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

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), 2012
Contents

1 Introduction ............................................................................................................................ 1
2 The Netherlands .................................................................................................................... 4
3 France ................................................................................................................................... 5
4 Germany ............................................................................................................................... 6
5 USA ....................................................................................................................................... 7
6 International .......................................................................................................................... 14
7 Bibliography .......................................................................................................................... 19
8 Abbreviations ........................................................................................................................ 36
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:

- 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
Security related standards, guidelines and regulatory documents

- 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 800-53. 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
- 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**: 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Privacy and Security of the Advanced Metering Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Guideline (Best practice)</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>Netbeheer Nederland Privacy and Security Working Group</td>
</tr>
<tr>
<td>Status</td>
<td>Final (revision 1.5)</td>
</tr>
<tr>
<td>Publication date</td>
<td>September 2009</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider</td>
</tr>
<tr>
<td></td>
<td>DSO</td>
</tr>
<tr>
<td></td>
<td>TSO</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D</td>
</tr>
<tr>
<td>Addressed Industry</td>
<td>Generic</td>
</tr>
<tr>
<td>Geographic relevance</td>
<td>The Netherlands</td>
</tr>
<tr>
<td>Related standards</td>
<td>N/A</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 3 France

<table>
<thead>
<tr>
<th>Name</th>
<th>Managing Information Security in an Electric Utility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Guideline (Technical report)</td>
</tr>
<tr>
<td><strong>Group/initiative/organisation</strong></td>
<td>CIGRE, JWG D2/B3/C2-01 Security for Information Systems and Intranets in Electric Power Systems</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Final</td>
</tr>
<tr>
<td><strong>Publication date</strong></td>
<td>September 2005</td>
</tr>
<tr>
<td><strong>Target audience</strong></td>
<td>Manufacturer or Integrator</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider</td>
</tr>
<tr>
<td></td>
<td>DSO</td>
</tr>
<tr>
<td></td>
<td>TSO</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D</td>
</tr>
<tr>
<td><strong>Addressed Industry</strong></td>
<td>Electricity distribution / transportation</td>
</tr>
<tr>
<td><strong>Geographic relevance</strong></td>
<td>France</td>
</tr>
<tr>
<td><strong>Related standards</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
## 4 Germany

<table>
<thead>
<tr>
<th>Name</th>
<th>VGB R175. IT security for generating plants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Guideline (good practices)</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>VGB Group</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Publication date</td>
<td>May 2006</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator: 1 &lt;br&gt; Security tools and services Provider: 2 &lt;br&gt; DSO: 0 &lt;br&gt; TSO: 2 &lt;br&gt; Retail Energy Provider: 0</td>
</tr>
<tr>
<td>Addressed Industry</td>
<td>Power generation</td>
</tr>
<tr>
<td>Geographic relevance</td>
<td>Germany</td>
</tr>
<tr>
<td>Related standards</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**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.
## USA

<table>
<thead>
<tr>
<th>Name</th>
<th>NERC CIP 002 – 009. Reliability Standards for the Bulk Electric Systems in North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Regulation</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>North American Electric Reliability Corporation (NERC)</td>
</tr>
<tr>
<td>Status</td>
<td>Final. Revision 4.</td>
</tr>
<tr>
<td>Publication date</td>
<td>January 2011</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator 2</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider 1</td>
</tr>
<tr>
<td></td>
<td>DSO 1</td>
</tr>
<tr>
<td></td>
<td>TSO 1</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider 1</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D 0</td>
</tr>
<tr>
<td>Addressed Industry</td>
<td>Electricity transportation / distribution</td>
</tr>
<tr>
<td>Geographic relevance</td>
<td>North America</td>
</tr>
<tr>
<td>Related standards</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>NISTIR 7628. Guidelines for Smart Grid Cyber Security:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Vol. 1, Smart Grid Cyber Security Strategy,</td>
</tr>
<tr>
<td></td>
<td>Architecture, and High-Level Requirements.</td>
</tr>
<tr>
<td></td>
<td>- Vol. 2, Privacy and the Smart Grid.</td>
</tr>
<tr>
<td></td>
<td>- Vol.3, Supportive Analyses and References.</td>
</tr>
<tr>
<td>Type</td>
<td>Guideline (Technical report)</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>National Institute of Standards and Technology (NIST)</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Publication date</td>
<td>August 2010</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider</td>
</tr>
<tr>
<td></td>
<td>DSO</td>
</tr>
<tr>
<td></td>
<td>TSO</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Addressed Industry</th>
<th>Electricity distribution</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Geographic relevance</th>
<th>Worldwide</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Related standards</th>
<th>N/A</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Volume 1 includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>● The high level security requirements for the Smart Grid for each of the 22 logical interface categories included.</td>
</tr>
<tr>
<td></td>
<td>● Cryptographic and key management issues across the scope of systems and devices found in the Smart Grid along with potential alternatives.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Volume 2 includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Volume 3 includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>● Classes of potential vulnerabilities for the Smart Grid. Individual vulnerabilities are classified by category.</td>
</tr>
</tbody>
</table>
### Security related standards, guidelines and regulatory documents

<table>
<thead>
<tr>
<th>Name</th>
<th>Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Guideline</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Publication date</td>
<td>August 2002</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator 1</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider 1</td>
</tr>
<tr>
<td></td>
<td>DSO 2</td>
</tr>
<tr>
<td></td>
<td>TSO 2</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider 2</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D 0</td>
</tr>
<tr>
<td>Addressed Industry</td>
<td>Generic</td>
</tr>
<tr>
<td>Geographic relevance</td>
<td>USA</td>
</tr>
<tr>
<td>Related standards</td>
<td>N/A</td>
</tr>
<tr>
<td>Description</td>
<td>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</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Regulatory Guide 5.71. Cyber Security Programs for Nuclear Facilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Guideline/Regulatory</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Group/initiative/organisation</th>
<th>U.S. Nuclear Regulatory Commission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Publication date</td>
<td>January 2010</td>
</tr>
</tbody>
</table>

**Target audience**

- Manufacturer or Integrator: 1
- Security tools and services Provider: 2
- DSO: 0
- TSO: 2
- Retail Energy Provider: 0
- Academia and R&D: 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Risk Management Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Guidelines</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>U.S. Department of Energy</td>
</tr>
<tr>
<td>Status</td>
<td>Draft</td>
</tr>
<tr>
<td>Publication date</td>
<td>September 2011</td>
</tr>
<tr>
<td>Target audience</td>
<td></td>
</tr>
<tr>
<td>Manufacturer or Integrator</td>
<td>0</td>
</tr>
<tr>
<td>Security tools and services Provider</td>
<td>2</td>
</tr>
<tr>
<td>DSO</td>
<td>1</td>
</tr>
<tr>
<td>TSO</td>
<td>1</td>
</tr>
<tr>
<td>Retail Energy Provider</td>
<td>1</td>
</tr>
<tr>
<td>Academia and R&amp;D</td>
<td>0</td>
</tr>
</tbody>
</table>
Security related standards, guidelines and regulatory documents

<table>
<thead>
<tr>
<th><strong>Addressed Industry</strong></th>
<th>Electric Transmission/Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Geographic relevance</strong></td>
<td>North America</td>
</tr>
<tr>
<td><strong>Related standards</strong></td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
### 6 International

<table>
<thead>
<tr>
<th>Name</th>
<th>IEEE 1711. Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Standards</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>IEEE WGC6</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Publication date</td>
<td>February, 2011</td>
</tr>
</tbody>
</table>
| 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. |
IEC 62210. Power system control and associated communications - Data and communication security

- **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.
### Security related standards, guidelines and regulatory documents

<table>
<thead>
<tr>
<th>Name</th>
<th>IEC 62351. Data and communications security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Standard</td>
</tr>
<tr>
<td>Group/initiative/organisation</td>
<td>IEC TC57 WG15</td>
</tr>
<tr>
<td>Status</td>
<td>Final (revision 1)</td>
</tr>
<tr>
<td>Publication date</td>
<td>May 2007</td>
</tr>
<tr>
<td>Target audience</td>
<td>Manufacturer or Integrator 1</td>
</tr>
<tr>
<td></td>
<td>Security tools and services Provider 2</td>
</tr>
<tr>
<td></td>
<td>DSO 2</td>
</tr>
<tr>
<td></td>
<td>TSO 2</td>
</tr>
<tr>
<td></td>
<td>Retail Energy Provider 1</td>
</tr>
<tr>
<td></td>
<td>Academia and R&amp;D 1</td>
</tr>
<tr>
<td>Addressed Industry</td>
<td>Generic</td>
</tr>
<tr>
<td>Geographic relevance</td>
<td>Worldwide</td>
</tr>
<tr>
<td>Related standards</td>
<td>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).</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• IEC 62351-2 includes the definition of terms and acronyms used in the IEC 62351 standards.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• IEC 62351-7 addresses one area among many possible</td>
</tr>
</tbody>
</table>
Security related standards, guidelines and regulatory documents

<table>
<thead>
<tr>
<th>Name</th>
<th>IEEE 1402. Guide for Electric Power Substation Physical and Electronic Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Standard / Guideline</td>
</tr>
<tr>
<td><strong>Group/initiative/organisation</strong></td>
<td>IEEE E7.1402</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Final</td>
</tr>
<tr>
<td><strong>Publication date</strong></td>
<td>April 2000</td>
</tr>
</tbody>
</table>
| **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. |

- **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

**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


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

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


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


Security related standards, guidelines and regulatory documents


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


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

Security related standards, guidelines and regulatory documents

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


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.


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


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


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


Security related standards, guidelines and regulatory documents


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


Security related standards, guidelines and regulatory documents


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


Security related standards, guidelines and regulatory documents


Security related standards, guidelines and regulatory documents


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


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

222. —. 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. 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.


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.


Security related standards, guidelines and regulatory documents


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


Security related standards, guidelines and regulatory documents


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

Security related standards, guidelines and regulatory documents

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