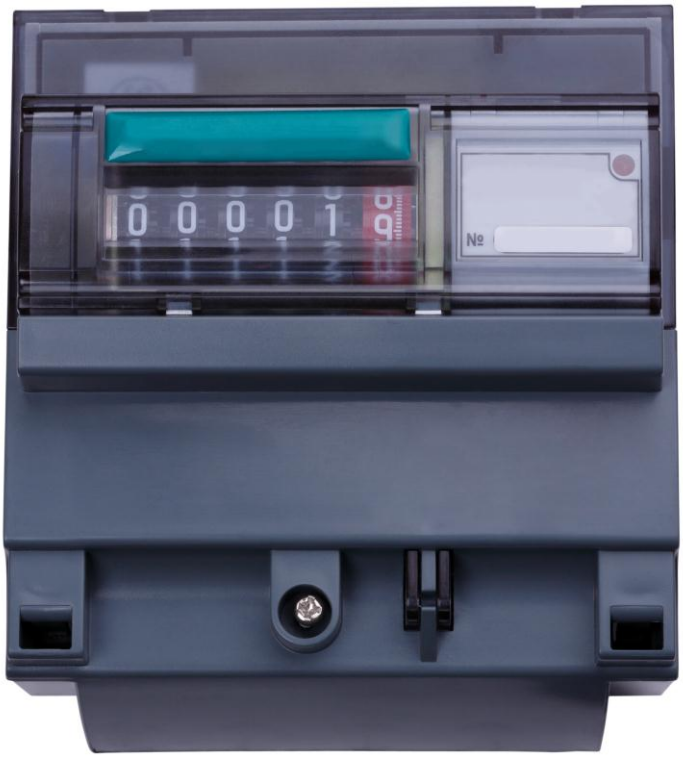
Smart Grid Security



Security related standards, guidelines and regulatory documents

[Deliverable – 2012-03-31]

This document is Annex 4 (of 5) to the ENISA study 'Smart Grid Security: Recommendations for Europe and Member States, June 2012'.

Contributors to this report

ENISA would like to recognise the contribution of the S21sec[1] team members that prepared this report in collaboration with and on behalf of ENISA:

- Elyoenai Egozcue,
- Daniel Herreras Rodríguez,
- Jairo Alonso Ortiz,
- Victor Fidalgo Villar,
- Luis Tarrafeta.

Agreements or Acknowledgements

ENISA would like to acknowledge the contribution of Mr. Wouter Vlegels and Mr. Rafał Leszczyna to this study.

[1] *S21sec, the contractor of ENISA for this study is an international security services company with offices in several countries.*

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@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to ''Smart Grid Security: Recommendations for Europe and Member States'', please use the following details:

- E-mail: Konstantinos.Moulinos@enisa.europa.eu

Contents

1 Introduction

All the information presented here has been based on the previous work done by ENISA on its document "Protecting Industrial Control Systems. Annex III – ICS Security Related Standards, Guidelines and Regulatory Documents" (1). This document provides an overview of existing methods, procedures and guidelines in the area of industrial control system and automation (cyber) security. The results of this document have been revised and filtered to include the last changes as well as to extract the relevant documents with respect to the electricity sector at its very different domains, including: generation, transmission/distribution, metering, etc. 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 are directly extracted from the document itself or from the website of the organization(s) behind them.

In the following lines we provide a list of the standards, guidelines and regulatory documents which were excluded for not being directly related with the power grid or other smart grid related concepts. However, these documents could be an important source of information for any stakeholder of the smart grid which needs to deal with industrial automation or control systems security. For a detailed outlook on all these documents we refer the reader to annex III of ENISA's report "Protecting Industrial Control Systems - Recommendations for Europe and Member States"(1).

As already mentioned, what follows is a comprehensive list of security documents not directly related with the power grid:

- IEC 62443. Security for Industrial Process Measurement and Control: Network and System Security
- Protection Profile for the Gateway of a Smart Metering System
- Security Profile for Advanced Metering Infrastructure
- ISO 27000
- ISO/IEC 15408, Evaluation criteria for IT security (also known as "Common Criteria")
- ISA 99. Manufacturing and Control System Security
- Cyber Security Assessments of Industrial Control Systems. A good practice guide
- Configuring & managing remote access for industrial control systems. A good practice guide
- Good practice guide - Process Control and SCADA Security
- Firewall deployment for SCADA and process control networks. A good practice guide
- Process Control Domain (PCD) – Security Requirements for Vendors
- NAMUR NA 115. IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries
- VDI/VDE 2182 Series
- OLF Guideline No. 104. Information security baseline requirements for process control, safety and support ICT systems

- OLF Guideline No. 110. Implementation of information security in Process Control, Safety and Support ICT Systems during the engineering, procurement and commissioning phases
- CheckIT.
- CRIOP
- Guide to Increased Security in Industrial Control Systems
- NIST SP 800-82. Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-53. Recommended Security Controls for Federal Information Systems
- NISTIR 7176. System Protection Profile - Industrial Control Systems
- Field Device Protection Profile for SCADA Systems in Medium Robustness Environments
- AGA Report No. 12. Cryptographic Protection of SCADA Communications
- API 1164, Pipeline SCADA Security
- API Security Guidelines for the Petroleum Industry
- 21 Steps to improve Cyber Security for SCADA systems
- Catalogue of Control Systems Security: Recommendations for Standards Developers
- Securing your SCADA and Industrial Control Systems

Finally, the following lines provides a concise explanation 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**[2]**:** Standard, guidelines, or regulatory document.
- **Group/initiative/organization:** Group, initiative or organization responsible for the creation of the standard, guideline or regulatory document (e.g. ANSI/ISA).
- **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: Manufacturer or Integrator, Security tools and services Provider, DSO, TSO, Retail Energy Provider, Academia and R&D, Public Bodies. Standardization bodies have not been included for obvious reasons. The level of

[2] ***Guidelines include*** *recommended security good practices, technical reports on specific topics and any worksheet supporting activities such as risk analysis, security requirements definition for Smart Grid components, SG components assessment from a security perspective, etc.*

Standards *include documents intended for defining new security mechanisms or frameworks focusing on interoperability or certification aspects.*

Regulatory documents *are either security guidelines or standards that are considered mandatory from a legal perspective of because it is de facto standard for an industrial association (e.g. DSO operators)*

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:** Generic (Electrical sector), electricity distribution / transportation, Substation Automation, etc.
- **Geographic relevance:** Worldwide, European, Subgroup of European Countries, and National.
- **Related standards:** 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.

2 The Netherlands

Name	Privacy and Security of the Advanced Metering Infrastructure
Type	Guideline (Best practice)
Group/initiative/organisation	Netbeheer Nederland Privacy and Security Working Group
Status	Final (revision 1.5)
Publication date	September 2009
Target audience	Manufacturer or Integrator 1 Security tools and services Provider 2 DSO 2 TSO 1 Retail Energy Provider 0 Academia and R&D 0
Addressed Industry	Generic
Geographic relevance	The Netherlands
Related standards	N/A
Description	The Privacy and Security Working Group defines the framework that will serve as the foundation for securing the advanced metering infrastructure. This foundation must safeguard the availability, integrity and confidentiality of information arising and minimise any damage caused by security incidents within the advanced metering infrastructure. This framework can be used by individual grid operators to implement security requirements and measures. The grid operator itself will specify a timetable indicating when it will comply with these security requirements and measures.

3 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	Manufacturer or Integrator 1 Security tools and services Provider 2 DSO 2 TSO 2 Retail Energy Provider 1 Academia and R&D 0
Addressed Industry	Electricity distribution / transportation
Geographic relevance	France
Related standards	N/A
Description	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.

4 Germany

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	Manufacturer or Integrator 1 Security tools and services Provider 2 DSO 0 TSO 2 Retail Energy Provider 0
Addressed Industry	Power generation
Geographic relevance	Germany
Related standards	N/A
Description	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. 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.

5 USA

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	Manufacturer or Integrator 2 Security tools and services Provider 1 DSO 1 TSO 1 Retail Energy Provider 1 Academia and R&D 0
Addressed Industry	Electricity transportation / distribution
Geographic relevance	North America
Related standards	N/A
Description	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. 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. 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, 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, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. **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.

Name	NISTIR 7628. Guidelines for Smart Grid Cyber Security: • 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	Manufacturer or Integrator	2
	Security tools and services Provider	1
	DSO	1
	TSO	1
	Retail Energy Provider	1
	Academia and R&D	0
Addressed Industry	Electricity distribution	
Geographic relevance	Worldwide	
Related standards	N/A	
Description	**Volume 1** includes: • 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	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	Manufacturer or Integrator	1
	Security tools and services Provider	1
	DSO	2
	TSO	2
	Retail Energy Provider	2
	Academia and R&D	0
Addressed Industry	Generic	
Geographic relevance	USA	
Related standards	N/A	
Description	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. This document considers ICS from a very high level of abstraction. It treats them as any other system (i.e. as a	

	blackbox) 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.

Name	Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities	
Type	Guideline/Regulatory ***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.*	
Group/initiative/organisation	U.S. Nuclear Regulatory Commission	
Status	Final	
Publication date	January 2010	
Target audience	Manufacturer or Integrator Security tools and services Provider DSO TSO Retail Energy Provider Academia and R&D	1 2 0 2 0 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.

Name	Risk Management Process	
Type	Guidelines	
Group/initiative/organisation	U.S. Department of Energy	
Status	Draft	
Publication date	September 2011	
Target audience	Manufacturer or Integrator	0
	Security tools and services Provider	2
	DSO	1
	TSO	1
	Retail Energy Provider	1
	Academia and R&D	0

Addressed Industry	Electric Transmission/Distribution
Geographic relevance	North America
Related standards	N/A
Description	The Department of Energy, in collaboration with the National Institute of Standards and Technology and the North American Electric Reliability Corporation, has released a draft of the Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline for public comment. The RMP Guideline was drafted by a joint public-private sector team that also included representatives from the Federal Energy Regulatory Commission, the Department of Homeland Security, and utilities. The initiative to develop the RMP Guideline is led by the Department's Office of Electricity Delivery and Energy Reliability. The RMP Guideline is designed to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. This guideline offers a flexible approach to managing cybersecurity risks across all levels of the organization. Feedback provided by industry, vendors, and other electricity sector stakeholders will be used to further refine and improve the RMP Guideline prior to final publication.

6 International

Name	IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
Type	Standards
Group/initiative/organisation	IEEE WGC6
Status	Final
Publication date	February, 2011
Target audience	Manufacturer or Integrator 2 Security tools and services Provider 0 DSO 2 TSO 2 Retail Energy Provider 2 Manufacturer or Integrator 2
Addressed Industry	Substation automation
Geographic relevance	Worldwide
Related standards	AGA 12, part 1: IEEE 1711 incorporates the American Gas Association cryptographic protocol (SCADAsafe), 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. 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 (2).
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 independent of the underlying communications protocol. 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.

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 (66).
Publication date	May 2003
Target audience	Manufacturer or Integrator 1 Security tools and services Provider 2 DSO 1 TSO 1 Retail Energy Provider 1 Academia and R&D 1
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 62351. Data and communications security.
Type	Standard
Group/initiative/organisation	IEC TC57 WG15
Status	Final (revision 1)
Publication date	May 2007
Target audience	Manufacturer or Integrator 1 Security tools and services Provider 2 DSO 2 TSO 2 Retail Energy Provider 1 Academia and R&D 1
Addressed Industry	Generic
Geographic relevance	Worldwide
Related standards	IEC 60870-5 (IEC 101, IEC 104, DNP3) (3), IEC 60870-6 (TASSE.2/ICCP)(4), IEC 61850(5) (6), IEC 61970 (7), and the IEC 61968 (8).
Description	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-toend security issues. • **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 operations. • **IEC 62351-2** includes the definition of terms and acronyms used in the IEC 62351 standards. • **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. • **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. Other parts are expected to follow to address more areas of information security.

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	Manufacturer or Integrator	1
	Security tools and services Provider	0
	DSO	2
	TSO	2
	Retail Energy Provider	0
	Academia and R&D	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 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	Manufacturer or Integrator	2
	Security tools and services Provider	0
	DSO	2
	TSO	2
	Retail Energy Provider	1
	Academia and R&D	1
Addressed Industry	Electricity distribution / transportation	
Geographic relevance	Worldwide	
Related standards	NERC CIP 002 – 009 (9)(10)(11)(12)(13)(14)(15)(16)	
Description	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 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.	

7 Bibliography

1. **European Network and Informations Security Agency (ENISA).** *Protecting Industrial Control Systems - Recommendations for Europe and Member States.* 2011.

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

3. **International Electrotechnical Commission (IEC).** *IEC 60870-5: Telecontrol equipment and system.* 2007.

4. —. *IEC 60870-6: Telecontrol equipment and systems.* 2005.

5. —. *IEC 61850: Communication networks and systems in substations.* 2011.

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

7. —. *IEC 61970: Common Information Model (CIM) / Energy Management.*

8. —. *IEC 61968: Common Information Model (CIM) / Distribution Management.*

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

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

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

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

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

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

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

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

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

18. **Zhang, Zhen.** *Smart Grid in America and Europe: Similar Desires, Different Approaches (Part 2). .* 2011.

19. —. *Smart Grid in America and Europe: Similar Desires, Different Approaches (Part 1).* . 2011.

20. **Yin Hong, Chang.** *Cyber Security of a Smart Grid: Vulnerability Assessment.* s.l. : http://www.ece.nus.edu.sg/stfpage/elejp/FYP/CYH09.pdf, 2010.

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

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

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

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

25. **Syngres, Eric Knapp.** *Industrial Network Security. Securing critical infrastructure Networks for Smart Grid, SCADA and other Industrial Control Systems.* .

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

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

28. **Snyder, Mike.** *Smart Grid Synergy.* [Online] http://ict2020.tiaonline.org/may_june_2009/policy_stimulus.cfm.

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

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

31. **Mo, Yilin, et al.** *Cyber–Physical Security of a Smart Grid Infrastructure.* s.l. : http://sparrow.ece.cmu.edu/group/pub/Mo-Kim-etal-ProcIEEE-2011.pdf, 2011.

32. **Masica, Ken.** *Securing WLANs using 802.11i. Draft. Recommended Practice.* 2007.

33. —. *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments.* 2007.

34. **Lewis, Adam.** *ERN-CIP: European reference network for critical infrastructure protection.* [Online] http://www.creatif-network.eu/workshop1/Lewis_session3.pdf.

35. **Lenzini, G., Oostdijk, M. and Teeuw, W.** *Trust, Security, and Privacy for the Advanced Metering Infrastructure.* s.l. : https://doc.novay.nl/dsweb/Get/Document-100649, 2009.

36. **Kwasinski, A.** *Implication of Smart-Grids development for communication systems in normal operation and during disasters.* 2010.

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

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

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

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

41. **Hayden, Ernie.** *There is No SMART in Smart Grid Without Secure and Reliable Communications.* s.l. : http://www.verizonbusiness.com/resources/whitepapers/wp_no-smart-in-smart-grid-without-secure-comms_en_xg.pdf.

42. **Hart, D.G.** *Using AMI torealize the Smart Grid. En Powerand energy society general meeting -Conversion and delivery of electrical energy in the 21st Century.* s.l. : IEEE 2008, 2008.

43. **Green, Brian D., Cote, J. R. and Simmins, John.** Smartgridinformation.info. [Online] 17 8 2010. [Cited: 30 12 2011.] http://www.smartgridinformation.info/pdf/2663_doc_1.pdf.

44. **Gorman, Siobhan.** *Electricity Grid in U.S. Penetrated By Spies.*

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

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

47. **Giordano, Vincenzo, et al.** *Smart Grid projects in Europe: lessons learned and current developments.* 2011.

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

49. **Flick, Tony and Morehouse, Justin.** *Securing the Smart Grid. Next Generation Power Grid Security.* 2011.

50. **Fan, Jiyuan and Zhang, Xiaoling.** Feeder Automation within the Scope of Substation Automation. [Online] 10 31, 2006. [Cited: 12 29, 2011.] http://www.ieee.org/portal/cms_docs_pes/pes/subpages/meetings-folder/PSCE/PSCE06/panel24/Panel-24-3_Feeder_Automation.pdf.

51. **Fan, Jiyuan, du Toit, Willem and Backschneider, Paul.** *Distribution Substation Automation in Smart Grid.*

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

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

54. **Ebinger, Charles and Massy, Kevin.** *Software and hard targets: enhancing Smart Grid cyber security in the age of information warfare.* s.l. : http://www.brookings.edu/~/media/Files/rc/papers/2011/02_smart_grid_ebinger/02_smart_grid_ebinger.pdf, 2011.

55. **Díaz Andrade, Carlos Andrés and Hernandez, Juan Carlos.** *Smart grid: Las TICs y la modernización de las redes de energía eléctrica – Estado del arte.* 2011.

56. **Davis, Mike.** *SmartGrid Device Security. Adventures in a new medium.* s.l. : https://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf, 2009.

57. **Conant, Rob.** *Toward a Global Smart Grid - The U.S. vs. Europe.* [Online] http://www.elp.com/index/display/article-display/2702271845/articles/utility-automation-engineering-td/volume-15/Issue_5/Features/Toward_a_Global_Smart_Grid_-_The_US_vs_Europe.html .

58. —. *Toward a Global Smart Grid - The U.S. vs. Europe.* [Online] http://www.elp.com/index/display/article-display/2702271845/articles/utility-automation-engineering-td/volume-15/Issue_5/Features/Toward_a_Global_Smart_Grid_-_The_US_vs_Europe.html.

59. **Coll-Mayor, Debora.** *Overview of strategies and goals.* [Online] http://www.4thintegrationconference.com/downloads/Strategies & Goals of Smartgrid in Europe.pdf.

60. **Cleveland, Frances.** *White Paper: Cyber Security Issues for the Smart Grid.* s.l. : http://www.xanthus-consulting.com/Publications/White_Paper_Cyber_Security_Issues_for_the_Smart_Grid.pdf, 2009.

61. **Clemente, Jude.** *The Security Vulnerabilities of Smart Grid.* s.l. : http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345, 2009.

62. **Chebbo, Maher.** *Recommendations of the SmartGrid ICT consultation Group to the European Commision.* 2010.

63. **Carpenter, Matthew and Wright, Joshua.** *Advanced metering infrastructure attack methodology.* 2009.

64. **Brodsy, Jacob and McConnell, Anthony.** *Jamming and Interference Induced Denial-of-Service Attacks on IEEE 802.15.4-Based Wireless Networks.* 2009.

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

66. —. *SCADA Supervisory and Data Acquisition.* 2004.

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

68. **Bartels, Guido.** *Combating Smart Grid Vulnerabilities.* s.l. : http://www.ensec.org/index.php?option=com_content&view=article&id=284:combating-smart-grid-vulnerabilities&catid=114:content0211&Itemid=374, 2011.

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

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

71. **Anderson, Roger N., et al.** *Computer-Aided Lean Management for the Energy Industry.* 2008.

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

73. **Amin, S. Massoud.** *Smart Grid: Overview, Issues and Opportunities. Advances and Challenges in Sensing, Modeling, Simulation, Optimization and Control.* s.l. : http://central.tli.umn.edu/CDC_Semi_plenary_Smart%20Grids_Massoud%20Amin_final.pdf, 2011.

74. **Abbott, Ralph E.** *The Successful AMI Marriage: When Water AMR and Electric AMI Converge.* [Online] http://www.waterworld.com/index/display/article-display/328763/articles/waterworld/volume-24/issue-5/editorial-feature/the-successful-ami-marriage-when-water-amr-and-electric-ami-converge.html.

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

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

77. **WirelessHART.** *WirelessHART.* [Online] http://www.hartcomm.org/protocol/wihart/wireless_technology.html.

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

79. —. *WGC1 - Application of Computer-Based Systems.* http://standards.ieee.org/develop/wg/WGC1.html.

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

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

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

83. **KEMA and ENA.** UK Smart Grid Cyber Security Report. *http://ses.jrc.ec.europa.eu/.* [Online] 2011. http://energynetworks.squarespace.com/storage/UK Smart Grid Cyber Security Report.pdf.

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

85. **Pacific Northwest National Labortory, U.S. Department of Energy.** *The Role of Synchronized Wide Area Measurements for Electric Power Grid Operations.* 2006.

86. **EURELECTRIC Networks Committee.** *The Role of Distribution System. Operators (DSOs) as Information Hubs.* 2010.

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

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

89. **International Energy Agency (IEA).** *Technology Roadmap. Smart Grids.* France : OCDE/IEA, 2011.

90. **EPRI.** *Technical and System Requirements for Advanced Distribution Automation.* 2004.

91. **International Federation of Automatic Control (IFAC).** TC 6.3. Power Plants and Power Systems — IFAC TC Websites. [Online] http://tc.ifac-control.org/6/3.

92. —. TC 3.1. Computers for Control — IFAC TC Websites. [Online] http://tc.ifac-control.org/3/1.

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

94. **CEN/CENELEC/ETSI Joint Working Group.** *Standards for Smart Grids.* 2011.

95. **European Commission. Directorate-General for Energy.** *Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. M/490.* s.l. : http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf.

96. Smart Substations. *Smart Substations:Desing, Operations and Maintenance.* [Online] http://www.smartsubstations.com.au/Event.aspx?id=664622.

97. **EnergieNed.** *Smart Meter Requirements. Dutch Smart Meter specification and tender dossier.* s.l. : http://www.energiened.nl/_upload/bestellingen/publicaties/288_Dutch%20Smart%20Meter%20%20v2.1%20final%20Main.pdf, 2008.

98. **European Commision. Energy.** *Smart Grids Task force.* [Online] http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm.

99. **U.S. Department of Energy.** *Smart Grid System Report.* 2009.

100. **Industrial Defender.** *Smart Grid Safety vs Confidentiality.* s.l. : http://blog.industrialdefender.com/?p=756, 2011.

101. **Enerweb.** *Smart grid Information Report.* s.l. : http://enerweb.co.za/brochures/Smart%20Grid%20Information%20Report.pdf, 2011.

102. **IEEE Smart grid.** *Smart Grid Conceptual Model.* [Online] http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model.

103. **Sonoma innovation.** *Smart Grid Communications Architectural Framework.* 2009.

104. **EU Commission Task Force for Smart Grids. Expert Group 4.** *Smart Grid aspects related to Gas.* 2011.

105. **European Commision.** Smart electricity Systems. *European CommisionJoint Research Centre.* [Online] http://ses.jrc.ec.europa.eu/.

106. **Siemens.** Smart Distribution. Distribution Automation and Protection. [Online] [Cited: 29 12 2011.] http://www.energy.siemens.com/fi/en/energy-topics/smart-grid/smart-distribution/distribution-automation-and-protection.htm.

107. **The Climate Group.** *smart 2020: enabling the low carbon economy in the information age.* [Online] 2008.

108. **Treehugger.** *SMART 2020 Report: Smart Grids Can Cut CO2 Emissions by 15 Percent.* [Online] 2011. http://www.treehugger.com/clean-technology/smart-2020-report-smart-grids-can-cut-co2-emissions-by-15-percent.html.

109. **smart 2020.** *Smart 2020 .* [Online] 2009. http://www.smart2020.org/.

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

111. **The AMI-SEC Task Force (UCAIug) and The NIST Cyber Security Coordination Task Group.** *SECURITY PROFILE FOR ADVANCED METERING INFRASTRUCTURE.* 2010.

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

113. **ABB.** *Security in the smart grid.* s.l. : http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf, 2009.

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

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

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

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

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

119. **RISI.** *Repository of Industrial Security Incidents.* [Online] http://www.securityincidents.org/.

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

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

122. **Wikipedia.** Recloser. [Online] [Cited: 12 26, 2011.] http://en.wikipedia.org/wiki/Recloser.

123. **Iberdrola.** Proyecto tipo para Centro de Transformación intemperie compacto. [En línea] Abril de 1997. [Citado el: 29 de Diciembre de 2011.] http://www.coitiab.es/reglamentos/electricidad/reglamentos/jccm/iberdrola/mt_2-11-05.htm.

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

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

126. —. *Process control and SCADA security. Guide 6. Engage projects.* Centre for the Protection of National Infrastructure.

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

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

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

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

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

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

133. **Institute of Electrical and Electronics Engineers (IEEE).** *P2030: IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.* 2011.

134. **Wikipedia.** *Outage management system.* [Online] http://en.wikipedia.org/wiki/Outage_management_system.

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

136. **OpenSG.** Open Smart Grid. *http://osgug.ucaiug.org.* [Online]

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

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

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

140. —. *NISTIR 7176: System Protection Profile - Industrial Control Systems.* Decisive Analytics. 2004.

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

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

143. —. *NIST SP 1108: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0.* 2010.

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

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

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

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

148. **European Commision.** *M/441:* . http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf : s.n., 2009.

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

150. —. ISA99 Committee - Home. [Online] http://isa99.isa.org/ISA99 Wiki/Home.aspx.

151. —. *ISA100, Wireless Systems for Automation.* [Online] www.isa.org/isa100.

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

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

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

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

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

157. —. IFIP TC 8 International Workshop on Information Systems Security Research. [Online] http://ifip.byu.edu.

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

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

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

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

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

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

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

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

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

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

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

169. **ICT4SMARTDG.** *ICT Solutions to enable Smart Distributed Generation.* 2011.

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

171. **Energie Vortex.** *http://www.energyvortex.com.* [Online] http://www.energyvortex.com/energydictionary/blackout__brownout__brown_power__rolling_blackout.html.

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

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

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

175. **BBC news.** *Hackers 'hit' US water treatment systems.* s.l. : http://www.bbc.co.uk/news/technology-15817335, 2011.

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

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

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

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

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

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

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

183. **National Institute of Standards and Technology (NIST).** FIPS PUB 199. *Standards for Security Categorization of Federal Information and Information Systems.* [Online] 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

184. **EU Commission Task Force for Smart Grids.** *Expert Group 1: Functionalities of smart grids and smart meters.* 2010.

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

186. **European Commission. Europ2 2020.** *Europe 2020 targets.* [Online] http://ec.europa.eu/europe2020/reaching-the-goals/targets/index_en.htm.

187. *Eur Lex.* [Online] http://eur-lex.europa.eu/en/index.htm.

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

189. **Instituto de Investigaciones Eléctricas de México.** *Estado del arte en Redes Inteligentes "Smart Grids". Automatización de la Distribución en las Redes Inteligentes.* México : s.n.

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

191. **Energie.gov.** *Energy Storage.* [Online] http://energy.gov/oe/technology-development/energy-storage.

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

193. *Energy Independence and Security Act of 2007.* s.l. : http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6enr.txt.pdf, 2007.

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

195. **U.S. Department of Energy.** *Electricity sector cyber-security risk management process guideline.* 2011.

196. **Government Accountability Office (GAO).** *Electricity grid modernization. Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed.* s.l. : http://www.gao.gov/new.items/d11117.pdf, 2011.

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

198. **Smarter Grid Solutions.** *Dynamic Line Rating - managing capacity.* [Online] http://www.smartergridsolutions.com/index.html?pid=153.

199. **National Institute of Standards and Technology (NIST).** *Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0.* 2011.

200. **Wikipedia.** *Distribution mangagement system.* [Online] http://en.wikipedia.org/wiki/Distribution_mangagement_system.

201. **Commission of the European communities.** *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* 1995.

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

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

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

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

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

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

208. **Thales.** *Critical Infrastructure Security. A Holistic Security Risk Management Approach.* s.l. : http://www.securitymanagement.com.au/content/file/CriticalISThales.pdf?asm=ad05637d37e2a8c1afeeda016804c85, 2008.

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

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

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

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

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

214. **Department of Energy (DoE).** Control Systems Security Publications Library. [Online] http://energy.gov/oe/control-systems-security-publications-library.

215. **United States Computer Emergency Readiness Team (US-CERT).** Control Systems Security Program: Industrial Control Systems Joint Working Group. [Online] http://www.us-cert.gov/control_systems/icsjwg/index.html.

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

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

218. **ICT4SMARTDG.** *Consensus on ICT solutions for a Smart Distribution at Domestic Level.* 2011.

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

220. **Commission of the European communities.** *Communication from the commission. Energy infrastructure priorities for 2020 and beyond – A Blueprint for an integrated European energy network. COM(2010) 677.* 2010.

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

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

223. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions: A Digital Agenda for Europe. COM(2010)245 final.* 2010.

224. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Energy 2020: A strategy for competitive, sustainable and secure energy. COM(2010) 639 final.* 2010.

225. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. Digital Agenda for Europe. COM(2010) 245.* 2010.

226. —. *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. COM(2011) 202 final.* 2011.

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

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

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

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

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

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

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

234. **Council of the European Union.** *Brussels European Council 8/9 march 2007. Presidency conclusions.* 2007.

235. **Power Systems Engineering Research Center.** *Automated Circuit Breaker Monitoring.* 2007.

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

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

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

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

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

241. **AMI-SEC-ASAP.** *AMI System Security Requirements.* 2008.

242. —. *AMI Security Implementation Guide.* 2009.

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

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

245. **Wikipedia.** Advanced Distribution Automation. [Online] [Cited: 02 01 2012.] http://en.wikipedia.org/wiki/Advanced_Distribution_Automation.

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

247. **Europe 2020.** *A resource-efficient Europe – Flagship initiative of the Europe 2020 Strategy.* [Online] http://ec.europa.eu/resource-efficient-europe/index_en.htm.

248. **EOS Energy Infrastructure Protection & Resilience Working Group.** *A global european approach for energy infrastructure protection & resilience.* s.l. : http://www.eos-eu.com/LinkClick.aspx?fileticket=DEvuI/4l1jU=&tabid=232, 2009.

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

250. **International Electrotechnical Commission (IEC).** *IEC 62443: Security for Industrial Process Measurement and Control: Network and System Security.* 2010.

251. —. *IEC TR 62210: Power system control and associated communications – Data and communication security.* 2003-05.

252. —. *ISO/IEC 15408: Information technology. Security techniques. Evaluation criteria for IT security.* 2009-2011.

253. **NAMUR.** *NAMUR NA 115 IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries.* 2006.

254. **VDI/VDE.** *VDI/VDE 2182: IT security for industrial automation.* 2011.

255. **SINTEF.** *CRIOP: A scenario method for Crisis Intervention and Operability analysis.* 2011.

256. **National Institute of Standards and Technology (NIST).** *Field Device Protection Profile for SCADA Systems in Medium Robustness Environments.* 2006.

257. **DLMS User Association.** *COSEM: Identification System and Interface Classes.* 2010.

258. —. *DLMS/COSEM: Architecture and Protocols.* 2009.

259. —. *DLMS/COSEM: Conformance Testing Process.* 2010.

260. —. *COSEM: Glossary of Terms.* 2003.

261. **IEC.** *IEC TS 62351-5: Power systems management and associated information exchange – Data and.*

262. **American National Standard (ANSI).** *ANSI C12.19: American National Standard for Utility Industry End Device Data Tables.* 2008.

263. —. *ANSI C12.18: American National Standard for Protocol Specification for ANSI Type 2 Optical Port.* 2006.

264. —. *ANSI C12.21: American National Standard for Protocol Specification for Telephone Modem Communication.* 2006.

8 Abbreviations

ACER	Agency for the Cooperation of Energy Regulators
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
BAN	Building Area Networks
BPL	Broadband over power line
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIA	Confidentially, Integrity and Availability
CO2	Carbon dioxide
COTS	Commercial of the Self
DG ENER	Directorate-General for Energy
DLMS/COSEM	Device Language Message specification/COmpanion Specification for Energy Metering
DLR	Dynamic Line Ratings
DMS	Distribution Management System
DSM	Demand Side Management
DSO	Distribution System Operators
EACI	European Association for Creativity and Innovation
EC	the European Commission
ENISA	European Network and Information Security Agency
ENTSO	European Network of Transmission System Operators for Electricity
ETP	Executive Training Programme
ETSI	European Telecommunications Standards Institute
EU	European Union
FAN	Field Area Network
FTP	File Transfer Protocol
GHG	Greenhouse Gas
GPRS	General Packet Radio Service
HAN	networks (Home Area Network
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IAC	Integrity, Availability, Confidentiality
IAN	Industrial Area Networks
ICS	Industrial Control Systems
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IPS/IDS	Intrusion Protection/Detection System
IP-Sec	Internet Protocol secure
ISM	Information Security Management

ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
LAN	Local Area Network
MAN	Metropolitan Area Network
MID	Measuring Instruments Directive
MPLS	Multiprotocol Label Switching
NAN	Neighbourhood Area Network
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OMS	Outage Management System
OWASP	Open Web Application Security Project
PLC	power line communications
R&D	Research and Development
RF	radio frequency
RTU	remote terminal units
SCADA	Supervisory Control and Data Acquisition
SFTP	Secure File Transfer Protocol
SG	Smart grid
SIEM	Security information and event management
SMART	standardization (S), monitoring (M) accounting (A) rethink (R) transformation (T)
SSH	Secure Shell
SW	Software
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunications Network
TSO	Transmission System Operators
UK	United Kingdom
USA/US	United States of America
VPN	Virtual Private Network
WAN	Wide Area Networks

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