IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 10: Security architecture guidelines

IEC/TR 62351-10:2012(E)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,…).
It also gives information on projects, replaced and withdrawn publications.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC/TR 62351-10

Edition 1.0 2012-10

TECHNICAL REPORT

colour inside

Power systems management and associated information exchange – Data and communications security – Part 10: Security architecture guidelines

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.200

ISBN 978-2-83220-419-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 10: Security architecture guidelines

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62351-10, which is a technical report, has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
57/1234/DTR	57/1265/RVC

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange – Data and communications security,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Cyber security becomes more and more a basic necessity in power control systems as standard IT and other forms of modern communication technology are being increasingly used for control and supervision of these systems. The application of IT communication technology demands the consideration of already existing vulnerabilities, which can be exploited by potential attackers, as recent intentional and unintentional cyber incidents on SCADA and other industrial control systems have shown. The increasing number of control system cyber incidents world-wide with medium to high impact underlines the importance of appropriate security measures (see [11][1]).

The International Electrotechnical Commission (IEC) Technical Committee (TC) 57 (Power Systems Management and Associated Information Exchange) is responsible for developing international standards for power system data communications protocols. Standards developed within TC 57 comprise for instance IEC 60870-5, IEC 61850, and IEC 62351 just to state a few. Especially the latter addresses technical security controls within power systems.

A security architecture as targeted here does not only comprise technical means like the application of dedicated security entities, security protocols or security options in communication protocols to secure power system entities or the communication network. It also describes operational guidelines considering the available technical base as well as the personnel controlling the power systems. Moreover, interactions with existing (security) infrastructures also affect overall system security.

In this Technical Report hands-on guidelines are proposed for the implementation of security mechanisms based on deployment examples, rather than a lecture or reference book for security in general. Therefore, available resources of information related to security of power systems or more general to security in Smart Grid are utilized and will be referenced as much as possible, without repeating their content here. Thus this Technical Report addresses both, the power system engineer and the traditional IT security engineer.

The examples used throughout this Technical Report are intended to better explain the influences of and the interactions with security. They are used as descriptive examples without the claim to be complete.

Clause 4 of this Technical Report specifies the specifics of the power systems industry, comprising differences in the security requirements compared to office systems as well as an overview about related standardization. It also introduces the TC 57 reference architecture as one base for the security architecture discussion.

Clause 5 establishes a general approach to a security architecture by using security domains and dedicated security controls within these domains and maps this approach to the power system domain based on examples use cases. Clause 5 also addresses the mapping of the NIST identified interface categories with the TC 57 architecture interfaces.

Clause 6 maps security controls with the IEC TC 57 power system architecture based on example scenarios. It starts with an overview scenario of power systems and digs into dedicated sub-scenarios like a substation deployment, the communication between a substation and a control centre and so on.

---

1 References in square brackets refer to the Bibliography.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE – DATA AND COMMUNICATIONS SECURITY –

Part 10: Security architecture guidelines

1 Scope

This part of IEC 62351, which is a Technical Report, targets the description of security architecture guidelines for power systems based on essential security controls, i.e. on security-related components and functions and their interaction. Furthermore, the relation and mapping of these security controls to the general system architecture of power systems is provided as a guideline to support system integrators to securely deploy power generation, transmission, and distribution systems applying available standards.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC/TS 62351-2, as well as the following apply.

3.1.1
de-militarized zone
DMZ
LAN segment / zone used to tier application/UI/file access between two other zones/segments

3.1.2
reliability
ability of a system to perform a required function under stated conditions for a specified period of time

3.1.3
security controls
technical or procedural security counter measures to avoid, counteract or minimize security risks

3.2 Abbreviations

For the purposes of this document, the following abbreviations apply.

ACL access control lists

BDEW	Bundesverband Für Energie- und Wasserwirtschaft
BES	bulk energy system
CA	certification authority that issues digital certificates
CSWG	cyber security working group
DHS	department of homeland security
DMZ	de-militarized zone
DoS	denial of service
DTLS	datagram transport layer security
DTR	draft technical report
HMAC	hashed message authentication codes
HTTPS	secure hypertext transfer protocol
HSM	hardware security module
IDS	intrusion detection system
IP	internet protocol
IPS	intrusion prevention system
LAN	local area network (it is the Ethernet IP network inside a security domain)
LDAP	lightweight directory access protocol
NTP	network time protocol
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NWIP	new work item proposal
OS	operating system
OTP	one time password authentication
RBAC	remote based access control
RDP	remote desktop protocol
PKI	public key infrastructure
SGIP	Smart Grid interoperability panel
SNMP	simple network management protocol
TCP	transmission control protocol
TPM	trusted platform module
TLS	transport layer security
TR	technical report
TS	technical specification
URL	uniform request locator
WIP	work in progress
WLAN	wireless local area network

4 Power systems – specifics and related standardization

4.1 Overview

Power generation, transmission, and distribution systems are characterized by the existence of two infrastructures in parallel, the electrical grid (1 in Figure 1), carrying the energy and the information infrastructure (2 in Figure 1) used to automate and control the electrical grid. Especially the information infrastructure is becoming more and more a critical part of power system operations as it is responsible not only for retrieving information from field equipment

but most importantly for submitting control commands. A dependable management of these two infrastructures is crucial and strongly relies on the information infrastructure as automation continues to replace manual operations. Hence, the reliability of the power system strongly depends on the reliability of the information infrastructure. Therefore the information infrastructure shall be managed to the level of reliability needed to provide the required stability of the power system infrastructure to prevent any type of outage.

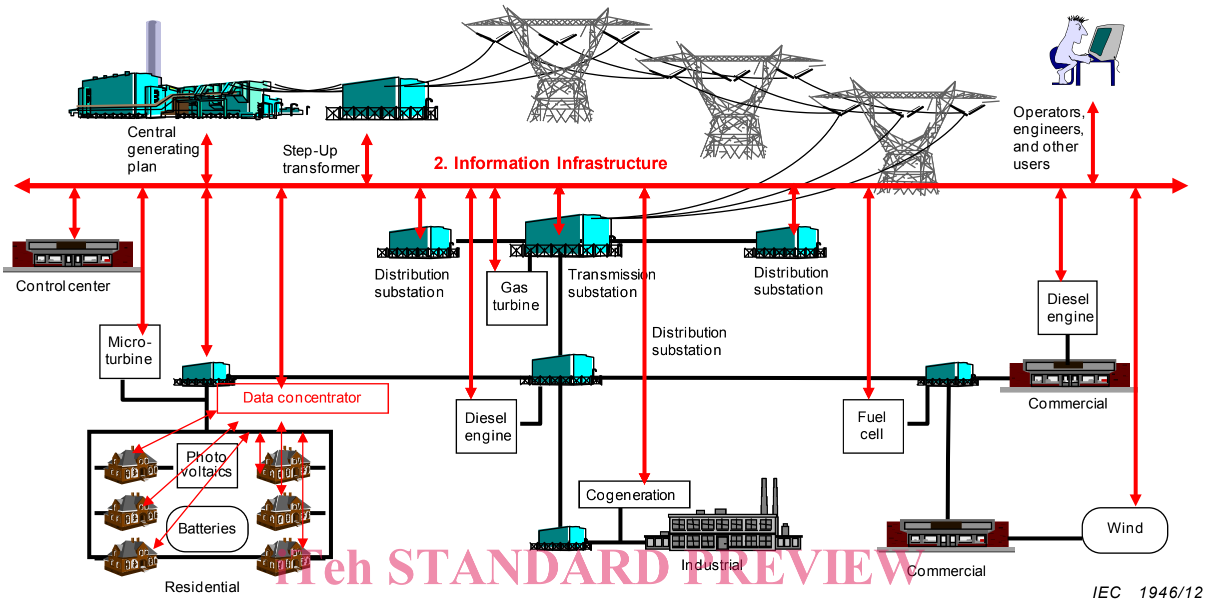

Figure 1 – Power systems – Management of two infrastructures (see Figure 11 of [40])

The present, rather centralized approach for power generation is evolving to a decentralized power generation involving existing power plants, power plants producing renewable energy (like wind parks) down to residences having their own micro power plants (e.g. solar cells). Moreover, electro mobility as potential energy storage will become more important and needs to be integrated into the current power system landscape. This increases the already high complexity of power systems even more. Furthermore, there is also the trend to interconnect the formerly closed and proprietary architectures with office environments and enterprise systems to allow new functionalities and increase cost effectiveness. The reverse side is that this may also lead to new vulnerabilities, which turn cyber security into a priority and a permanent challenge.

As the information infrastructure is the backbone of power system control, it needs appropriate protection to ensure the operation of power systems and support the required system reliability. Information security is the base for protecting the information infrastructure against intentional and unintentional cyber incidents but needs to take the power system specifics into account. These specifics are depicted in 4.2. Security as a major topic has been recognized by standardization bodies as outlined in 4.3, which does not provide a complete list of standards but lists the most important ones for the application domain. 4.4 focuses on the architecture of the IEC TC 57 spanning power systems management and associated information exchange.

4.2 Security specifics

The operational environment of the power systems information infrastructure differs from office environments or telecommunication environments in several aspects. Specific cyber security problems have been identified for instance in the NIST document set NIST IR 7628 (see [17], [18], and [19]). Volume 3 of NIST IR 7628 (see [19]) provides a list of evident and specific cyber security problems. These documents explain the enumerated operational, system, and device issues more specifically. Technical issues related to the definition of appropriate security measures have also been discussed as part of IEC/TS 62351-5 (see [43]).

The following list provides some examples for specifics in power systems out of the referenced documents and also provides additional examples (not a complete list):

– computer-constrained resources precluding many IT technologies;
– communication between components is often asymmetric and message oriented (like multicast);
– strict timing requirements (down to milliseconds);
– long lifetime or operation time of components (in the range of 10 to 30 years);
– based on the long operation time of the components, there are strong requirements for interoperability with legacy systems and for migration concepts;
– interoperability with legacy systems influences the maintainability of power systems and makes systems more complex, especially if maintenance and operation security is desired;
– limitations of connectivity of systems or system components to a central (control) network;
– higher availability and less latency requirements leading e.g. to missing or limited patch windows within customer facilities complicate the security patch process. Often customers do not or only reluctantly accept updates in their environment;
– interconnection of independent entities (producers / generators, other transport / distribution network operators and services);
– field devices may be installed in physically unprotected areas. Direct access to components by maintenance personnel is costly and often impractical as devices may be installed in widely distributed areas.

Figure 2 summarizes the differences for basic security services and practices between office networks and power system networks. The classifications low, medium, and high are comparable with the NISIR 7628 volume 1 (see [17]) impact levels.

	Energy Control Systems	Office IT
Anti-virus / mobile code	Uncommon / hard to deploy	Common / widely used
Component Lifetime	10-30 years	3-5 years
Outsourcing	Rarely used	Common
Application of patches	Use case specific	Regular / scheduled
Real time requirement	Critical due to safety	Delays accepted
Security testing / audit	Rarely (operational networks)	Scheduled and mandated
Physical Security	Very much varying	High
Security Awareness	Increasing	High
Confidentiality (Data)	Low – Medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x …	Medium, delays accepted
Non-Repudiation	High	Medium

IEC 1947/12

Figure 2 – Comparison office / power system security requirements

As seen, security objectives in power systems are focused on authentication and integrity protection rather than on confidentiality (which is typically the main objective in office and telecommunication environments). This is especially true for energy automation control and protection communication. Nevertheless, with the increased introduction of the advanced metering infrastructure (AMI) and the increasing demand for energy automation down to residential level, confidentiality is required to protect the user's privacy.

While the influences of the information infrastructure to the electrical infrastructure are obvious, there is also a feedback of the electrical infrastructure to the information

infrastructure. Information about states and events or engineering data in the electrical infrastructure can be used to derive relevant input for security controls in the information infrastructure. One example is the utilization of field device configuration data for the compilation of rules for intrusion detection/prevention systems (IDS/IPS) or firewall systems.

4.3 Relevant regulation and standardization activities

In this subclause 4.3 an overview of important domain specific regulation and standardization activities relating to security in Smart Grid systems is provided. This list is not complete and merely states the main standards considered in this report. For a survey on proposed standardization activities related to Smart Grid in general the IEC and NIST activities defining standardization roadmaps are referred to (the respective documents are referenced in the following list).

ISO/IEC

– ISO/IEC 27001 (see [5]), *Information technology – Security techniques – Information security management systems – Requirements*, specifies a set of information security management requirements designed to be used for certification purposes.

– ISO/IEC 27002 (see [6]), *Information technology – Security techniques – Code of practice for information security management*, establishes guidelines und general principles for initiating, implementing, maintaining, and improving information security management in an organization.

– IEC 62351 (all parts, see [25]) is being standardized by the IEC TC 57 WG 15 and defines data and communications security for power systems management and associated information exchange. It comprises security definitions for communication protocols, network and system management as well as role-based access control. IEC 62351 is extensible, thus allowing further parts to be added if necessary. The newest part will target the management of security credentials.

Table 1 provides an overview of the different parts and their standardization status regarding Edition 1. There is currently work going on to provide an Edition 2 of selected parts to address comments received from public reviews such as from the Federal Energy Regulatory Commission (FERC) or the Smart Grid Information Security Working Group (SGIS) as well as recent advances in cryptography.

Table 1 – IEC 62351 parts

IEC 62351	Definition of security services for	Standardization status
Part 1	Introduction and overview	TS
Part 2	Glossary of terms	TS
Part 3	Profiles including TCP/IP	TS, edition 2 is currently under review targeting an IS
Part 4	Profiles including MMS	TS
Part 5	Security for IEC 60870-5 and derivatives	TS, work on edition 2 is almost finished
Part 6	Security for IEC 61850 profiles	TS, will be updated in edition 2 to align with IEC TR 61850-90-5
Part 7	Network and system management (NSM) data object models	TS
Part 8	Role-based access control for power systems management	TS
Part 9	Key management	WIP
Part 10	Security architecture guidelines	TR (this document)
Part 11	Security for XML Files	NWIP

An overview of the different parts of IEC 62351 is provided either in IEC/TS 62351-1 (see [40]) or in a TC 57 WG 15 White Paper (see [37]). These documents also provide an overview of security services necessary to protect against certain threats from a more

general point of view and their mapping to the power domain by using IEC 62351 defined security technology.

– IEC 62443 (see [26]) is being standardized by IEC TC 65 and will reflect the publications of ISA 99, i.e. ISA 99 documents will be submitted to the IEC voting process. Hence, parts of IEC 62443 are likely to be similar, if not identical, to ISA 99. The IEC version is currently likely to contain one more standard (IEC 62443-2-4) which is not developed by ISA.

– The IEC Smart Grid strategic group (SG3) has issued the *Smart Grid standardization roadmap report* (SMB/4175/R see [22]) which encompasses requirements, status and recommendations of standards relevant for the Smart Grid. Security is covered in detail in a separate section of [22]. An overall security architecture capturing the complexity of the Smart Grid is requested. Besides this, the following recommendations pertaining to open items and necessary enhancements are listed:

  - a specification of a dedicated set of security controls (e.g. perimeter security and access control);
  - a defined compartmentalization of Smart Grid applications (domains) based on clear network segmentation and functional zones;
  - a specification comprising identity establishment (based on trust levels) and identity management;
  - necessity to consider security of the legacy components within standardization;
  - the harmonization with IEC 62443 [26] to achieve common industrial security standards;
  - a recommendation to review, adapt and enhance existing standards in order to support general and ubiquitous security across wired and wireless connections.

– ISO/IEC 15408 (see [23]) describes common criteria to specify functional security requirements as well as assurance requirements for components, devices, or systems. ISO/IEC 15408 is being mentioned here, as there are currently attempts to provide protection profiles and associated technical guidelines for smart meter gateways in certain countries (Germany).

IEEE (Institute of Electrical and Electronics Engineers)

– IEEE 1686-2007 (see [30]) is the *Standard for substation intelligent electronic devices (IEDs) cyber security capabilities*. The standard defines functions and features that shall be provided in substation intelligent electronic devices to accommodate critical infrastructure protection programs. It addresses security in terms of access, operation, configuration, firmware revision, and data retrieval from IEDs. Encryption for the secure transmission of data, both within and external to the substation is not part of this standard.

– IEEE P2030 (see [31]) provides a *Guide for Smart Grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads*. The document is intended to provide guidelines for power system architectures, communication and information technology architectures related to Smart Grid targeting the interoperability of involved components.

ISA (International Society of Automation)

– ISA-99 (see [32]) defines a framework addressing *Security for industrial automation and control systems*. It covers the processes for establishing an industrial automation and control systems security program based on risk analysis, establishing awareness and counter measures, and monitoring cyber security management systems. It describes several categories of security technologies and also the types of products available in those categories along with preliminary recommendations and guidance for using those security technologies. The standard consists of several sub-parts, which are in different state of completion.

CIGRE (International Council on Large Electric Systems)

– The guideline *Security for information systems and intranets in electric power systems* presents the work of Joint Working Group D2/B3/C2-01 and focuses on the importance of

handling information security within an electric utility, dealing with various threats and vulnerabilities, the evolution of power utility information systems from isolated to fully integrated systems, the concept of using security domains for dealing with information security within an electric utility, and the use of ISO/IEC 17799 [39]).

– WG D2.22 “Treatment of information security for electric power utilities”: Three reports *Risk assessment of information and communication systems* (see [34]), *Security frameworks for electric power utilities* (see [35]), and *Security technologies guideline* (see [36]) provide practical guidelines and experiences for determining security risks in power systems and the development of frameworks including control system security domains. This is done by elaborating the specific security requirements of these types of domains, and also by giving a view of interrelated domains and high-level frameworks that are necessary to manage corporate risks. Domain-specific cyber security controls are being defined and guidance is provided on how these controls can be applied to electric utility networks.

– WG D2.31 “Security architecture principles for digital systems in electric power utilities (EPUs)”: The new working group advances the results of D2.22 by identifying and developing security architecture principles for digital systems in EPUs. Topics to be addressed are defence in depth and graded approaches (zoning principles) in EPUs, Smart Grid relevant security architecture principles, developments of security architecture for digital systems addressing newly discovered threat scenarios as well as business demands and the support of technical control structures of the IT security architecture.

– JWG B5/D2.46 “Application and management of cyber security measures for Protection and Control systems” aims at identifying threats to protection and control systems to map them with existing to evaluate their effectiveness in providing a defence against the identified threats. Also targeted are practical organizational and technical guidelines for implementing cyber security in protection and control systems that minimizes these differences.

NERC (North American Electric Reliability Corporation)

– NERC’s mission is to ensure the reliability of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards and monitors users, owners, and operators for preparedness. NERC is a self-regulatory organization, subject to oversight by the US Federal Energy Regulatory Commission and governmental authorities in Canada. NERC has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP–002 through CIP–011 which are defined to provide a foundation of sound security practices across the bulk power system. These standards are not designed to protect the system from specific and imminent threats. They apply to operators of Bulk Electric Systems (see also [13]). The profiles originate in 2006. NERC-CIP provides a consistent framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional as well as non-functional requirements. Clause A.1 provides an overview of the different parts of NERC-CIP.

– The draft standard CIP-011 may not lead to new cyber security requirements, but it provides a new organization of the existing requirements in the current CIP standards and eliminates the non-routable protocol exception. The classification of Bulk Electric Systems (BES) into the three categories low, medium, and high impact BES cyber systems, and the mapping of these to security controls are new.

IETF (Internet Engineering Task Force)

– The IETF published RFC 6272, *Internet protocols for the Smart Grid* (see [38]), which contains an overview of security considerations and a fairly thorough list of potentially applicable security technology defined by the IETF. Several IETF standards are applicable in Smart Grid environments. These are enumerated in 5.4.4.

National activities

– The National Institute of Standards and Technology (NIST) is a US federal technology institute that develops and promotes measurement, standards, and technology. In 2009, NIST formed the Smart Grid interoperability panel (SGIP) as a public-private cooperation with over 600 members that develops frameworks and roadmaps, not standards. SGIP’s