). (n.d.). *LISTSERV 15.5 - ISA67-16WG5.* Retrieved 2011, from http://www.isa-online.org/cgi-bin/wa.exe?A0=ISA67-16WG5

INTERSECTION Project. (2008). *INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks (INTERSECTION)*. Retrieved 2011, from http://www.intersection-project.eu

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

IRRIIS Project. (2006). *Homepage of the IRRIIS project*. Retrieved 2011, from http://www.irriis.org

Jeff Trandahl, C. (2001). *USA Patriot Act (H.R. 3162).* Retrieved 2011, from http://epic.org/privacy/terrorism/hr3162.html

Masica, K. (2007). *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.*

Masica, K. (2007). *Securing WLANs using 802.11i. Draft. Recommended Practice.*

McAfee. (2011). *Global Energy Cyberattacks: "Night Dragon".* Retrieved 2011, from http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Meridian. (n.d.). *Meridian*. Retrieved 2011, from http://www.meridian2007.org

National Infrastructure Security Coordination Centre (NISCC). (2005). *Firewall deployment for scada and process control networks. good practice guide.* National Infrastructure Security Coordination Centre.

National Infrastructure Security Coordination Centre (NISCC). (2005). *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* British Columbia Institute of Technology (BCIT).

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

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

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

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

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

North American Electric Reliability Corporation (NERC). (2009). *Categorizing Cyber Systems. An Approach Based on BES Reliability Functions. Cyber Security Standards Drafting Team for Project 2008-06 Cyber Security Order 706.*

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

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

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

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

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

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

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

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

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

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

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

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

Open Smart Grid. (n.d.). *Open Smart Grid*. Retrieved 2011, from http://osgug.ucaiug.org/default.aspx

Rijksoverheid. (2009). *Scenario's Nationale Risicobeoordeling 2008/2009.* Retrieved 2011, from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/10/21/scenario-s-nationale-risicobeoordeling-2008-2009.html

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*.

SANS. (1989). *SCADA Security Advanced Training*. Retrieved 2011, from http://www.sans.org/security-training/scada-security-advanced-training-1457-mid

SANS. (2011). *The 2011 Asia Pacific SCADA and Process Control Summit - Event-At-A-Glance*. Retrieved 2011, from http://www.sans.org/sydney-scada-2011

Smart Grid Interoperability Panel (SGIP). (n.d.). *SGIP Cyber Security Working Group (SGIP CSWG)*. Retrieved 2011, from http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

Smith, S. S. (2006). *The SCADA Security Challenge: The Race Is On.*

Stouffer, K. A., Falco, J. A., & Scarfone, K. A. (2011). *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed*

Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology.

Suter, M., & Brunner, E. M. (2008). *International CIIP Handbook 2008 / 2009.*

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

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

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

The White House. (2001). *Executive Order 13231.* Retrieved 2011, from http://www.fas.org/irp/offdocs/eo/eo-13231.htm

The White House. (2007). *National Strategy for Information Sharing.* Retrieved 2011, from http://georgewbush-whitehouse.archives.gov/nsc/infosharing/index.html

Theriault, M., & Heney, W. (1998). *Oracle Security* (First Edition ed.). O'Reilly.

Tsang, R. (2009). *Cyberthreats, Vulnerabilities and Attacks on SCADA networks.*

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *Control Systems Security Program: Industrial Control Systems Cyber Emergency Response Team.* Retrieved 2011, from http://www.us-cert.gov/control_systems/ics-cert/

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *Control Systems Security Program: Industrial Control Systems Joint Working Group.* Retrieved 2011, from http://www.us-cert.gov/control_systems/icsjwg/index.html

United States Computer Emergency Readiness Team (US-CERT). (n.d.). *US-CERT: United States Compueter Emergency readiness Team*. Retrieved 2011, from http://www.us-cert.gov

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

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

VIKING Project. (2008). *Vital Infrastructure, Networks, Information and Control Systems Management*. Retrieved 2011, from http://www.vikingproject.eu

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

Web application Security Consortium. (2009). *Web Application Firewall Evaluation Criteria*. Retrieved 2011, from http://projects.webappsec.org/w/page/13246985/Web Application Firewall Evaluation Criteria

Weiss, J. (2010). *Protecting Industrial Control Systems from Electronic Threats.* Momentum Press.

West, A. (n.d.). *SCADA Communication protocols.* Retrieved 2011, from http://www.powertrans.com.au/articles/new pdfs/SCADA PROTOCOLS.pdf

ZigBee. (n.d.). *ZigBee Home Automation Overview*. Retrieved 2011, from http://www.zigbee.org/Standards/ZigBeeHomeAutomation/Overview.aspx

Zwan, E. v. (2010). Security of Industrial Control Systems, What to Look For. *ISACA Journal Online*.

3. Abbreviations

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

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

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

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

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

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu