



Protecting Industrial Control Systems

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

[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

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2011

Contents

1	ICS Security Related Standards, Guidelines and Policy Documents	1
1.1	International	2
1.2	Multilateral initiatives.....	25
1.3	United Kingdom	29
1.4	The Netherlands	34
1.5	France	36
1.6	Germany	37
1.7	Norway.....	44
1.8	Sweden	52
1.9	USA.....	54
2	References	80
3	Abbreviations.....	91

1 ICS Security Related Standards, Guidelines and Policy Documents

All the information presented here has been based on the previous work done in the ESCoRTS project, and specifically on “D2.1 - Survey of Existing Methods, Procedures and Guidelines” (ESCoRTS Project, 2009). This document provides “an overview of existing methods, procedures and guidelines in the area of control system (cyber) security. It takes into account activities of international organizations, important national activities in Europe and the US (as far as the consortium was aware of these activities), as well as the most important branch specific activities (international and national)” (ESCoRTS Project, 2009). The results of this document have been revised and updated to include the last changes as well as those identified new guidelines, standards and regulations that have been published since May 2009, date of publication of the ESCoRTS deliverable. Moreover, the way in which the information is organised is also different since it has been adapted to the objectives of this study. To this regard, is worth noting that all descriptions being provided for each of the documents presented are directly extracted from the document itself or from the website of the organization(s) behind them. What follows is an introduction to the different information fields that have been included into the tables where each standard/guideline/regulation is presented.

- **Name:** Name of the standard, good practice/guideline.
- **Type:** Standard, guidelines, or regulation/law.
- **Group/initiative/organisation:** Group, initiative or organisation responsible for the creation of the standard, guideline (e.g. ANSI/ISA), or regulatory document.
- **Status:** Draft, Final [revision x |version x].
- **Publication date:** Date of publication of the draft/final version of the standard, guideline or regulatory document.
- **Target audience:** Specifies which, among the stakeholder types identified in this study, can be more interested in the guideline, standard, or regulatory document. The possible stakeholder types are: ICS software and equipment manufacturers, ICS integrators, security tools and services providers, operators, and research/academia. Standardisation bodies have not been included for obvious reasons. The level of relevance of the standard, good practice/guideline to each one of these stakeholders is classified by level of relevance: 0 – no/minor relevance; 1 – some relevance; 2 – strong relevance.
- **Addressed Industry:** All, Generic (ICS in general), SCADA, automation, chemistry, electricity distribution/transportation, nuclear generation, water, railway transportation, oil and gas distribution, etc.
- **Geographic relevance:** Worldwide, European, Subgroup of European Countries, and National.

- **Related documents:** Other identified standards, guidelines, or regulatory documents, not necessarily related to cyber security, which have a strong relationship with the document being described.
- **Description:** short description on the content of the standard, guideline, or regulatory document.

1.1 International

Name	IEC 62351. Data and communications security.	
Type	Standard	
Group/initiative/organisation	IEC TC57 WG15	
Status	Final (revision 1)	
Publication date	May 2007	
Target audience	ICS software and equipment manufacturers:	2
	ICS integrators:	1
	Security tools and services providers:	1
	Operators:	1
	Research and Academia:	0
Addressed industry	Energy	
Geographic relevance	Worldwide	
Related standards	IEC 60870-5 (IEC 101, IEC 104, DNP3), IEC 60870-6 (TASSE.2/ICCP), IEC 61850, IEC 61970, and the IEC 61968	
Description	<p>The scope of the IEC 62351 series is information security for power system control operations. The primary objective is to “Undertake the development of standards for security of the communication protocols defined by IEC TC 57, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. Undertake the development of standards and/or technical reports on end-to-end security issues.</p> <p>IEC 62351-1 provides an introduction to the remaining parts of the standard, primarily to introduce the reader to various aspects of information security as applied to power system</p>	

	<p>operations.</p> <p>IEC 62351-2 includes the definition of terms and acronyms used in the IEC 62351 standards.</p> <p>IEC 62351-3 to IEC 62351-6 specify security standards for the IEC TC 57 communication protocols. These can be used to provide various levels of protocol security, depending upon the protocol and the parameters selected for a specific implementation. They have also been designed for backward compatibility and phased implementations.</p> <p>IEC 62351-7 addresses one area among many possible areas of end-to-end information security, namely the enhancement of overall management of the communications networks supporting power system operations.</p> <p>Other parts are expected to follow to address more areas of information security.</p> <p>For more information see (ESCoRTS Project, 2009).</p>
--	--

Name	IEC 62210. Power system control and associated communications - Data and communication security	
Type	Standard	
Group/initiative/organisation	IEC TC57	
Status	Final (obsolete since 2009). It is a precursor of the IEC 62351 series of standards and will not be maintained (ESCoRTS Project, 2009).	
Publication date	May 2003	
Target audience	ICS software and equipment manufacturers:	2
	ICS integrators:	0
	Security tools and services providers:	1
	Operators:	0
	Research and Academia:	0
Addressed Industry	Electrical distribution/transportation	
Geographic relevance	Worldwide	
Related standards	IEC 62351	
Description	This standard applies to computerised supervision, control, metering, and protection systems in electrical utilities. It deals with security aspects related to communication protocols used within and between such systems, the access to, and use of the systems. This standard discusses realistic threats to the system and its operation, the vulnerability and the consequences of intrusion, actions and countermeasures to improve the current situation.	

Name	IEC 62443. Security for Industrial Process Measurement and Control: Network and System Security.	
Type	Standard	

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Group/initiative/organisation	IEC TC 65 WG 10										
Status	Draft (parts of the standard have been published in version 1.0)										
Publication date	<p>The publication date depends on the standard:</p> <ul style="list-style-type: none"> • IEC/TS 62443-1-1:2009 • IEC 62443-2-1:2010 • IEC/TR 62443-3-1:2009 • IEC/PAS 62443-3-1:2008 										
Target audience	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">ICS software and equipment manufacturers:</td> <td style="text-align: right; padding: 2px;">2</td> </tr> <tr> <td style="padding: 2px;">ICS integrators:</td> <td style="text-align: right; padding: 2px;">1</td> </tr> <tr> <td style="padding: 2px;">Security tools and services providers:</td> <td style="text-align: right; padding: 2px;">1</td> </tr> <tr> <td style="padding: 2px;">Operators:</td> <td style="text-align: right; padding: 2px;">2</td> </tr> <tr> <td style="padding: 2px;">Research and Academia:</td> <td style="text-align: right; padding: 2px;">1</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	2										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	ISA99. There is an agreement between ISA and IEC by which ANSI/ISA99 standards will form the base documents for the IEC 62443 series.										
Description	<p>IEC 62443 is a series of standards currently under development. Several parts have been already published:</p> <p>IEC/TS 62443-1-1:2009 is a Technical Specification which defines the terminology, concepts and models for Industrial Automation and Control Systems (IACS) security. It establishes the basis for the remaining standards in the IEC 62443 series.</p> <p>IEC 62443-2-1:2010 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on</p>										

how to develop those elements. The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

IEC/TR 62443-3-1:2009 Is a Technical Report that provides a current assessment of various cyber security tools, mitigation counter-measures, and technologies that may effectively apply to the modern electronically based IACSs regulating and monitoring numerous industries and critical infrastructures. It describes several categories of control system-centric cyber security technologies, the types of products available in those categories, the pros and cons of using those products in the automated IACS environments, relative to the expected threats and known cyber vulnerabilities, and, most important, the preliminary recommendations and guidance for using these cyber security technology products and/or countermeasures.

IEC/PAS 62443-3-1:2008 is a Publicly Available Specification that establishes a framework for securing information and communication technology aspects of industrial process measurement and control systems including its networks and devices on those networks, during the operational phase of the plant's life cycle. It provides guidance on a plant's operational security requirements and is primarily intended for automation system owners/operators (responsible for ICS operation).

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	ISO 27000										
Type	Standard										
Group/initiative/organisation	ISO/IEC JTC1/SC27 (Joint Technical Committee 1/Sub Committee 27)										
Status	Final										
Publication date	<p>The publication date depends on the standard:</p> <ul style="list-style-type: none"> • ISO/IEC 27000:2009 • ISO/IEC 27001:2005 • ISO/IEC 27002:2005 • ISO/IEC 27003:2010 • ISO/IEC 27004:2009 • ISO/IEC 27005:2011 • ISO/IEC 27006:2007 • ISO/IEC 27011:2008 • ISO/IEC 27031:2011 										
Target audience	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">ICS software and equipment manufacturers:</td> <td style="text-align: right;">1</td> </tr> <tr> <td>ICS integrators:</td> <td style="text-align: right;">1</td> </tr> <tr> <td>Security tools and services providers:</td> <td style="text-align: right;">1</td> </tr> <tr> <td>Operators:</td> <td style="text-align: right;">2</td> </tr> <tr> <td>Research and Academia:</td> <td style="text-align: right;">0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	All										
Geographic relevance	Worldwide										
Related standards	N/A										
Description	The ISO/IEC 27000-series (also known as the 'ISMS Family of Standards' or 'ISO27k' for short) comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).										

The series provides good practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope, covering more than just privacy, confidentiality and IT or technical security issues. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.

At present, eleven of the standards in the series are published and available, while several more are still under development. The most relevant ones are briefly described below (for a more detailed explanation please refer to (ESCoRTS Project, 2009)):

ISO/IEC 27000:2009: Overview and vocabulary. This standard provides an overview of information security management systems, which form the subject of the information security management system (ISMS) family of standards, and defines related terms. As a result of implementing ISO/IEC 27000:2009, all types of organization (e.g. commercial enterprises, government agencies and non-profit organizations) are expected to obtain:

1. An overview of the ISMS family of standards;
2. An introduction to information security management systems (ISMS);
3. A brief description of the Plan-Do-Check-Act (PDCA) process; and
4. An understanding of terms and definitions in use throughout the ISMS family of standards.

The objectives of ISO/IEC 27000:2009 are to provide terms and

definitions, and an introduction to the ISMS family of standards that:

1. Define requirements for an ISMS and for those certifying such systems;
2. Provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;
3. Address sector-specific guidelines for ISMS; and
4. Address conformity assessment for ISMS.

ISO/IEC 27001:2005: ISMS Requirements. This standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following:

- use within organizations to formulate security requirements and objectives;
- use within organizations as a way to ensure that security risks are cost effectively managed;
- use within organizations to ensure compliance with laws and regulations;
- use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- definition of new information security management processes;
- identification and clarification of existing information security management processes;

- use by the management of organizations to determine the status of information security management activities;
- use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization;
- use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- implementation of business-enabling information security;
- use by organizations to provide relevant information about information security to customers.

This standard was published in October 2005, essentially replacing the old BS7799-2 standard. BS7799 itself was a long standing standard, first published in the nineties as a code of practice. As this matured, a second part emerged to cover management systems. It is this against which certification is granted.

ISO/IEC 27002:2005: Code of practice for information security management. This standard comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007. Its technical content is identical to that of ISO/IEC 17799:2005. ISO/IEC 17799:2005/Cor.1:2007 changes the reference number of the standard from 17799 to 27002.

ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains good practices of control objectives and controls in the following areas of information security management:

- security policy;
- organization of information security;
- asset management;
- human resources security;
- physical and environmental security;

- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management;
- compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

ISO/IEC 27003:2010: ISMS Implementation guidance. This standard focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.

ISO/IEC 27004:2009: Measurement. This standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

ISO/IEC 27004:2009 is applicable to all types and sizes of organization.

ISO/IEC 27005:2011: Information security risk management. This standard provides guidelines for information security risk management.

It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011.

ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

ISO/IEC 27006:2007: Requirements for bodies providing audit and certification of information security management systems. This standard specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by anybody providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for anybody providing ISMS certification.

ISO/IEC 27011:2008: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security management in telecommunications organizations.

The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

ISO/IEC 27031:2011: Guidelines for information and

communication technology readiness for business continuity.

This standard describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. It applies to any organization (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner.

The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.

Name	ISO/IEC 15408, Evaluation criteria for IT security (also known as “Common Criteria”)
Type	Standard
Group/initiative/organisation	JTC 1 Information technology/SC 27 Security techniques
Status	Final
Publication date	The publication date depends on the standard part: <ul style="list-style-type: none"> • ISO/IEC 15408-1:2009 • ISO/IEC 15408-2:2008 • ISO/IEC 15408-3:2008
Target audience	ICS software and equipment manufacturers: 2 ICS integrators: 1 Security tools and services providers: 2 Operators: 1 Research and Academia: 1
Addressed industry	All
Geographic relevance	Worldwide
Related standards	N/A
Description	The 'Common Criteria (CC)' is a multi-part standard. Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements, vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and

standard manner.

ISO/IEC 15408-1:2009: Part 1: Introduction and general model, establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model.

General information about the evaluation methodology is given in

ISO/IEC 18045 and the scope of evaluation schemes is provided.

ISO/IEC 15408-2:2008: Part 2: Security functional components, defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes.

ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

ISO/IEC 15408-3:2008: Part 3: Security assurance components, defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.

ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	IEEE 1686-2007. Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
Type	Standard
Group/initiative/organisation	IEEE
Status	Final
Publication date	December, 2007
Target audience	ICS software and equipment manufacturers: 2 ICS integrators: 0 Security tools and services providers: 1 Operators: 1 Research and Academia: 0
Addressed Industry	Electricity distribution/transportation
Geographic relevance	Worldwide
Related standards	NERC CIP 002 - 009
Description	<p>The standard defines the functions and features to be provided in substation IEDs to accommodate CIP programs. Specifically, the standard states which safeguards, audit mechanisms, and alarm indications shall be provided by the vendor of the IED with regard to all activities associated with access, operation, configuration, firmware revision, and data retrieval from an IED. The standard also allows the user to define a security program around these features, and alert the user if an IED does not meet this standard as to the need for other defensive measures (technical and/or procedural) that may need to be taken. The encryption</p>

for the secure transmission of data both within and external to the substation is not part of this standard as this is addressed in other efforts.

This standard can be applied to any substation IED. Although the standard is designed to provide the tools and features for a user to implement an IED security effort in response to NERC CIP requirements, the standard is applicable to any IED where the user requires security, accountability, and auditability in the configuration and maintenance of the IED.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	IEEE 1402. Guide for Electric Power Substation Physical and Electronic Security										
Type	Standard / Guideline										
Group/initiative/organisation	IEEE E7.1402										
Status	Final										
Publication date	April, 2000										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Energy Substation Automation										
Geographic relevance	Worldwide										
Related standards	N/A										
Description	In this standard, security issues related to human intrusion upon electric power supply substations are identified and discussed. Various methods and techniques presently being used to mitigate human intrusions are also presented in this guide.										

Name	IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links										
Type	Standard										
Group/initiative/organisation	IEEE WGC6										
Status	Final										
Publication date	February, 2011										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>0</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>1</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	1	Security tools and services providers:	0	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	2										
ICS integrators:	1										
Security tools and services providers:	0										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Substation automation										
Geographic relevance	Worldwide										
Related standards	<p>AGA 12, part 1: IEEE 1711 incorporates the American Gas Association cryptographic protocol (SCADAsecure), written to implement requirements in IEEE 1689 and improvements in this protocol suggested by Sandia National Laboratories, as well as lessons learned from utility field testing.</p> <p>Note: The draft effort IEEE P1689 was an introductory standard accompanying IEEE 1711. However, IEEE P1689 was withdrawn and its requirements integrated into IEEE 1711 (Holstein D. K., 2008).</p>										
Description	A cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of serial links is defined in this trial use standard. Specific applications or hardware implementations are not addressed, and the standard is										

	<p>independent of the underlying communications protocol.</p> <p>IEEE 1711 defines a specific serial security protocol for two types of cryptographic modules: SCADA Cryptographic Modules (SCM's) to protect the serial SCADA channel, and Maintenance Cryptographic Modules (MCM's) to protect the maintenance channel, which is typically a dial-up connection.</p>
--	--

Name	ISA 99. Manufacturing and Control System Security.	
Type	Standards and guidelines (good practices and technical reports)	
Group/initiative/organisation	ANSI/ISA-99	
Status	Only ANSI/ISA-99.01.01-2007, ANSI/ISA-TR99.01.02-2007, and ANSI/ISA-99.02.01-2009 are published. All other parts are in draft at different maturity stages.	
Publication date	ANSI/ISA-99.01.01-2007: October, 2007. ANSI/ISA-TR99.01.02-2007: October, 2007. ANSI/ISA-99.02.01-2009: January, 2009.	
Target audience	ICS software and equipment manufacturers:	2
	ICS integrators:	2
	Security tools and services providers:	2
	Operators:	2
	Research and Academia:	2
Addressed Industry	Generic	
Geographic relevance	Worldwide	
Related standards	N/A	
Description	<p>The ISA99 series addresses electronic security within the industrial automation and control systems environment. The series will serve as the foundation for the IEC 62443 series of the same titles, as being developed by IEC TC65 WG10, "Security for industrial process measurement and control - Network and system security."</p> <p>The ISA99 series includes the following:</p> <p>ANSI/ISA-99.01.01-2007 (previously named ANSI/ISA-99.00.01-2007), Security for Industrial Automation and Control Systems:</p>	

Concepts, Terminology and Models. This standard establishes the context for all of the remaining standards in the series by defining the terminology, concepts and models to understand electronic security for the industrial automation and control systems environment.

ANSI/ISA-TR99.01.02-2007 (previously named ANSI/ISA-TR99.00.01-2007), Security Technologies for Manufacturing and Control Systems. This Technical Report (TR) describes various security technologies in terms of their applicability for use with industrial automation and control systems. This report will be updated periodically to reflect changes in technology.

ANSI/ISA-99.02.01-2009, Establishing an Industrial Automation and Control Systems Security Program. This standard describes the elements to establish a cyber security management system and provides guidance on how to meet the requirements for each element.

ANSI/ISA-99.02.02 (in development), Operating an industrial automation and control system security program. This standard will address how to operate a security program after it is designed and implemented. This includes the definition and application of metrics to measure program effectiveness.

ANSI/ISA-99.03.xx (in development), Technical security requirements for industrial automation and control systems (in development). These standards will define the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a security point of view. Based on these characteristics, the standards will establish the security requirements that are unique to this class of

systems.

For further information refer to (ESCoRTS Project, 2009).

1.2 Multilateral initiatives

Name	Cyber Security Assessments of Industrial Control Systems. A good practice guide.										
Type	Guideline (Good practice)										
Group/initiative/organisation	CPNI (UK) and DHS (USA)										
Status	Final (revision 1)										
Publication date	April, 2011										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>0</td> </tr> <tr> <td>ICS integrators:</td> <td>0</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>1.2.1 2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	0	ICS integrators:	0	Security tools and services providers:	1	Operators:	1.2.1 2	Research and Academia:	0
ICS software and equipment manufacturers:	0										
ICS integrators:	0										
Security tools and services providers:	1										
Operators:	1.2.1 2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	<ul style="list-style-type: none"> • Good practice guide - Process Control and SCADA Security. • Firewall deployment for SCADA and process control networks. A good practice guide. • Configuring & managing remote access for industrial control systems. A good practice guide. 										
Description	<p>This guide has been prepared to assist asset owners in procuring and executing cyber security tests of their Industrial Control, Supervisory Control and Data Acquisition (SCADA), Distributed Control (DCS) and/or process control (PCS) systems, hereafter generically referred to as an industrial control system (ICS). The guide's purpose is to educate asset owners on the general process of a cyber security test and provide insight on specific testing methods so owners learn to prescribe a custom</p>										

assessment that will maximise the output of their testing budget.

This guide also doubles as a checklist for internal teams performing cyber security assessments to ensure their plans cover the high-risk areas of an ICS. It lists some possible testing methods and describes pros and cons for each method based on the cyber security ICS testing experience of Idaho National Laboratory (INL). Asset owners are able to apply this information in the decision-making process for planning an ICS assessment.

This guide does not describe how to execute specific cyber security tests; rather, it focuses on what should be covered in an ICS cyber security assessment.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	Configuring & managing remote access for industrial control systems. A good practice guide.										
Type	Guideline (Good practice)										
Group/initiative/organisation	CPNI (UK) and DHS (USA)										
Status	Final (revision 1)										
Publication date	May, 2011										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>0</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>2</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	0	ICS integrators:	1	Security tools and services providers:	2	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	0										
ICS integrators:	1										
Security tools and services providers:	2										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	<ul style="list-style-type: none"> • Good practice guide - Process Control and SCADA Security. • Firewall deployment for SCADA and process control networks. A good practice guide. • Cyber Security Assessments of Industrial Control Systems. A good practice guide. 										
Description	<p>This document provides guidance for developing secure remote access strategies for organisations that use industrial control systems. This document is for use in developing or updating strategies related to managing remote connectivity between operational assets, peers, vendors, operators and other elements that require access to critical information, devices or process data.</p> <p>Although this document is titled Configuring and Managing</p>										

	<p>Remote Access for Control Systems, the material is intended to be applicable to any architecture involving industrial control systems, process control systems, Supervisory Control and Data Acquisition (SCADA), or distributed control systems. The term industrial control systems is to be considered a general term applying to all these system types sharing similar characteristics and is in line with the definitions used by the contemporary communities of interest and other standards bodies.</p>
--	---

1.3 United Kingdom

Name	Good practice guide - Process Control and SCADA Security.										
Type	Guideline (Good practices)										
Group/initiative/organisation	CPNI										
Status	Final (revision 2)										
Publication date	June, 2008										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>2</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	2	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	2										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	<ul style="list-style-type: none"> • Cyber Security Assessments of Industrial Control Systems. A good practice guide. • Firewall deployment for SCADA and process control networks. A good practice guide. • Configuring & managing remote access for industrial control systems. A good practice guide. 										
Description	<p>This set of guidelines is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. It proposes a framework consisting of seven elements for addressing process control security.</p> <p>Process control and SCADA security, General Guidance. The aim of this document is to provide good practice principles for</p>										

process control and SCADA security. Specifically this document:

- Provides an overview of the necessity for process control and SCADA system security
- Highlights the differences between process control and SCADA system security and IT security.
- Describes the key principles used to develop the whole framework.
- Identifies seven elements for addressing process control system security and for each.
- Presents good practice principles.

Process control and SCADA security guide 1, Understand the Business Risk. This guide provides guidance on assessing the business risk and ongoing assessment of this risk. It does not provide detailed risk assessment techniques or methodologies.

Process control and SCADA security guide 2, Implement Secure Architecture. This guide provides good practice guidance on deciding on appropriate security architecture for process control systems. It does not provide detailed technical solutions, architectures or standards.

Process control and SCADA security guide 3, Establish Response Capabilities. This guide provides guidance on establishing response capabilities relating to digital security threats in process control and SCADA systems. It does not provide detailed response plans or procedures as these will vary from organisation to organisation and system to system.

Process control and SCADA security guide 4, Improve Awareness and Skills. This document develops the element by

looking in detail at each of the key areas and provides generic guidance on improving process control security skills within organisations. This guide does not provide detailed process control security awareness or training course requirements.

Process control and SCADA security guide 5, Manage Third Party Risk. This document provides good practice guidance managing third party risks to process control system security. This guide does not provide detailed policies or methodologies.

Process control and SCADA security guide 6, Engage Projects. This guide provides good practice guidance on building security considerations into process control security projects. This document does not provide detailed process control security requirements as these will vary from system to system.

Process control and SCADA security guide 7 - Establish Ongoing Governance. This guide provides good practice guidance for defining and implementing appropriate governance frameworks for process control systems security. This document will not provide detailed policies and standards or procedures.

Name	Firewall deployment for SCADA and process control networks. A good practice guide.										
Type	Guideline (Good practice)										
Group/initiative/organisation	CPNI. However, it was previously published by the National Infrastructure Security Co-ordination Centre (NISCC), a predecessor organisation to the CPNI.										
Status	Final (revision 2)										
Publication date	June, 2008										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>0</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	0	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	0										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed industry	Generic										
Geographic relevance	UK										
Related standards	<p>Good practice guide - Process Control And SCADA Security.</p> <p>Cyber Security Assessments of Industrial Control Systems. A good practice guide.</p>										
Description	<p>This document is result of the investigation and compilation of the current practices in SCADA/PCN firewall deployment. The intent was to examine the “state of the art” in firewall architectures, deployment and management used to protect industrial control environments.</p> <p>In March 2004, the research team sent out requests for information regarding the use of firewalls in industrial settings to approximately 60 organizations and industry news lists. A</p>										

total of 10 vendors, including firewall manufacturers, IT security firms and control systems manufacturers, responded in some form. Approximately 15 industrial users from the petroleum, chemical, food, and electrical sectors also responded. The vendor and end-user organizations were a mix of North American and European-based firms. This information provided was in the form of personal interviews, white papers, policy manuals, network audit reports and security product literature. In addition, draft documents from standards organizations involved in industrial control security were obtained. These included documents from the American Petroleum Institute (API), the Industrial Automation Open Networking Association (IAONA), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE) and the Instrumentation, Systems and Automation Society (ISA).

All collected information was summarized by the research team in terms of firewall architecture, design, deployment and management to determine current security practises. These practices were then analysed and scored for their likely effectiveness in the industrial control environment. The results of this analysis indicated that there were a significant number of different solutions used by the industry and the security effectiveness of these can vary widely.

1.4 The Netherlands

Name	Process Control Domain (PCD) – Security Requirements for Vendors										
Type	Regulation (Industrial Mandate)										
Group/initiative/organisation	WIB, EI and EXERA (EWE)										
Status	Final (revision 2)										
Publication date	October 2010										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	2										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	France, UK, The Netherlands										
Related standards	N/A										
Description	<p>This document specifies requirements and gives recommendations for IT security to be fulfilled by vendors of process control & automation systems to be used in Process Control Domains (PCDs).</p> <p>This covers both policy; addressing the Vendor’s organization, IT security processes technological solutions and governance of IT security. When a Vendor’s solution complies with this set of requirements, the solution is considered by the WIB to be PCD Security Compatible.</p> <p>An “End User” or “the Principal” shall comply with its own security policies, standards and specifications for the PCD and</p>										

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

	<p>this can vary for each Principal. These requirements documents a subset of a Principal's security policies, standards and specifications for the PCD, containing the common requirements of all Principals into one set of minimum requirements for Vendors to comply with.</p>
--	--

1.5 France

Name	Managing Information Security in an Electric Utility										
Type	Guideline (Technical report)										
Group/initiative/organisation	CIGRE, JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems										
Status	Final										
Publication date	September, 2005										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>0</td> </tr> <tr> <td>ICS integrators:</td> <td>0</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	0	ICS integrators:	0	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	0										
ICS integrators:	0										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Electricity distribution/transportation										
Geographic relevance	France										
Related standards	N/A										
Description	<p>The purpose of this paper is to give an overview of the information security problem for an electric utility and to raise the awareness of the need to implement security to mitigate attacks on information systems and intranets. Hence, the paper is addressing the question of “Why is Information Security important for the electric power industry?” Also, guidance for how to solve the problem is discussed; it is proposed that security is treated from a domain point of view, instead of a traditional hardware perspective. Conceptually, this approach of using domains and sub domains has been a useful mechanism to study the attacks on information systems and intranets.</p>										

1.6 Germany

Name	NAMUR NA 115. IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries										
Type	Guideline (worksheet)										
Group/initiative/organisation	NAMUR WA2/AK2.8 (Working Area 2. Automation Systems for Processes and Plants/Working Group 8. Internet/Intranet)										
Status	Final										
Publication date	June, 2006										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>2</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	2	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	2										
ICS integrators:	2										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Automation										
Geographic relevance	Germany/Europe										
Related standards	N/A										
Description	<p>The purpose of this NAMUR worksheet is to illustrate the boundary conditions applicable to IT security products in automation engineering from the point of view of the user.</p> <p>The NAMUR worksheet addresses:</p> <ul style="list-style-type: none"> Manufacturers and system integrators. This worksheet provides them with information on specific boundary conditions in the process industry that govern the implementation of measures and/or design of new systems. Users, who should consider appropriate criteria when making purchasing decisions. <p>This NAMUR worksheet addresses both aspects (i.e. in addition to</p>										

	<p>measures that are indispensable for current systems, it also examines the development of future industrial automation systems from the point of view of IT security).</p>
--	--

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	VDI/VDE 2182 Series	
Type	Guideline (good practices)	
Group/initiative/organisation	VDI (The Association of German Engineers)	
Status	Depends on the part of the series: <ul style="list-style-type: none"> • VDI/VDE 2182 Part 1: Final • VDI/VDE 2182 Part 2.1: Draft • VDI/VDE 2182 Part 2.2: Draft • VDI/VDE 2182 Part 3.1: Draft • VDI/VDE 2182 Part 3.2: Draft • VDI/VDE 2182 Part 3.3: Draft 	
Publication date	Depends on the part of the series: <ul style="list-style-type: none"> • VDI/VDE 2182 Part 1: January 2011 • VDI/VDE 2182 Part 2.1: January 2011 • VDI/VDE 2182 Part 2.2: February 2011 • VDI/VDE 2182 Part 3.1: April 2011 • VDI/VDE 2182 Part 3.2: January 2011 • VDI/VDE 2182 Part 3.3: January 2011 	
Target audience	ICS software and equipment manufacturers:	2
	ICS integrators:	2
	Security tools and services providers:	1
	Operators:	2
	Research and Academia:	0
Addressed Industry	Industrial Automation	
Geographic relevance	Germany	
Related standards	N/A	
Description	VDI/VDE 2182 Part 1: IT-security for industrial automation -	

General model. This guideline describes how specific measures can be implemented in order to guarantee the IT security of automated machines and plant; aspects of the automation devices, automation systems, and automation applications used are considered. A uniform, feasible procedure for ensuring IT security throughout the entire life cycle of automation devices, systems, and applications is described, based on common terms and definitions agreed by the manufacturers of automation devices and systems and their users (e.g., machine manufacturers, integrators, and operators). The life cycle covers the development, integration, operation, migration, and decommissioning phases. This guideline defines a simple procedure model for the development and description of IT Security. The model consists of eight steps.

VDI/VDE 2182 Part 2.1: IT-security for industrial automation - Example of use of the general model for manufacturer in factory automation - Programmable Logic Controller (PLC). The guideline draft supplements the guideline VDI/VDE 2182 Part 1. Exemplarily the guideline shows the application of the general model introduced in VDI/VDE 2182 Part 1 for the realization of IT security for devices, machines and plants by clearly-defined measures. For this purpose the guideline shows the application from the view of a manufacturer. The guideline thereby substantiates the relevance and practicability of the general models given in VDI/VDE 2182 Part 1.

VDI/VDE 2182 Part 2.2: IT security for industrial automation - Example of use of the general model in factory automation for

machine manufacturers and plant manufacturers - Forming press. The guideline supplements the guideline VDI/VDE 2182 Part 1. Exemplarily the guideline shows the application of the general model introduced in VDI/VDE 2182 Part 1 for the realization of IT security for devices, machines and plants by clearly-defined measures. For this purpose the guideline shows the application from the view of a manufacturer. The guideline thereby substantiates the relevance and practicability of the general models given in VDI/VDE 2182 Part 1.

VDI/VDE 2182 Part 3.1: IT security for industrial automation - Example of use of the general model for manufacturers in factory automation - Process control system of a LDPE plant. The guideline supplements the guideline VDI/VDE 2182 Part 1. Exemplarily the guideline shows the application of the general model introduced in VDI/VDE 2182 Part 1 for the realization of IT security. For this purpose the guideline shows the application from the view of a manufacturer of automation systems. The guideline thereby substantiates the relevance and practicability of the general models given in VDI/VDE 2182 Part 1.

VDI/VDE 2182 Part 3.2: IT security for industrial automation - Example of use of the general model for integrators in process industry - LDPE reactor. The guideline draft supplements the guideline VDI/VDE 2182 Part 1. Exemplarily the guideline shows the application of the general model introduced in VDI/VDE 2182 Part 1 for the realization of IT security for devices, machines and plants by clearly-defined measures. For this purpose the guideline shows the application from the view of an integrator of automatic

control engineering in plants for continuous and intermittent procedure or energetic processes. The guideline substantiates the relevance and practicability of the general models by example of a Low Density Polyethyl(LPDE-)reactor. Preparing measures, the application of the individual points of the procedure model, the requirements of the operator to the integrator and the integrator to the equipment manufacturers and the necessary documentations are described and represented in detail.

VDI/VDE 2182 Part 3.3: IT security for industrial automation - Example of use of the general model for integrators in process industry - LDPE plant. The guideline draft supplements the guideline VDI/VDE 2182 Part 1. Exemplarily the guideline shows the application of the general model introduced in VDI/VDE 2182 Part 1 for the realization of IT security for devices, machines and plants by clearly-defined measures. For this purpose the guideline shows the application from the view of a plant operator. The guideline substantiates the relevance and practicability of the general models by example of a Low Density Polyethyl(LPDE-)reactor. Preparing measures, the application of the individual points of the procedure model, the requirements of the operator to the integrator and the integrator to the equipment manufacturers and the necessary documentations are described and represented in detail.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	VGB R175. IT security for generating plants
Type	Guideline (good practices)
Group/initiative/organisation	VGB Group
Status	Final
Publication date	May 2006
Target audience	<p>ICS software and equipment manufacturers: 1</p> <p>ICS integrators: 2</p> <p>Security tools and services providers: 1</p> <p>Operators: 2</p> <p>Research and Academia: 1</p>
Addressed Industry	Power generation
Geographic relevance	Germany
Related standards	N/A
Description	<p>This guideline aims to provide the operators of power plants with hints and recommendations on how to improve their IT security. In this context, the guideline focuses on the functionality of the instrumentation and control (I&C) system that is necessary to control the power plants which should not be affected by threats to the IT systems.</p> <p>The guideline also provides hints on the organisation and management of the IT administration and IT systems themselves. Manufacturers and suppliers of both I&C systems and IT infrastructure will be requested to implement the guideline, to offer solutions for the specific requirements in the power plants and to realise these together with the operators.</p>

1.7 Norway

Name	OLF Guideline No. 104. Information security baseline requirements for process control, safety and support ICT systems	
Type	Guideline (good practice)	
Group/initiative/organisation	Norwegian Oil Industry Association (OLF)	
Status	Final (Revision 5)	
Publication date	January 2009	
Target audience	ICS software and equipment manufacturers:	1
	ICS integrators:	2
	Security tools and services providers:	1
	Operators:	2
	Research and Academia:	0
Addressed Industry	Oil industry	
Geographic relevance	Norway	
Related standards	OLF Guideline No. 110 ISO/IEC 27001	
Description	<p>This document contains the OLF Information Security Baseline Requirements (ISBR) for ICT systems in process control, safety and support networks. The guideline consists of 16 requirements to operators and suppliers within the oil and gas industry on the NCS. The controls documented are considered “good practice” for information security, and all of the measures shall be implemented, unless particular business circumstances render some of the controls inapplicable. The controls deemed not to be applicable must be justified and documented.</p> <p>The OLF Information Security Baseline Requirements are</p>	

	<p>additional to the company's own information security policy and regulations, as well as subject to national legislation.</p> <p>The controls are founded on ISO/IEC 27001:2005 (former BS 7799-2), adapted to the oil and gas sector. This ISBR list is not pre-emptive or exhaustive – each organisation has to implement additional controls and security measures to obtain the level of information security which is necessary for their business. Implementing all the controls in this ISBR will not guarantee that security incidents cannot occur.</p>
--	--

Name	OLF Guideline No. 110. Implementation of information security in Process Control, Safety and Support ICT Systems during the engineering, procurement and commissioning phases	
Type	Guideline (good practice)	
Group/initiative/organisation	Norwegian Oil Industry Association (OLF)	
Status	Final (Revision 2)	
Publication date	January 2009	
Target audience	ICS software and equipment manufacturers:	2
	ICS integrators:	2
	Security tools and services providers:	2
	Operators:	2
	Research and Academia:	1
Addressed Industry	Oil industry	
Geographic relevance	Norway	
Related standards	OLF Guideline No. 104	
Description	<p>The “Information Security Baseline Requirements for Process Control, Safety and support ICT Systems” (ISBR) guideline was issued in June 2006. The guideline consists of 16 requirements to operators and suppliers within the oil and gas industry on the NCS. ISBR’s requirement #8 demands that information security of ICT components shall be integrated in the engineering, procurement, and commissioning processes. This document focuses on the activities which need to be performed during the different phases of engineering, procurement and commissioning, with respect to the different ISBR requirements in the OLF Guideline no. 104.</p> <p>The document lists the typical phases that are included in the engineering, procurement, and commissioning processes. The</p>	

	<p>name of the phases may vary from company to company, and the activities may be shifted in time during a project depending on the companies' methodologies. The companies may have different approaches to the implementation of information security depending on the risk picture and the scope of the project. This document will not specify in detail how the baseline requirements shall be fulfilled, but rather take an overview of the topics which need to be considered by the project organisation as well as the operating organisation.</p>
--	---

Name	CheckIT										
Type	Guideline										
Group/initiative/organisation	Developed by NSM (National Authority for Information security), NTNU (The Norwegian University for Science and Technology) and SINTEF, with active participation from Telenor, Statoil, Norsk Hydro.										
Status	Final										
Publication date	2006										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>0</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	0	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	0										
Operators:	2										
Research and Academia:	0										
Addressed industry	All										
Geographic relevance	Norway										
Related standards	N/A										
Description	<p>People, as individuals as well as a group, have a great impact on information and information security. Values, attitudes and the organisational culture form the basis upon which one deals with sensitive information. This checklist/tool aims to give an overview of values, attitudes and organisational culture related to information security.</p> <p>The CheckIT tool was developed to help organizations improve their safety and security cultures. The CheckIT questionnaire has 31 questions, each of which has three alternative answers corresponding to distinct cultural levels:</p>										

- Level 1: Denial culture
- Level 3: Rule-based culture
- Level 5: Learning/generative culture (application of best practices)

The goal is to rate an organization on a five-point numerical scale. The scale provides a normalized score for the organization, which makes it possible to compare results over time or between organizations.

Name	CRIOP										
Type	Guideline										
Group/initiative/organisation	HFC (Human Factors in Control Systems) forum										
Status	Final										
Publication date	2003 (revision 2)										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed industry	All										
Geographic relevance	Norway										
Related standards	ISO 11064										
Description	<p>CRIOP is a methodology to verify and validate the ability of a control centre to safely and effectively handle all modes of operations including start up, normal operations, maintenance and revision maintenance, process disturbances, safety critical situations and shut down.</p> <p>The methodology can be applied to central control rooms, driller's cabins, cranes and other types of cabins, onshore, offshore and emergency control rooms.</p> <p>The methodology is based on several standards and was in 1997 recommended as a preferred methodology in NORSOK S-002.</p> <p>CRIOP is short for Crisis Intervention and Operability analysis. The CRIOP method focuses on the interaction between people,</p>										

	<p>technology and organisations. One of the most important principles of the CRIOP method is to verify that a focus is kept on important human factors, in relation to operation and handling of abnormal situations in offshore control centres, and to validate solutions and results.</p>
--	--

1.8 Sweden

Name	Guide to Increased Security in Industrial Control Systems										
Type	Guideline (good practices)										
Group/initiative/organisation	MSB, the Swedish Contingencies Agency (formerly SEMA, the Swedish Emergency Management Agency)										
Status	Final										
Publication date	May 2010										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>1</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	1	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	1										
Research and Academia:	0										
Addressed Industry	SCADA systems										
Geographic relevance	Sweden/Europe										
Related standards	NERC CIP, NIST SP 800-82, DOE 21 Steps, OLF 104, CPNI GPG										
Description	<p>The purpose of this document is to provide support and increase awareness of the need for increased security in industrial control systems. The first edition of the document was published in October 2008 and was well received both nationally and internationally.</p> <p>This guide provides fundamental recommendations on security in industrial control systems. The document also provides tips on where additional information can be found. The recommendations we provide are affiliated with internationally recognised recommendations, practices and standard work methods.</p>										

	<p>The recommendations given here are supported by the members of FIDI-SC and work with the document has been significantly facilitated by the generous help received from representatives of the forum.</p>
--	--

1.9 USA

Name	NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security.										
Type	Guideline (Technical report and good practices)										
Group/initiative/organisation	National Institute of Standards and Technology (NIST)										
Status	Final										
Publication date	June 2011										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	NIST SP 800-53										
Description	The purpose of this document is to provide guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.										

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	NIST SP 800-53. Recommended Security Controls for Federal Information Systems.										
Type	Guideline (Good practices)										
Group/initiative/organisation	National Institute of Standards and Technology (NIST)										
Status	Final, revision 3										
Publication date	August 2009										
Target audience	<table border="0"> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	Worldwide										
Related standards	NIST SP 800-82. Section 6 of this document also provides initial guidance on how 800-53 security controls apply to ICS.										
Description	<p>The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government.</p> <p>ICS-specific guidance is included in Appendix I: Industrial Control Systems – Security Controls, Enhancements, and</p>										

Supplemental Guidance.

- *ICS Supplemental Guidance* provides organizations with additional information on the application of the security controls and control enhancements in Appendix F to ICS and the environments in which these specialized systems operate. The Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls).
- *ICS Enhancements (one or more)* provide enhancement augmentations to the original control that may be required for some ICS.
- *ICS Enhancement Supplemental Guidance* provides guidance on how the control enhancement applies, or does not apply, in ICS environments.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	NISTIR 7176. System Protection Profile - Industrial Control Systems										
Type	Guideline										
Group/initiative/organisation	NIST										
Status	Final (revision 1)										
Publication date	October 2004										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>1</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	2										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Generic										
Geographic relevance	USA										
Related standards	ISO/IEC 15408 (Common Criteria)										
Description	<p>This guideline is designed to present a cohesive, cross-industry, baseline set of security requirements or System Protection Profiles (SPP) for new industrial control systems. It intends to provide an ISO 15408 based starting point in formally stating security requirements associated with industrial control systems (ICS). This SPP includes security functional requirements (SFRs) and security assurance requirements (SARs) that extend ISO 15408 to cover issues associated with systems. These extensions are based on current ISO subcommittee work to extend ISO 15408 to cover the accreditation of systems and the evaluation of system protection profiles and system security targets. These extensions broaden consideration of security controls to include non-technical controls based on procedural and management functions.</p> <p>According to ISO/IEC 15408-1, the security environment, the</p>										

security objectives, and the security functional requirements for an industrial control system are presented. The evaluation assurance level is EAL 3+.

This protection profile refers to Common Criteria, version 2.1. Presently, evaluations will follow CC, version 3.1. Thus, this PP cannot be applied directly.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	Field Device Protection Profile for SCADA Systems in Medium Robustness Environments										
Type	Guideline										
Group/initiative/organisation	NIST/PCSRF										
Status	Draft (revision 0.75)										
Publication date	June 2006										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>1</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	2										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Generic										
Geographic relevance	USA										
Related standards	ISO/IEC 15408 (Common Criteria)										
Description	<p>This Protection Profile specifies the minimum security requirements for SCADA field devices used by a U.S. Government or commercial organization in medium robustness environments.</p> <p>This Protection Profile is intended for the following uses:</p> <ul style="list-style-type: none"> For vendors, this Protection Profile defines the requirements, as identified by the SCADA community, which must be addressed by SCADA field devices such as PLC's, RTU's and IED's in a vendor's Security Target. For SCADA asset owners, this Protection Profile is useful in identifying requirements that can be considered in purchasing specifications. Alternately, asset owners can require products to demonstrate compliance with this Protection Profile. 										
Name	NISTIR 7628. Guidelines for Smart Grid Cyber Security:										

	<ul style="list-style-type: none"> • Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. • Vol. 2, Privacy and the Smart Grid. • Vol.3, Supportive Analyses and References. 										
Type	Guideline (Technical report)										
Group/initiative/organisation	National Institute of Standards and Technology (NIST)										
Status	Final										
Publication date	August, 2010										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>2</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>2</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	2	Operators:	2	Research and Academia:	2
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	2										
Operators:	2										
Research and Academia:	2										
Addressed Industry	Electricity distribution										
Geographic relevance	Worldwide										
Related standards	N/A										
Description	<p>Volume 1 includes:</p> <ul style="list-style-type: none"> • Background information on the Smart Grid and the importance of cyber security in ensuring the reliability of the grid and the confidentiality of specific information. It also discusses the cyber security strategy for the Smart Grid and the specific tasks within this strategy. • A high level diagram that depicts a composite high level view of the actors within each of the Smart Grid domains and includes an overall logical reference model of the Smart Grid, including all the major domains. This architecture focuses on a short-term view (1–3 years) of the Smart Grid. • The high level security requirements for the Smart Grid for each of the 22 logical interface categories included. • Cryptographic and key management issues across the 										

scope of systems and devices found in the Smart Grid along with potential alternatives.

Volume 2 includes:

- A privacy impact assessment for the Smart Grid with a discussion of mitigating factors. It also identifies potential privacy issues that may occur as new capabilities are included in the Smart Grid.

Volume 3 includes:

- Classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.
- Identifies a number of specific security problems in the Smart Grid. Currently, these security problems do not have specific solutions.
- Research and Development themes that identify where the state of the art falls short of meeting the envisioned functional, reliability, and scalability requirements of the Smart Grid.
- An overview of the process that is being used to assess standards against the high level security requirements included in this report.
- Key power system use cases that are architecturally significant with respect to security requirements for the Smart Grid.

Name	NERC CIP 002 – 009. Reliability Standards for the Bulk Electric Systems in North America	
Type	Regulation	
Group/initiative/organisation	North American Electric Reliability Corporation (NERC)	
Status	Final. Revision 4.	
Publication date	January 2011	
Target audience	ICS software and equipment manufacturers:	1
	ICS integrators:	1
	Security tools and services providers:	1
	Operators:	2
	Research and Academia:	0
Addressed Industry	Electricity transportation/distribution	
Geographic relevance	North America	
Related standards	N/A	
Description	<p>NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.</p> <p>These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.</p> <p>Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations,</p>	

for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.

Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

Standard CIP-006-4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

Standard CIP-008-4 ensures the identification, classification,

	<p>response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.</p> <p>Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.</p>
--	--

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	AGA Report No. 12. Cryptographic Protection of SCADA Communications.										
Type	Standard										
Group/initiative/organisation	American Gas Association (AGA) 12 Cryptography Working Group										
Status	Draft (discontinued)										
Publication date	March, 2006										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>2</td> </tr> <tr> <td>ICS integrators:</td> <td>2</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	2	ICS integrators:	2	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	2										
ICS integrators:	2										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Gas, electricity, wastewater and pipeline systems										
Geographic relevance	North America										
Related standards	N/A										
Description	<p>The purpose of the AGA 12 series is to save SCADA system owners' time and effort by proposing a comprehensive system designed specifically to protect SCADA communications. While the use of cryptographic protection is not required, the purpose of the AGA 12 series is to develop practices that are intended to provide secure and easy-to-implement cryptography.</p> <p>End users may use the AGA 12 series to establish the general requirements for procuring a SCADA cyber security solution by including this specification in their procurement requirements. System integrators may use the AGA 12 series to ensure that SCADA cyber security is specified properly, and that the system test plan meets all the requirements needed to commission its security solution. Finally, manufacturers of SCADA hardware,</p>										

software, and firmware may use the AGA 12 series to ensure that their product offerings address the needs of the end user for SCADA cyber security.

The AGA 12 Task Group decided to split the AGA 12 report and number them as follows:

- AGA 12, Part 1: Cryptographic Protection of SCADA Communications: Background, Policies & Test Plan
- AGA 12, Part 2: Cryptographic Protection of SCADA Communications: Retrofit Link Encryption for Asynchronous Serial Communications
- AGA 12, Part 3: Cryptographic Protection of SCADA Communications: Protection of Networked Systems
- AGA 12, Part 4: Cryptographic Protection of SCADA Communications: Protection Embedded in SCADA Components

The lack of funding has prevented additional work on the standard from being completed. As a result, only Part 1 is available.

AGA 12, Part 1 focuses on the background needed to understand the threats to SCADA communications, it considers an approach to develop security policies for protection of SCADA communications, furthermore system level requirements, and a general plan for testing equipment. The main focus is embedding of cryptography and key management into SCADA system components.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	API 1164, Pipeline SCADA Security
Type	Guideline (Good practices)
Group/initiative/organisation	American Petroleum Institute (API)
Status	Final, revision 2
Publication date	June, 2009
Target audience	<p>ICS software and equipment manufacturers: 0</p> <p>ICS integrators: 1</p> <p>Security tools and services providers: 1</p> <p>Operators: 2</p> <p>Research and Academia: 0</p>
Addressed Industry	Oil and gas distribution, Generic.
Geographic relevance	North America
Related standards	N/A
Description	<p>This guideline is specifically designed to provide the operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual companies.</p> <p>This SCADA security program provides a means to improve the security of the pipeline SCADA operation by:</p> <ul style="list-style-type: none"> • Analyzing vulnerabilities of the SCADA system that can be exploited by unauthorized entities. • Listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks. • Providing a comprehensive list of practices to harden the core architecture. • Providing examples of industry good practices. <p>This document on SCADA security provides guidance to operators</p>

of Oil and Gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document is not limited to pipelines regulated under Title 49 CFR 195.1, but should be viewed as a listing of good practices to be employed when reviewing and developing standards for a SCADA system.

This document embodies the "API Security Guidelines for the Petroleum Industry."

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	Security Guidelines for the Petroleum Industry										
Type	Guideline (Good practices)										
Group/initiative/organisation	American Petroleum Institute (API)										
Status	Final										
Publication date	April, 2005										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>0</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	0	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	0										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Oil and gas distribution, Generic.										
Geographic relevance	North America										
Related standards	N/A										
Description	<p>The objective of this document is to provide general guidance to owners and operators of U.S. domestic petroleum assets for effectively managing security risks and provide a reference of certain applicable Federal security laws and regulations that may impact petroleum operations.</p> <p>API has developed this guidance for the petroleum industry as a reference to be used with other available sources. This document does not attempt to provide an all-inclusive list of security considerations, but more as a basis for what might be considered when evaluating and implementing security measures. Additionally, it is recognized that certain information included in a security program needs to remain confidential. Petroleum companies should consider a confidentiality program to understand what information can be shared and what should</p>										

remain confidential.

This document is embodied by API 1164, Pipeline SCADA Security Standard.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	21 Steps to improve Cyber Security for SCADA systems										
Type	Guidelines (Good practices)										
Group/initiative/organisation	President’s Critical Infrastructure Protection Board, Department of Energy (DoE)										
Status	Final										
Publication date	2002										
Target audience	<table border="0"> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Generic										
Geographic relevance	USA										
Related standards	N/A										
Description	<p>The Guideline provides short descriptions of 21 essential steps for improving SCADA security. These steps are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.</p>										

Name	Catalogue of Control Systems Security: Recommendations for Standards Developers.										
Type	Guideline (technical report)										
Group/initiative/organisation	DHS. Control Systems Security Program. National Cyber Security Division.										
Status	Final										
Publication date	September 2009										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>1</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Generic										
Geographic relevance	USA										
Related standards	NIST SP 800-53, ISA99										
Description	<p>This catalogue presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalogue are grouped into 19 families, or categories, that have similar emphasis. The recommendations within each family are displayed with a summary statement of the recommendation, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the recommendation under special situations.</p> <p>This catalogue is not limited for use by a specific industry sector but can be used by all sectors to develop a framework needed to produce a sound cyber security program. This catalogue should be</p>										

viewed as a collection of recommendations to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security standards for control systems. The recommendations in this catalogue are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cyber security standards specific to their individual security needs.

The main chapter of this catalogue contains a detailed listing of recommended controls from several sources. The organization of each recommendation is based on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, but modified to convey control system language. The following recommended controls are organized into families primarily based on NIST SP 800-53 but with contributions from “Key Elements to a Cyber Security Management System,” (Clause 5) found in the Draft Instrumentation, Systems, and Automation Society (ISA)-d9900.02 document. The “Requirement” section for each security control includes detailed recommended security practices and mechanisms. The “Supplemental Guidance” section provides additional information that may be beneficial for understanding and implementing the recommendation. The last section, “Requirement Enhancements,” includes supplementary security constraints for the recommendation that will result in a more secure environment based on the organization’s predetermined level of protection required for the control system used for the critical process. Not all the recommendations are appropriate for all applications, so it will be necessary to determine the level of

	<p>protection needed and only apply the guidance as appropriate.</p> <p>The following recommendations were obtained from a review of the controls found in various industry standards. Similar controls were identified, and a single recommendation prepared that addressed the intent of the original controls.</p>
--	---

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

Name	Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities										
Type	Guideline										
Group/initiative/organisation	U.S. Department of Energy. Office of Energy Assurance										
Status	Final										
Publication date	August 2002										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>0</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	0
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	0										
Addressed Industry	Energy facilities										
Geographic relevance	USA										
Related standards	N/A										
Description	<p>The purpose of this document is to provide some general guidance and a starting point so that a smaller energy facility is able to identify its critical functions and assets, become aware of threats and vulnerabilities, evaluate and rank the threats in terms of the incidents they may cause, and initiate a security enhancement program, if appropriate.</p> <p>This document considers ICS from a very high level of abstraction. It treats them as any other system (i.e. as a black box) inside an energy facility, describing their properties, helping identifying interdependencies with other systems, etc. This is enough for the purpose of the document which is described above.</p>										
Name	Securing your SCADA and Industrial Control Systems										

Type	Guideline (good practices)										
Group/initiative/organisation	DHS/Department of State - Technical Support Working Group (TSWG)										
Status	Final (version 1.0)										
Publication date	December 2005										
Target audience	<table> <tr> <td>ICS software and equipment manufacturers:</td> <td>1</td> </tr> <tr> <td>ICS integrators:</td> <td>1</td> </tr> <tr> <td>Security tools and services providers:</td> <td>1</td> </tr> <tr> <td>Operators:</td> <td>2</td> </tr> <tr> <td>Research and Academia:</td> <td>1</td> </tr> </table>	ICS software and equipment manufacturers:	1	ICS integrators:	1	Security tools and services providers:	1	Operators:	2	Research and Academia:	1
ICS software and equipment manufacturers:	1										
ICS integrators:	1										
Security tools and services providers:	1										
Operators:	2										
Research and Academia:	1										
Addressed Industry	Generic										
Geographic relevance	USA										
Related standards	N/A										
Description	<p>This guidebook provides information for enhancing the security of Industrial Control Systems (ICS). The information is a comprehensive overview of industrial control system security, including administrative controls, architecture design, and security technology. This guide is intended for all sectors that use ICS technology. This is a guide for enhancing security, not a how-to manual for building an ICS, and its purpose is to teach ICS managers, administrators, operators, engineers, and other ICS staff what security concerns they should be taking into account.</p> <p>This guide does not constitute a standard, and it is not a substitute for standards documents. Neither is this guide a comprehensive security manual. It does not go into detail about any specific technologies; it covers ICS security too broadly to be used as a standalone document. Standards and vendor documents should</p>										

	be consulted for help in properly securing a specific ICS configuration.
--	--

Name	Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities
Type	Guideline/Regulatory <i>Note: The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency's regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required.</i>
Group/initiative/organisation	U.S. Nuclear Regulatory Commission
Status	Final
Publication date	January 2010
Target audience	ICS software and equipment manufacturers: 1 ICS integrators: 1 Security tools and services providers: 2 Operators: 2 Research and Academia: 0
Addressed Industry	Nuclear power plants
Geographic relevance	US/Worldwide
Related standards	NIST SP 800-53, NIST SP 800-82
Description	Title 10, of the Code of Federal Regulations, Section 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54) (Ref. 1) requires, in part, that U.S. Nuclear Regulatory Commission (NRC) licensees provide high assurance that digital computer and communication systems and

networks are adequately protected against cyber attacks, up to and including the design-basis threat.

This regulatory guide provides an approach that the NRC staff deems acceptable for complying with the Commission's regulations regarding the protection of digital computers, communications systems, and networks from a cyber attack as defined by 10 CFR 73.1. Licensees may use methods other than those described within this guide to meet the Commission's regulations if the chosen measures satisfy the stated regulatory requirements.

RG 5.71 describes a regulatory position that promotes a defensive strategy consisting of a defensive architecture and a set of security controls based on standards provided in NIST SP 800-53 and NIST SP 800-82, "Guide to Industrial Control Systems Security," dated September 29, 2008 (Ref. 13). NIST SP 800-53 and SP 800-82 are based on well-understood cyber threats, risks, and vulnerabilities, coupled with equally well-understood countermeasures and protective techniques. Furthermore, NIST developed SP 800-82 for use within industrial control system (ICS) environments, including common ICS environments in which the information technology (IT)/ICS convergence has created the need to consider application of these security controls. RG 5.71 divides the above-noted security controls into three broad categories: technical, operational, and management.

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 Critical Infrastructure (CPNI). (n.d.). *Meridian Process Control Security Information Exchange (MPCSIE)*. Retrieved 2011, from <http://www.cpni.nl/informatieknooppunt/internationaal/mpcsie>

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

- 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 committee and the committee 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 committee and the committee 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>

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

- 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-2010stuxnet2010-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*.
- International 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/pspace/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.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

- 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*.

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

- 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 PCS/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*

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

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.* Department 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 Computer 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/WebApplicationFirewallEvaluationCriteria>

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

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

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

Annex III. ICS Security Related Standards, Guidelines and Policy Documents

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