A Review of Standards with Cybersecurity Requirements for Smart Grid

Rafał Leszczyna

PII: S0167-4048(18)30280-3
DOI: 10.1016/j.cose.2018.03.011
Reference: COSE 1317

To appear in: *Computers & Security*

Received date: 26 September 2017
Revised date: 20 December 2017
Accepted date: 27 March 2018

Please cite this article as: Rafał Leszczyna, A Review of Standards with Cybersecurity Requirements for Smart Grid, *Computers & Security* (2018), doi: 10.1016/j.cose.2018.03.011

Highlights

- Completely new (2017), updated review of standards related to cybersecurity requirements for smart grids
- The most recent versions of standards analysed
- High assurance of completeness due to the application of a repeatable and systematic literature search and analysis method
- The details of the research method provided
- Explicitly defined standards selection and evaluation criteria
- 17 standards described from cyber security requirements perspective
- The relationships between cybersecurity requirements analysed
- All the standards referenced to the IEC smart grid architecture

A Review of Standards with Cybersecurity Requirements for Smart Grid

Rafał Leszczyna*

Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland
e-mail: rle@zie.pg.gda.pl

Abstract

Assuring cybersecurity of the smart grid is indispensable for the reliable operation of this new form of the electricity network. Experts agree that standardised solutions and practices should be applied in the first place. In recent years many new standards for smart grids have been published, which paradoxically results in the difficulty of finding a relevant publication in this plethora of literature. This paper presents results of a study which aimed at addressing this issue by identifying all standards that define cybersecurity requirements applicable to smart grids. Based on a systematic literature review seventeen relevant standards were identified that are described in this paper with a focus on the requirements and characterised with respect to evaluation criteria. The relationships between the standards have been analysed to understand where the standards overlap or complement each other and where they are completely independent – as far as cybersecurity requirements are concerned. This together with the requirements-focused descriptions of the standards can serve as a useful guidance on cybersecurity requirements for smart grid components that should help practitioners in choosing the standards that are applicable to their area or a specific problem.

Keywords: cybersecurity, information security, smart grid, standards, security requirements, cyber-physical systems, industrial control systems, SCADA

1. Introduction

In traditional enterprises violation of cybersecurity in the majority of cases results in financial losses, while other, more serious consequences are rather seldom. Unfortunately, smart grids highly differ at that point. The effects of targeting them cyberattacks can be very detrimental, having an impact on the health, safety or economic situation of citizens or proper functioning of governments [61]. Securing the smart grid requires novel, multidisciplinary approaches that combine various technologies and incorporates managerial, policy, legal aspects and more [79, 61]. Security experts agree that standardised solutions and practices should be used in the first place [73, 74]. In recent years numerous smart grid standards have been published. This results in the situation that operators may find it difficult to orientate themselves in this plethora of literature. For instance, it is possible that they would miss a standard (or standards) which more than others respond to their specific problem.

To address this challenge and to ensure that experts consider all applicable standards, a research was conducted that aimed at identifying all standards which define cybersecurity requirements that can be applied to the smart grid. Cybersecurity requirements depict characteristics, features or functions that need to be present in a system to assure its cybersecurity. Identification of the requirements is one of the first steps in a system safeguarding process [42]. Properly recognised and defined requirements are key factors that determine if the achieved security is true or only illusory. This paper brings in all the identified standards that describe cybersecurity requirements applicable to smart grids (based on a structured study). The standards are characterised in regard to the requirements and criteria-based indications are provided that aim at helping the operators to choose the standards which are applicable to their area and that address their individual goals. This is in order to altogether constitute a comprehensive guideline on standardised cybersecurity requirements for smart grids. Following a systematic literature review that comprised three main stages (see Section 3), 17 cybersecurity publications of relevance have been identified, which are presented in this paper. To the best of author's knowledge a study that addresses this subject has not been performed so far. Some of the publications are not standards in the strict meaning of this word. They are originally labelled by their authors as guidelines, technical reports, special publications or regulations. However since the studies treat these publications as standards, they are included in the evaluation. In fact the majority of these documents have become *de facto* standards[1].

The paper is organised as follows. Section 2 introduces the concept of the smart grid and other fundamental concepts that are used in the paper. The method of the research and standards' selection and evaluation criteria are described in Sections 3 and 4. The key part of the paper (see Section 5) is dedicated to the demonstration of standards that specify cybersecurity re-

*Corresponding author

[1] De-facto standard – a custom, convention, company product, corporate standard, etc. that becomes generally accepted and dominant and is widely used and applied.

quirements applicable to the smart grid. There the standards are shortly characterised focusing on the requirements, also the relationships between the requirements are investigated. Finally, after the presentation of related work in Section 6, the paper concludes with closing remarks.

2. Smart grid

According to the European Commission the *smart grid* is "an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added" [13]. The European Smart Grid Task Force understands smart grids as "electricity networks that can efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety" [13]. The American Department of Energy (DoE) defines the smart grid as a "class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumers of electricity in homes and businesses. They offer many benefits to utilities and consumers – mostly seen in big improvements in energy efficiency on the electricity grid and in the energy users' homes and offices."

The traditional grid is centralised and relies on electromechanical components. Monitoring of the infrastructure and failure recoveries are done manually, which introduces many limitations. In the smart grid, on the contrary, electric energy comes from various distributed sources, connected to electricity network and communication infrastructure. To improve smart grid operation, various digital devices and sensors are applied. In effect, the smart grid presents self-monitoring and self-recovery capabilities and exposes high-level of adaptiveness [24]. Advantages of the smart grid include [56]:

- improved quality and reliability of power delivery,
- facilitated deployment of distributed energy sources and renewable sources,
- enhanced resilience to disruption and ability of self-recovery,
- more predictive maintenance,
- automated operation and maintenance,
- wider consumer choice.

However the smart grid introduces also new challenges, including security and privacy concerns resulting from the high dependence on Information and Communication Technologies (ICT) and the interconnection with the Internet [48]. Each network connection, network layer and applied technology becomes a potential target for an attacker as one of the initial steps in gaining access to other components of the system. The new form of electricity network is exposed to a very large number cyber-threats which, to make the situation even worse, evolve dynamically. Advanced Persistent Threats (APT), including the famous Stuxnet [22] and its successors (Duqu, Red October and others), botnets, zero-days or Distributed Denial of Service Attacks (DDoS) – are threats which emerged or impressively evolved in only five recent years. The new variant of Black Energy, called Disakil is suspected to be the cause of the Ukrainian power outages in December, 2015 [72]. Apart from that, there are completely new risks inherently introduced by new functions of the modern electric infrastructure. These, for example, include attacks on smart metering systems. Smart meters constitute a critical system component, because they are connected to other home devices such as smart appliances and charging stations, and compromising them opens a way for reaching these devices. Additionally to that, the location of some smart grid components at end-users' facilities or in public places renders them practically all-time, fully accessible to potential intruders [5, 26]. Effective and reliable protection of smart grids is one of the key enablers of their adoption.

Cyber-Physical Systems (CPS) [51], to which belong smart grids, differ in many respects from regular ICT systems. Prepared to satisfy strict performance and reliability requirements, usually they operate in real-time, where delays are highly undesirable. Also outages are not acceptable in the majority of cases and therefore fault-tolerance techniques are applied such as components redundancy. Additionally, interruptions in the operation of CPS have immediate and magnified effects on the continuity of production. Thus common ICT routines such as rebooting can not be applied. A large number of CPS control and monitor critical processes (e.g. nuclear power generation or gas production), where the associated risks are much higher than in the case of ICT. In result, security priorities and risk management objectives for the two types of systems are distinct [70].

3. Research method

Based on a systematic review of the existing literature, the research described in this paper aimed at identification of standards that define cybersecurity requirements for smart grids. The literature survey was based on the approach of Webster and Watson [77]. According to the approach, the literature search should commence with exploring the most established literature sources, article databases and proceedings. Then the *backward analysis* is performed, in which citations in the identified documents are reviewed in order to determine earlier documents of relevance. This is followed by the *forward analysis* where articles that cite the key documents recognised in the previous steps are searched for using a scientific database (the authors recommend Web of Science). The Webster and Watson approach is concept-centric i.e. concepts determine the organising framework of a review. Accordingly, the closing phase of the literature review is demarcated when new concepts are not found in the identified set of documents [77]. In the study described

in this paper an analogous systematic search process was imposed to identify standards, scientific papers and books, as well as technical reports that describe cybersecurity standards for smart grids. The strict discipline of the process aimed at assuring its repetitiveness and comprehensiveness, as well as providing the high level of certainty that all standards relevant to the subject would be identified (completeness). The research was composed of three main parts, namely the literature search, the literature analysis and the standards' selection.

Literature search. Databases of widely recognised publishers that address the topics of information security, energy systems, computer science and similar, namely the Association for Computing Machinery (ACM), Elsevier, IEEE, Springer and Wiley, were searched for keywords: "smart grid", "security" and "standard". Then it was followed by the search in aggregative databases that store records of various publishers – EBSCOhost, Scopus and Web of Science. In the first step, an electronic search was performed of the keywords in any descriptive metadata of publications. This led to the identification of as much as 34,388 records. Such abundant number of publications resulted from the mode of operation of search engines. Some of them looked independently for each of the keywords, other for all of them at once. Thus the search needed a refinement by looking solely at titles, keywords and abstracts, respectively. The descriptive data of the resulting around 700 records were then analysed manually to elicit 79 publications that seemed relevant to the research. An in-depth review of these publications led to the identification of 58 papers which to various extent addressed the subject of smart grid security standards (Table 1). The majority of them just mentioned selected standardisation initiatives or some standards, but 8 [64, 28, 63, 44, 27, 21, 76, 75] presented more comprehensive studies.

Literature analysis. The publications identified during the in-depth review were read completely or their relevant parts in order to recognise smart grid security standards and initiatives. This part also included the analysis of cited references. In result some additional reports of relevance (e.g. [16, 78, 10, 68] were found. The following initiatives related to smart grid standardisation were identified [27, 29, 43, 10]:

- CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) [11, 27],
- European Commission Smart Grid Mandate Standardization M/490 [20, 29],
- German Standardization Roadmap E-Energy / Smart Grid [16],
- IEC Strategic Group 3 Smart Grid [12, 33, 34, 68, 29],
- IEEE 2030 [37, 28, 23, 29],
- ITU-T Smart Grid Focus Group,
- Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for Smart Grid [10],
- OpenSG SG Security Working Group [59, 23],
- Smart Grid Interoperability Panel [57, 27, 29],
- The State Grid Corporation of China (SGCC) Framework [69, 29].

These activities were primarily dedicated to the development of new standards and guidelines, but also indicated already existent standards relevant to the subject. Among them, the work of IEC needs to be noted, as it plays a particular role in this paper. IEC prepared and maintains a very useful website with the Smart Grid Standards Map [34] – an interactive graphical tool that facilitates identification of relationships between standards and smart grid components (see Figure 1). It also visualises all smart grid components that are addressed by a selected standard. At the moment, as much as 512 standards are registered to the website and "new standards are added regularly". The map allowed for indicating to which smart grid components are relevant the standards described in this paper. This is illustrated by the *applicability* criterion described in Section 4. It needs to be noted, that the map, while useful for indicating the smart grid components, is limited in regard to cybersecurity standards. When choosing "security" component (in the "Mapping View"), 8 standards and standards' series are enlisted: IEC 61400-25, IEC 61850-90-5, IEC 62056-5-3, IEC 62351 series, IEC 62443 series, ISO/IEC 15118, ISO/IEC 27001 and ISO/IEC 27002. This is just a subset of available standards and standards' series relevant to cybersecurity identified in the study described in this paper. In this respect this paper aims at constituting a comprehensive source of information on smart grid standards with cybersecurity requirements. Moreover as the IEC database doesn't contain NIST, NERC, DHS and other US publications described in this paper, they were referenced to the map by the author.

To avoid any duplication of work, the initiatives and the 8 scientific studies mentioned earlier were analysed in the first order in the search for standards related to smart grid cybersecurity. Additionally, the literature search phase was extended to identify other (possibly all) smart grid cybersecurity standards' identification initiatives which revealed ongoing or concluded projects that are completely or partially dedicated to smart grid standards' stocktaking [3, 4]. It became evident that these undertakings address the subject from various perspectives and provide different sets of standards.

Standards selection. The selection criteria described in Section 4 were applied to the identified standards. As a result 44 standards (e.g. ISO/IEC 27001, ISO/IEC 27002, NERC CIP 002, NERC CIP 003) or *standards' series* (e.g. ISO/IEC 27000 series, NERC CIP) related to smart grid cybersecurity were depicted. These standards were analysed in search for definitions of cybersecurity requirements.

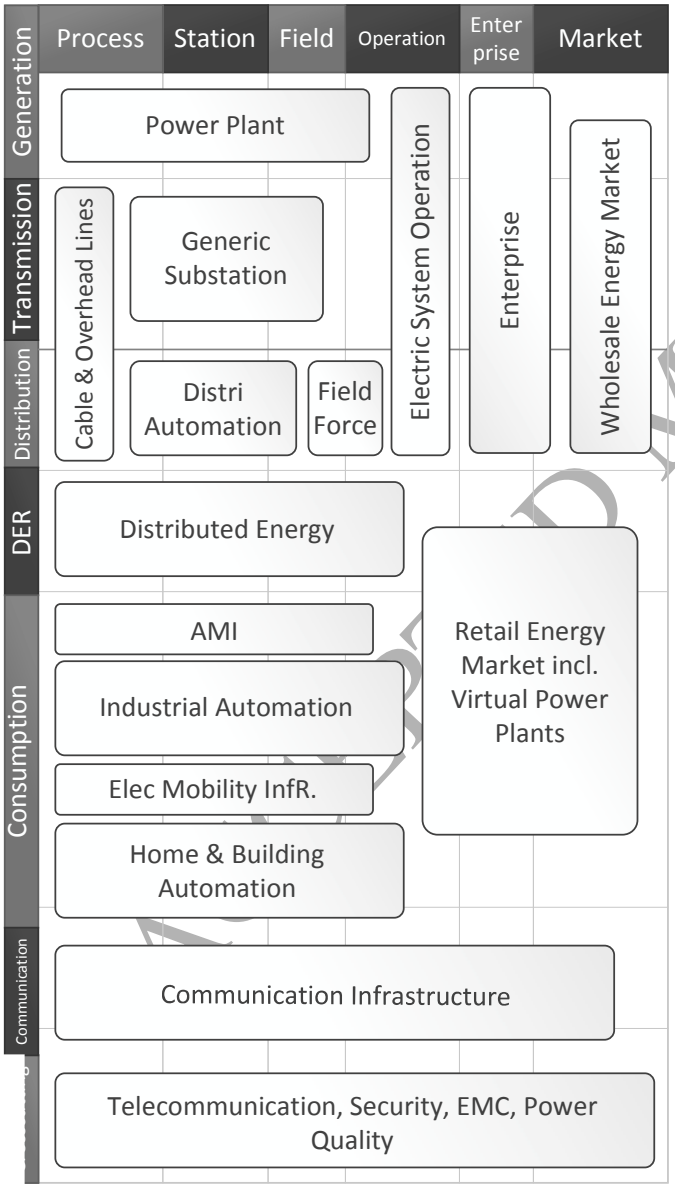
[0] Search results repeated findings from searches in other databases.

[1] In the Web of Science database the first search was in the Topic field due absence of all metadata search

Table 1: Literature search summary.

Source	All metadata	Title	Abstract	Keywords	In-depth review	Relevant
ACM DL	23	0	14	1	6	6
Elsevier SD	5674	0	30	3	9	9
IEEE Xplore	509	3	152	16	27	22
Springer	19 619	234	n.a.	n.a.	14	4
Wiley	2677	0	9	3	7	3
EBSCOhost	258	4	129	7	16	15
Scopus	5361	5	288	145	11	5
WoS	267[1]	3	n.a.	n.a.	16[2]	0
Total	34 388	249	622	175	79	58

[1] The search was in the Topic field due to the absence of all metadata search.
[2] Search results repeated findings from searches in other databases.



gure 1: Smart grid components based on the IEC Smart Grid Standards Map 4].

4. Standards' selection and evaluation criteria

A literature search analogous to the one described in the previous section was dedicated to the identification of attributes that facilitate characterisation and comparison of standards. In result 17 publications related to evaluation of standards [64, 80, 50, 25, 18, 8, 71, 60, 67, 46, 66, 45, 6, 30, 62, 47, 17] were identified. In principle the documents discuss information security (12) or smart grid (2) standards. Three of them are dedicated to other normative documents (green building, IT interoperability, Machine to Machine and the Internet of Things).

Sunyaev [71] describes complete literature analysis approach and defines as much as 40 standards' evaluation criteria, which include e.g. availability, skills needed, scalability, maturity level, compliance etc. The criteria are grouped into three classification areas: general information system (IS) security approach characteristics, general IS security approach characteristics related to healthcare and healthcare specific IS security approach characteristics. Sommestad et al. [67] present a quantitative standards' evaluation method that comprises three phases: selection; grouping of recommendations and threats; quantifying focus of standards. Standard selection criteria are defined which include availability in English, focus on Industrial Automation and Control Systems' (IACS) security or type of publishing organisation. The comparison of standards is quantitative, based on counting the occurrences of particular keywords in the compared texts. Beckers et al. [8] developed a structured, conceptual model for analysis of standards and a template that facilitates its application. A common terminology is defined. The paper comprises a good discussion of other standards' surveys. Siponen and Wilson [66] also distinguish between selection and assessment criteria. The former include recent release and wide acceptance of scholars and practitioners. The latter: the scope of application and the type of evidence.

Several papers define qualitative criteria. Arora [6] evaluates standards according to their focus, scope, structure, organisational model etc. Phillips et al. [62] compare technical features (including band, range and data) and security features (confidentiality, integrity, availability). ENISA's evaluation of Privacy Enhancing Technologies [18] distinguishes between maturity and stability, privacy policy implementation and

Table 2: Standards' evaluation criteria.

Criterion	Description
Scope	Indicates to which particular subject the standard is dedicated.
Type	Depicts whether the standard presents technical solutions or more general, high-level guidance.
Applicability	Indicates to which smart grid components the standard can be applied.
Range	Geographical coverage of the standard, whether it is national or international.
Publication	Date of publication of the standard.

usability. Zhang et. al [80] – objective and measures (idea analysis), Gazis [25] – maturity, layers, arrangement, domain, definitions, audience, etc. Eastaughffe et al. [17] focus on the domain-specific features such as safety management agents, integrity levels, human factors, assurance techniques or post-development issues. Kuligowski [46] compares standards' terminology, maps controls and documents, and defines qualitative/quantitative criteria that include the effectiveness of security standards, number of certifications, number of privacy data breaches, target organisations etc. Another approach is presented in NIST SP 800-29 [47] where the content of documents is compared, section by section. Similarly in the works of Kosanke [45] and Metheny [49] domain-specific comparison criteria are presented. While Ruland et al. [64] and Idaho National Laboratory [30] just overviews surveyed standards.

Summarising, the publications present standards' evaluation approaches or criteria for various domains, but none of them provides smart grid-specific criteria. Sunyaev [71] in his study dedicated to the healthcare sector depicts an impressive number of 40 security assessment-related criteria. Based on the analysis, the following, not exclusive *selection criteria* were chosen. A standard to be selected for a content based evaluation (see the previous Section) needed to be: (a) published in English, (b) referenced in smart grid standard identification studies or papers, (c) published by a standardisation body or governmental institution, (d) related to security requirements or cybersecurity. The *evaluation criteria* which serve in comparing the selected standards are presented in Table 2.

5. Results of the analysis

The following sections provide a characterisation of the standards in relation to security requirements they define. The summary of the analysis is presented in Table 5 and 6.

1. NISTIR 7268

NISTIR 7628 Guidelines for Smart Grid Cyber Security is three-volume report which defines a comprehensive framework for smart grid stakeholders that can be used for developing and cybersecurity strategies for their organisations [58]. The report was developed by the Smart Grid Interoperability Panel-Cyber Security Working Group (SGIP-CSWG), formerly the Cyber Security Coordination Task Group (CSCTG). In 2012, the organisation comprised over 780 participating institutions from 22 stakeholder groups, including private sector (utilities, vendors, and service providers), academia, regulatory organisations, state and local government, and U.S. federal agencies [52].

Chapter three of the report describes more than 180 high-level security requirements structured into 19 thematic groups, or families, with similar objectives (see Table 3). The analyses which led to the selection of these security requirements, including the risk assessment process, are described in Chapter 3 and extended in Appendix G of the report. The requirements were selected from a large set, where the three main sources were the standards described in this paper: NIST SP 800-53, NERC CIP and DHS Catalog. A mapping between requirements in NISTIR 7628 and these three standards is presented in Appendix A of NISTIR 7628 [58].

After being selected, the requirements were modified to respond to the characteristics of the electric sector and the smart grid. The security requirements are assigned to the three categories [58]:

- compliance, risk, and governance – to be addressed at the organisation level,
- common technical – to be applied to all logical interface categories,
- or unique technical – applicable to one or more logical interface categories.

5.2. NERC CIP

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards are US standards mandatory for the North American Bulk Electric System. They address the security of cyberassets indispensable for the reliable operation of the electric grid. The set of standards consists of 11 publications which require that [54]:

- Cybersystems and assets critical for the reliable operation of the electric system are identified and documented based on thorough risk assessment.
- Minimum security management controls are deployed.
- Personnel with authorised access to critical cyberassets underwent personnel risk assessments and proper training and present a sufficient level of security awareness.
- Electronic security perimeters and their access points are identified and secured.
- Methods, processes, and procedures for securing cyberassets within the electronic security perimeters are defined.
- Physical security program for the protection of the critical cyberassets is devised and implemented.
- Cybersecurity incidents are detected, categorised, addressed and reported.

Table 3: NISTIR 7628 requirements families. Source [58].

SG.AC	Access Control	SG.AT	Awareness and Training
SG.AU	Audit and Accountability	SG.CA	Security Assessment and Authorization
SG.CM	Configuration Management	SG.CP	Continuity of Operations
SG.IA	Identification and Authentication	SG.ID	Information and Document Management
SG.IR	Incident Response	SG.MA	Smart Grid Information System Development and Maintenance
SG.MP	Media Protection	SG.PE	Physical and Environmental Security
SG.PL	Planning	SG.PM	Security Program Management
SG.PS	Personnel Security	SG.RA	Risk Management and Assessment
SG.SA	Smart Grid Information System and Services Acquisition	SG.SC	Smart Grid Information System and Communication Protection
SG.SI	Smart Grid Information System and Information Integrity		

- Recovery plans for critical cyberassets are defined and implemented.
- Baseline configurations are defined and documented, configuration changes are documented and properly managed.
- Vulnerability assessments are conducted periodically.

5.3. IEC 62443

IEC 62443-2-1:2010 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program [31] describes the elements and the development process of a cybersecurity management system (CSMS) for control systems and automation technology. Because IEC 62443-2-1 is based on ISO/IEC 27001, the requirements specified there are similar to the requirements in ISO/IEC 27001. However, an alternative organisation of the requirements is introduced to increase the readability of the standard by combining similar requirements into larger subclauses and by providing considerable informative guidance in Annex A. There the similarities between the requirements in the two standards are explained and the requirements mappings are presented [31].

IEC 62443-3-3:2013 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels defines detailed technical control system requirements associated with the seven foundational requirements described in IEC 62443-1-1 [32]:

- Identification and authentication control (IAC),
- Use control (UC),
- System integrity (SI),
- Data confidentiality (DC),
- Restricted data flow (RDF),
- Timely response to events (TRE),
- Resource availability (RA).

The definitions include the requirements for capability security levels of a control system [32]. For each system requirement a baseline requirement is provided that comprises rationale for its implementation as well as supplementary guidance. Many requirements are extended with one or more enhancements that enable achieving higher security levels [32]. Four security levels are defined for functional requirements. The control system capability level 0 for a specific functional requirement is equal to no requirements. The remaining security levels are defined as follows [32]:

- SL 1 – protecting from eavesdropping and an accidental disclosure of information,
- SL 2 – preventing an unauthorised disclosure of information to an attacker actively searching for it using simple methods with low resources, generic skills and low motivation,
- SL 3 – protecting from an unauthorised disclosure of information to an attacker actively searching for it using complex methods with moderate resources, automation technology and control systems specific skills and moderate motivation,
- SL 4 – preventing an unauthorised disclosure of information to an attacker actively searching for it using complex methods with extended resources, automation technology and control systems specific skills and high motivation.

5.4. IEEE C37.240

IEEE C37.240 Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems [36] presents baseline cybersecurity requirements dedicated to electric substations' communication systems (automation, protection and control). The requirements are moderately technical (present technical solutions but without detailed specifications). They fall into the following categories:

- High level requirements and priorities for interface categories – in form of a mapping of a hypothetical substation cybersecurity program with the NISTIR 7628 requirements.

- Requirements for communication components (substation network devices, switches, routers, serial-device servers, firewalls, VPN's and key management).
- Functional requirements that regard access to IEDs, communication paths, dial-up and dedicated-line connections.
- User authentication and authorisation – assuring only authorised access to system components using authentication and authorisation techniques, blocking unauthorised login attempts, communication sessions, authorisation logging, password management and Role-Based Access Control.
- Data-in-motion protection – encrypting all data that are transferred between cybersecurity zones.
- Configuration management – central management of software and device configurations, quality assurance, configuration authentication.
- Security event auditing and analysis/incident response – assessments of security incidents that reflect attack source, nature and reasons, as well as time and location of the incident.
- Security testing – periodic reviews of cybersecurity policy and procedures, penetration testing, physical security audits, audits of firewall policies and software versions and patches.

5.5. Cyber Security Procurement Language for Control Systems

DHS Cyber Security Procurement Language for Control Systems [14] defines procurement security requirements for Industrial Control and Automation Systems (IACS). The requirements are grouped into high-level topics, each addressing a particular control system security area of concern [14]:

- System hardening: removal of dispensable software, host intrusion detection systems, file and system access permissions, hardware configuration, heartbeat signals and software deployment.
- Perimeter protection: firewalls, network intrusion detection systems and honeypots.
- Account management: default, guest, or anonymous accounts management, session management, passwords and authentication, account events' logging (auditing), Role-Based Access Control (RBAC), single sign-in and non-disclosure agreements.
- Coding practices – development of secure, highly reliable software.
- Flaw mitigation – reporting and documenting flaws and tracking corrective actions.
- Detection and protection from malicious software.
- Secure network addressing and name resolution.
- End devices – hardening Intelligent Electronic Devices (IEDs), Remote Termina Units (RTUs), Programmable Logic Controllers (PLCs), sensors, actuators and meters.
- Remote access – secure use and configuration of dial-up and dedicated line modems, Internet protocols, Virtual Private Networks, serial communication.
- Physical security related to cybersecurity components – component's and perimeters' access control, manual override control, intra-perimeter communication.
- Network segregation – secure use and configuration of network devices, correct design of the network architecture.

For each requirement a rationale is described, example specification language as well as factory acceptance test measures and site acceptance test measures are provided for verification if products' security objectives are satisfied at the vendor's and the purchaser's location subsequently.

5.6. Privacy and Security of the Advanced Metering Infrastructure

Dutch guideline *Privacy and Security of the Advanced Metering Infrastructure* [55] presents requirements "to achieve a sufficiently high level of security for the advanced metering infrastructure". The requirements have been elicited in a risk-assessment based process which included stakeholders analysis and definition of security goals. If a requirement was formulated in accordance with ISO 27002, an adequate indication is provided. The requirements are classified into the following groups:

- General measures – security policies, protection of Personally Identifiable Information (PII), assigning security roles and responsibilities, change management, access management, procurement issues, incident management and business continuity, compliance.
- Device-specific requirements and measures (meter and DC) – security characteristics and operation of AMI devices.
- Requirements and measures relating to data communication.
- Requirements and measures specifically for the central system.

The specifications vary between moderately technical and general (organisational).

5.7. AMI System Security Requirements

AMI System Security Requirements [9] provides utility industry and vendors with a broad set of detailed, technical or organisational security requirements for Advanced Metering Infrastructure (AMI) to be used in the procurement process. Numerous (almost 500) requirements are specified grouped in three categories:

- Primary security services (functional requirements) – related to confidentiality and privacy, integrity, availability, identification, authentication, authorisation, non-repudiation and accounting.
- Secondary security services (supportive for functional) – regarding anomaly detection, system separation, cryptography, events' logging (auditing), resource management, trust and certificates.
- Assurance – focused on the development of smart grid solutions, security training, personnel security, strategic planning, monitoring and reviewing security policies, operational activities, accountability and access control.

5.8. DHS Catalog

Catalog of Control Systems Security: Recommendations for Standards Developers published by the U.S. Department of Homeland Security presents good practices collected from various industrial organisations. The recommendations, presented in the form of (250) requirements grouped into 19 categories ('families'), are broad in scope in order to provide a flexibility level that enables developing sound cybersecurity standards specific to individual security needs [15]. This structure follows the organisation of NIST SP 800-53, on which the DHS Catalog is strongly based. The families were realigned to facilitate security management of control system environments. The requirements include contributions from "Key Elements to a Cyber Security Management System" specified in the draft dISA-99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program document [15]. The requirements address the areas presented in Table 4.

5.9. ISO/IEC 27019

ISO/IEC TR 27019:2013 Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry was prepared by DIN Deutsches Institut für Normung e. V. and was adopted under a special "fast-track procedure" by Joint Technical Committee ISO/IEC JTC 1, Information technology, in parallel with its approval by the national bodies of ISO and IEC [41]. It extends the ISO/IEC 27000 standards to the area of control systems and automation technology used in the energy sector, providing the domain-specific interpretation guidance on the ISO/IEC 27002-based information security management that extends from the business to the process control level [41]. An integral part of ISO/IEC TR 27019 is a collection of procurement requirements for manufacturers, system integrators, external and in-house planners, implementers and operators. The standard advises that a security requirements analysis and a supplementary individual risk analysis should be carried out before a procurement of process control devices or software [41].

5.10. ISO/IEC 27001

ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements defines the requirements for complete life-cycle (establishing, implementing, operating, monitoring, reviewing, maintaining and improving) of an Information Security Management System (ISMS) in an organisation. The requirements enable the implementation of security controls tailored to the needs of individual organisations or their divisions. The requirements are generic and intended to be applicable to organisations of any type, size and nature. They refer to the following areas of information security management [40]:

- Analysing and understanding the context of an organisation.
- The top management (CEOs, managers etc) commitment to information security activities and policies.
- Establishing and communicating a security policy.
- Planning of information protection actions and tasks.
- Information security risk assessment and treatment.
- Identifying and assuring required assets and competences.
- Security communication and awareness raising.
- Preparation, sharing and maintaining all relevant documentation,
- Planing, implementing and monitoring operative actions necessary to fulfil security requirements.
- Evaluation of effectiveness and efficiency of security related activities.
- Detection and removal of nonconformities, continuous improvement.

5.11. Other standards with cybersecurity requirements applicable to smart grid

Among standards in the IEC 62351 series, *IEC 62351-3:2014 Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP* defines specific, technical security requirements for TCP/IP-based protocols in Industrial Control and Automation Systems (IACS) that regard use of encryption, certificates or Message Authentication Codes (MACs). The standard is dedicated to developers of protocols or applications that use them.

IEEE Std 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities [35] specifies security requirements (referred to as 'features') for Intelligent Electronic Devices (IEDs) used in the electric sector (note the scope change in comparison to IEEE 1686:2007 which was focused on *substation* IEDs). The requirements are related to access control, events' logging (audit), security monitoring and control, secure configuration changing, accessing communication

Table 4: DHS Catalog requirements areas. Source: [15]

Security Policy	Organizational Security
Personnel Security	Configuration Management
System and Services Acquisition	Risk Management and Assessment
Strategic Planning	System and Communication
Information and Document Management	System Development and Maintenance
Security Awareness and Training	System and Information Integrity
Media Protection	Incident Response
Access Control	Audit and Accountability
Monitoring and Reviewing Control System Security Policy	Physical and Environmental Security
Security Program Management	

ports and firmware quality. For the latter a reference to IEEE Std C37.231 is provided. The descriptions are moderately technical in the sense that they indicate technical controls that should be applied, but without providing implementation details.

Part 2 of *ISO 15118 Road vehicles – Vehicle to grid communication interface* [38] defines network and application protocol security requirements for interfaces between electric vehicles and Electric Vehicle Supply Equipment [38].

GB/T 22239 Information Security Technology – Baseline for Classified Protection of Information System Security [1] is a Chinese general-purpose standard dedicated to information systems of any type, published in June, 2008. It defines security requirements for information systems at five security levels. The requirements are split between technical and managerial. The former regard physical, network, host, application and data security. The latter describes establishing and operating a security management system, personnel security and security during deployment, operation and maintenance of an information system.

GB/T 20279 Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products [2] is a Chinese, national standard which presents technical security requirements for host and network firewalls, data diodes and similar. The requirements are divided between functional, assurance, environmental adaptation and performance. They are intended for use during design, development and tests of separation devices. The organisation of the standard can pose a challenge for its reading and browsing as the numeration level of sections reaches six (e.g. "5.2.3.1.1.2 Control function for basic information flow").

ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules [39] defines technical security requirements for cryptographic modules used in security systems that protect sensitive information in computer and telecommunication systems. The standard is directed to the developers of the modules as well as their operators.

VGB-Standard IT Security for Generating Plants [7] specifies security requirements for power plants. Over 50 general or moderately technical requirements are defined, which fall into five categories: general, organisational, technical, physical security and documentation.

5.12. Relationships between requirements in the standards

The relationships between cybersecurity requirements in the identified standards are presented in Figure 2. The unidirectional solid arrows indicate which standards served as an input during the development of other specifications. For instance the requirements in NISTIR 7628 result from the analysis and adoption of the requirements in NERC CIP, DHS Catalog and NIST SP 800-53. The dashed bidirectional arrows show congruence between standards. NIST SP 800-53 is highly convergent with ISO 27001 (see below), while ISO 27002 is just an informative extension of ISO 27001 that aims at explaining ISO 27001 concepts. In this sense it can be perceived as identical to ISO 27001 as far as the conceptual coverage is concerned. The horizontal lanes depict the scope of the standards in regard to cybersecurity requirements, their level of generality and/or thematic coverage. For instance NERC CIP and ISO 27001, are general scope, high-level standards not particularly focused on smart grids. IEC 62351 or ISO 19790 on the other hand are highly technical, very specialised standards that specify the details of communication protocols or cryptographic primitives.

NIST SP 800-53 which gives foundations for many other standards, including DHS Catalog, NISTIR 7628, or IEEE 1686, is congruous with ISO 27001, starting from Revision 3[2]. This is owing to the effort of NIST, which conducted a so called 'convergence initiative', that provided controls' and risk management concepts' mappings between the standards as well as the integration of ISO/IEC 27001 into NIST's risk management approach (since Revision 4). As a result organisations complying with NIST SP 800-53 will be also satisfying ISO/IEC 27001 requirements, after only some minor adjustments (described in Appendix H of NIST SP 800-53).

NERC CIP and GB/T 22239 present high-level requirements independent of each other and from ISO 27001 and NIST SP 800-53. GB/T 22239 to a high degree covers the security domains of ISO 27001, but does this it from national, Chinese, perspective. In contrast to the ISO standard, it introduces security levels. Differently to other standards on this level (in Figure 2), NERC CIP is orientated towards the protection of the critical infrastructure of the US electric grid.

[2]NIST SP 800-53 Rev. 2 and earlier were consistent with ISO 17799 and other standards.

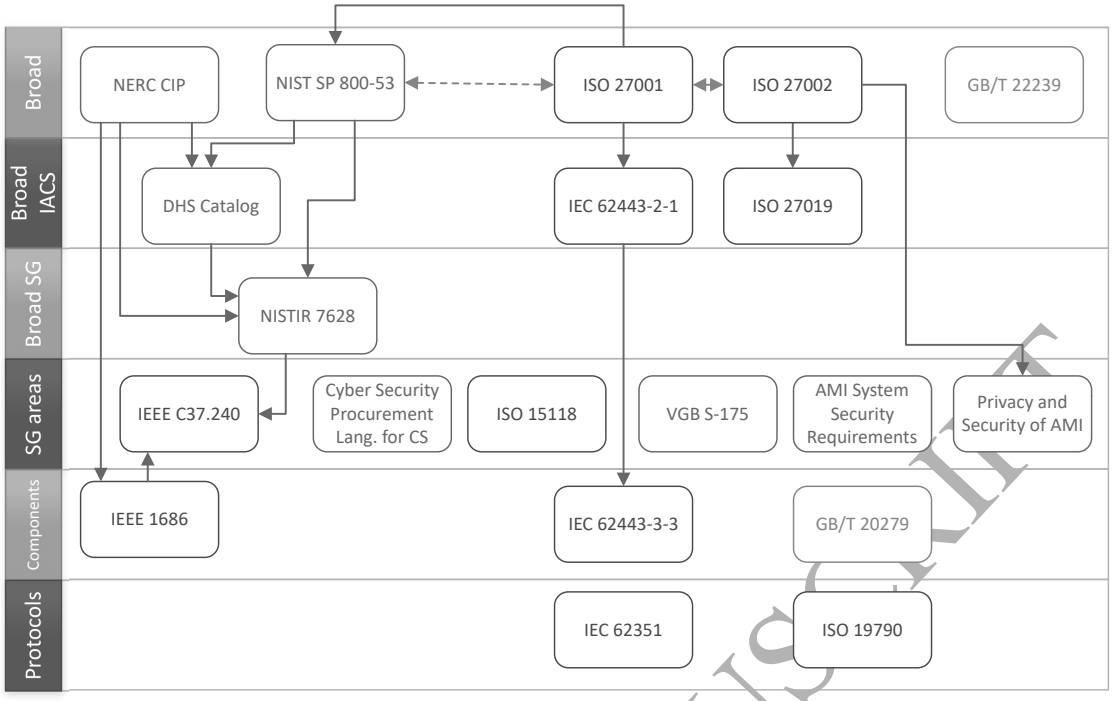


Figure 2: Relationships between requirements in the identified standards. Unidirectional solid arrows indicate which standards served as an input during the development of other specifications. Dashed bidirectional arrows show congruence between standards. Horizontal lanes depict the scope of the standards in regard to cybersecurity requirements, their level of generality and/or thematic coverage.

DHS Catalog, ISO 27019 as well as IEC 62443-2-1 are high-level, non-technical standards, dedicated to the security of IACS. DHS Catalog is based on NIST SP 800-53 Rev. 3 and follows its organisation (19 families of security requirements), but each requirement is adopted to IACS and supplemented with IACS-specific guidance. Appendix A contains a mapping between DHS Catalog and other 15 standards, including NIST SP 800-53, NERC CIP, ISO 27001, AGA and ISA. The mapping shows that DHS Catalog covers the security concepts of NIST SP 800-53 and NERC CIP. It is also highly congruent with ISO 27001 (probably as a consequence of the NIST SP 800-53 compatibility with ISO 27001 described in the previous paragraph). In comparison to the standards, DHS Catalog, provides more requirements (250, NIST SP 800-53 Rev. 3 – 194).

IEC 62443-2-1 and ISO 27019 are both based on ISO 27001. IEC 62443-2-1 is more extensive, while ISO 27019 more adherently follows the structure of ISO 27001. Both standards present different approaches to describe the requirements. IEC 62443-2-1 offers more detailed, practical descriptions while ISO 27019 is rather concise. It is worth to note that ISO 27019 contains a more elaborated section on procurement requirements, to which a separate appendix (Annex B) is devoted. In IEC 62443-2-1 the important subject of controls systems acquisition is addressed more generally. NISTIR 7628 is primarily based on NIST SP 800-53, NERC CIP and DHS Catalog. It has similar thematic coverage and the level of technical details (low) to the above standards, but it is directly dedicated to the smart grid infrastructure. The congruence between the standards is illustrated by the mapping in Appendix A of NISTIR 7628.

NISTIR 7628 has general orientation, it is not concentrated on a particular smart grid area and its cybersecurity problems. The six standards in the 'SG area' lane (see Figure 2), on the other hand, are focused standards, dedicated to concrete sector domains and issues. IEEE C37.240 to substations, Cyber Security Procurement Language for Control Systems to systems' acquisition and design in IACS, ISO 15118 to plug-in electric vehicles (PEVs) communication, while AMI System Security Requirements and Privacy and Security of AMI to the advanced metering infrastructure. IEEE C37.240 refers to NISTIR 7628 and for high-level requirements indicates the interfaces of the NISTIR smart grid architecture which are valid for electric substations. At the same time it sends to the more technically oriented IEEE 1686 for cybersecurity requirements of substation communications devices. Privacy and Security of AMI aims at complementing ISO 27002 and assumes its previous implementation by grid operators. Indications are provided for each requirement as to the ISO 27002 security area it addresses.

IEEE 1686, IEC 62443-3-3, and GB/T 20279 define cybersecurity for technical components of information systems. IEEE 1686:2013 for intelligent electronic devices (IEDs) in the electric sector, in response to NERC CIP regulations. IEC 62443-3-3 for IACS (assuming that a security program has been established and is being operated in accordance with IEC 62443-2-1). GB/T 20279 – for network and terminal separation products. The two standards located in the lowest lane in Figure 2 (IEC 62351 and ISO 19790) specify detailed technical requirements for generic elements of information systems such as secure communication or cryptographic protocols. The standards are independent of other standards and address disjoint areas.

5.13. Summary and comparison of standards

The requirements specified in the standards differ in the level of technical details, the scope and the thematic coverage (see Table 5 and 6). Some publications extend or partially repeat the requirements from other standards, while other are complementary or completely independent (see Figure 2). Four standards define cybersecurity requirements for IACS, two – for AMI. Power plants, PEVs and electric sectors IEDs are addressed each by one focused standard. Other documents are dedicated or can be adopted to the whole smart grid architecture, or describe very specific generic IT components. The electric substations as well as IACS distinguish from other smart grid domains in regard to the coverage by cybersecurity requirements, which are defined from general to technical, including practical implementation remarks. The similar coverage by cybersecurity requirements would be desirable for other smart grid areas. For instance there could be a standard analogous to IEEE C37.240 for each area of the smart grid.

5.14. Other findings

During the analysis of the standards useful mappings between requirements in a given publication and in other standards were identified. They include:

- The broad mapping of the DHS Catalog requirements to the requirements defined in 15 other publications (AGA12-1, AGA12-2, FIPS 140-2, API 1164, 2nd Edition, API Security Guidelines 3rd Edition, CAG: 20 Critical Controls, ISO 17799, ISO 27001, IEC 62351, IEEE 1402, ISA99-1, ISA99-2, NRC Reg Guide 5.71, NERC CIP rev. 3 and NIST SP800-53 Rev. 3) in Appendix A: Cross Reference of Standards of the DHS Catalog of Control Systems Security [15].
- The mapping between NISTIR 7628 Rev. 1 and NIST SP 800-53 Rev. 4, DHS Catalog and NERC CIP (1-9) Version 3 October 2010[3] presented in Appendix A of NISTIR 7628 [58].
- Mappings of ISO/IEC 27001 to NIST SP 800-53 Rev. 4 and NIST SP 800-53 to ISO/IEC 27001 included in Table H-1 and Table H-2 of NIST SP 800-53 Rev. 4 [53].

6. Related work

As mentioned in Section 3, during the literature search smart grid standardisation initiatives were identified that indicated already existent standards relevant to cybersecurity. The studies are based on expert knowledge and don't aim at the scientific completeness of their analyses. Thus they don't indicate a systematic method which would serve this purpose. In result they provide diverse sets of standards and address the subject from various perspectives.

[3] In 2012, the Electric Power Research Institute (EPRI) published a mapping the previous NISTIR 7628 version to the newer, fourth version of NERC CIP].

Additionally to that 8 scientific papers were discovered (see Section 3) that focus on identifying smart grid cybersecurity standards [64, 28, 63, 44, 27, 21, 76, 75]. Among them, the analysis presented by Wang et al. in [76] is the most systematic. In the first step, the authors perform a literature review based on transparent criteria (standard source, relevance to smart grid cybersecurity and representativeness). They indicate 17 publications that include such recognised standards as NISTIR 7628, IEEE 1686-2007, NERC CIP, NIST SP 800-53 and SP 800-82 or DHS Catalog [76].

All these studies expose varying levels of completeness and often address the subject from a specific angle. With the exception of [76], they don't provide details of a systematic method used in the evaluation, nor selection/evaluation criteria. Many of them are, in fact, just loose overviews of smart grid security related standards and guidelines. None of the studies is dedicated to the subject of cybersecurity requirements of for smart grid domains and components.

The research described in this paper presents the following distinctive features:

- It is dedicated to cybersecurity requirements – to the best of author's knowledge there are no other publications which address this subject despite its importance and actuality.
- It provides high assurance of completeness due to the application of a repeatable, systematic and rigorous literature search and analysis method with the explicitly defined selection and evaluation criteria (see Section 4).
- The details of the research method are provided (see Section 3).
- It constitutes a guide through smart grid standards that specify cybersecurity requirements – 17 standards and guidelines are described from the security requirements perspective, referred to each other and related to evaluation criteria.
- The relationships between cybersecurity requirements are analysed (see Section 5.12, and Figure 2).
- Additionally all the standards are referenced to the IEC smart grid architecture (see Figure 1) to illustrate relations between standards and smart grid components.

7. Conclusions

The analysis shows that several standards and guidelines have been published that define cybersecurity requirements for- or applicable to- smart grids. They present various level of details and coverage. There are documents dedicated to specific components of the smart grid including substations (1), power plants (1), AMI (2), IACS (4), IEDs (1) and PEV (1), as well as publications that can be adopted to the whole smart grid architecture (see Table 5 and 6). This paper brings in all the relevant standards into one place (based on a systematic study), and overviews the cybersecurity requirements which they specify. Also (criteria-based) indications are provided that aim at

Table 5: Smart grid or power systems' standards which define cybersecurity requirements.

	Standard	Scope	Applicability	Type	Range	Pub.
1.	NISTIR 7628	Smart grid cybersecurity	All components	General, technical	US[1]	2014
2.	NERC CIP	Bulk electric system cybersecurity	All components	General	US	2013
3.	IEC 62443	IACS cybersecurity	IACS (SCADA)	Technical	Worldwide	2009
4.	IEEE C37.240	Cybersecurity of communication systems	Substations	Technical	Worldwide	2014
5.	Cyber Security Procurement Language for CS	Cybersecurity requirements for procurement	IACS (SCADA)	Technical	US	2008
6.	Privacy and Security of AMI	Security and privacy requirements	AMI	General	Netherlands	2010
7.	AMI System Security Requirements	Cybersecurity requirements for procurement	AMI	Technical	US	2008
8.	DHS Catalog	IACS cybersecurity	IACS (SCADA)	General	US	2009
9.	ISO/IEC 27019	Power systems' IACS security	IACS (SCADA)	General	Worldwide	2013
10.	IEC 62351	Security of communication protocols	All components	Technical	Worldwide	2007
11.	IEEE 1686	Cybersecurity	IEDs	Technical	Worldwide	2007
12.	ISO 15118	Vehicle-grid communication	PEV and relevant comm. infr.	Technical	Worldwide	2014
13.	VGB S-175	Cybersecurity requirements for power plants	Power plants	Technical	Germany	2014

[1] NIST Special Publications and Internal Reports are widely recognised and applied worldwide.

Table 6: General application standards and guidelines that specify cybersecurity requirements.

	Standard	Scope	Type	Range	Pub.
14.	ISO/IEC 27001	IS management	General	Worldwide	2013
15.	GB/T 22239	IS management	General, technical	China	2008
16.	GB/T 20279	Security requirements for firewalls and similar devices	General, technical	China	2015
17.	ISO/IEC 19790	Security requirements for cryptographic modules	Technical	Worldwide	2012

helping choose the standards which are applicable to a particular smart grid area and/or that address specific goals.

Security requirements in NISTIR 7628 are an amalgam of requirements defined in several sources: NIST SP 800-53, DHS Catalog, NERC CIP, and the NRC Regulatory Guidance, modified to match the specific needs of the smart grid and the electric sector. To facilitate compliance assessments a detailed guide [65] has been published together with a companion spreadsheet. For these reasons the publication might be the first choice of reference as far as general requirements, applicable to all smart grid components, are concerned.

When looking at particular smart grid areas, the electric substations as well as IACS are distinctly covered by cybersecurity requirements. The available standards define them on ifferent levels, from general to technical and supplement with actical implementation guidelines. The analogous coverage cybersecurity requirements of other smart grid domains, for stance by developing standards similar to IEEE C37.240, would advantageous.

References

References

[1] (2008). GB/T 22239:2008 – Information Security Technology – Baseline for Classified Protection of Information System Security. Technical report.

[2] (2015). GB/T 20279-2015 – Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products. Technical report.

[3] (2017a). SoES – Security of Energy Systems.

[4] (2017b). STARGRID – STandard Analysis supporting smart eneRgy GRID developmen.

[5] Aillerie, Y., Kayal, S., Mennella, J.-p., Samani, R., Sauty, S., and Schmitt, L. (2013). Smart Grid Cyber Security.

[6] Arora, V. (2005). Comparing different information security standards : COBIT v s . ISO 27001. *Carnegie Mellon University, Qatar*, pages 7–9.

[7] Bartsch, M., Ewich, T., Freckmann, C., Heming, R., Huckschtag, M., Kanisch, H., Krietemeyer, T., Mallon, M., Menauer, J., Schaeffer, P., Schugt, H., Seebens, J., Vogelpoth, C., Walter, T., Zevenberge, I., and Kaiser, J. (2014). VGB-S 175 – IT Security for Generating Plants. Technical report.

[8] Beckers, K., Côté, I., Fenz, S., Hatebur, D., and Heisel, M. (2014). A Structured Comparison of Security Standards. pages 1–34. Springer International Publishing.

[9] Brown, B., Singletary, B., Willke, B., Bennett, C., Highfill, D., Houseman, D., Cleveland, F., Lipson, H., Ivers, J., Gooding, J., McDonald, J., Greenfield, N., and Li, S. (2008). AMI System Security Requirements v1.01. Technical report.

[10] CEN-CENELEC-ETSI JWG (2011). Final report Standards for Smart Grids.

[11] CEN-CENELEC-ETSI Smart Grid Coordination Group (2014a). SG-CG/M490/H_Smart Grid Information Security. Technical report.

[12] CEN-CENELEC-ETSI Smart Grid Coordination Group (2014b). Smart Grid Set of Standards Version 3.1. Technical report.

[13] Commission, E. (2011). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Smart Grids: From Innovation To Deployment COM(2011) 202. Technical report, European Commission.

[14] DHS (2008). Cyber Security Procurement Language for Control Systems Version 1.8. Technical report.

[15] DHS (2009). Catalog of Control Systems Security: Recommendations for Standards Developers. Technical report.

[16] DKE (2013). German Roadmap E-Energy/Smart Grid 2.0. Technical report, German Commission for Electrical, Electronic & Information Technologies of DIN and VDE.

[17] Eastaughffe, K., Cant, A., and Ozols, M. (1999). A framework for assessing standards for safety critical computer-based systems. In *Proceedings 4th IEEE International Software Engineering Standards Symposium and Forum (ISESS'99). 'Best Software Practices for the Internet Age'*, pages 33–44. IEEE Comput. Soc.

[18] ENISA (2016). PETs controls matrix: A systematic approach for assessing online and mobile privacy tools. Technical report.

[19] EPRI (2012). Mapping the National Institute of Standards and Technology Interagency Report 7628 Security Requirements to the North American Electric Reliability Corporation Critical Infrastructure Protection Standards. Technical report.

[20] European Commission (2011). M/490 Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment. Technical report.

[21] Falk, R. and Fries, S. (2011). Smart Grid Cyber Security - An Overview of Selected Scenarios and Their Security Implications. *PIK - Praxis der Informationsverarbeitung und Kommunikation*, 34(4):168–175.

[22] Falliere, N., Murchu, L. O., and Chien, E. (2011). W32.Stuxnet Dossier. Technical report, Symantec Security Response.

[23] Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., Zhu, Z., Lambotharan, S., and Chin, W. H. (2013). Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Communications Surveys & Tutorials*, 15(1):21–38.

[24] Fang, X., Misra, S., Xue, G., and Yang, D. (2012). Smart Grid The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, 14(4):944–980.

[25] Gazis, V. (2017). A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Communications Surveys & Tutorials*, 19(1):482–511.

[26] Ghansah, I. (2012). Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks. Technical report, Sacramento.

[27] Goraj, M., Gill, J., and Mann, S. (2012). Recent developments in standards and industry solutions for cyber security and secure remote access to electrical substations. In *11th IET International Conference on Developments in Power Systems Protection (DPSP 2012)*, pages 161–161. IET.

[28] Griffin, R. W. and Langer, L. (2015). Chapter 7 Establishing a Smart Grid Security Architecture. In *Smart Grid Security*, pages 185–218.

[29] Hauer, I., Styczynski, Z. A., Komarnicki, P., Stotzer, M., and Stein, J. (2012). Smart grid in critical situations. Do we need some standards for this? A german perspective. In *2012 IEEE Power and Energy Society General Meeting*, pages 1–8. IEEE.

[30] Idaho National Laboratory (2005). A Comparison of Cross-Sector Cyber Security Standards. Technical report.

[31] IEC (2010). IEC 62443-2-1: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.

[2] IEC (2013). IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

[3] IEC (2017a). Smart Grid.

[4] IEC (2017b). Smart Grid Standards Map.

[5] IEEE (2013). IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.

[36] IEEE Power & Energy Society. Power System Relaying Committee., IEEE Power & Energy Society. Substations Committee., Institute of Electrical and Electronics Engineers., and IEEE-SA Standards Board. (2014). C37.240-2014 – IEEE standard cybersecurity requirements for substation automation, protection, and control systems. Technical report.

[37] IEEE Standards Association (2015). IEEE Smart Grid Interoperability Series of Standards.

[38] ISO (2014). ISO 15118-2:2014 Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements. Technical report.

[39] ISO/IEC (2012). ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules. Technical report.

[40] ISO/IEC (2013a). ISO/IEC 27001:2013: Information technology Security techniques Information security management systems Requirements.

[41] ISO/IEC (2013b). ISO/IEC TR 27019:2013: Information technology Security techniques Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

[42] ISO/IEC (2016). ISO/IEC 27000:2016 Information technology Security techniques Information security management systems Overview and vocabulary.

[43] Kanabar, M. G., Voloh, I., and McGinn, D. (2012a). A review of smart grid standards for protection, control, and monitoring applications. In *2012 65th Annual Conference for Protective Relay Engineers*, pages 281–289. IEEE.

[44] Kanabar, M. G., Voloh, I., and McGinn, D. (2012b). Reviewing smart grid standards for protection, control, and monitoring applications. In *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, pages 1–8. IEEE.

[45] Kosanke, K. (2006). ISO Standards for Interoperability: a Comparison. In *Interoperability of Enterprise Software and Applications*, pages 55–64. Springer-Verlag, London.

[46] Kuligowski, C. (2009). *Comparison of IT Security Standards*. PhD thesis.

[47] Lee, A., Snouffer, S. R., Easter, R. J., Foti, J., and Casar, T. (2001). NIST SP 800-29 A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2. Technical report.

[48] Liu, J., Xiao, Y., Li, S., Liang, W., and Chen, C. L. P. (2012). Cyber Security and Privacy Issues in Smart Grids. *IEEE Communications Surveys & Tutorials*, 14(4):981–997.

[49] Metheny, M. (2013). Comparison of Federal and International Security Certification Standards. In *Federal Cloud Computing*, pages 195–216. Elsevier.

[50] Metheny, M. (2017). Comparison of federal and international security certification standards. In *Federal Cloud Computing*, pages 211–237. Elsevier.

[51] Mitchell, R. and Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, 46(4):1–29.

[52] National Institute of Standards and Technology (NIST). NIST Smart Grid Collaboration Wiki.

[53] National Institute of Standards and Technology (NIST) (2013). *NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations*. U.S. Government Printing Office.

[54] NERC (2017). CIP Standards.

[55] Netbeheer Nederland (2010). Privacy and Security of the Advanced Metering Infrastructure. Technical report.

[56] NIST (2012). NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards. Technical report, National Institute of Standards and Technology.

[57] NIST (2014a). NIST SP 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. Technical report, Na.

[58] NIST (2014b). NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity. Technical report, NIST.

[59] OpenSG (2017). Security Working Group. Technical report.

[60] Overman, T. M., Davis, T. L., and Sackman, R. W. (2010). High assurance smart grid. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10*, page 1, New York, New York, USA. ACM Press.

[61] Pearson, I. L. (2011). Smart grid cyber security for Europe. *Energy Policy*, 39(9):5211–5218.

[62] Phillips, T., Karygiannis, T., and Huhn, R. (2005). Security Standards for the RFID Market. *IEEE Security and Privacy Magazine*, 3(6):85–89.

[63] Rosinger, C. and Uslar, M. (2013). Smart Grid Security: IEC 62351 and Other Relevant Standards. In *Standardization in Smart Grids - Introduction to IT-Related Methodologies, Architectures and Standards*, pages 129–146.

[64] Ruland, K. C., Sassmannshausen, J., Waedt, K., and Zivic, N. (2017). Smart grid security an overview of standards and guidelines. *Elektrotechnik und Informationstechnik*, 134(1):19–25.

[65] SGIP (2012). Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security.

[66] Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5):267–270.

[67] Sommestad, T., Ericsson, G. N., and Nordlander, J. (2010). SCADA system cyber security A comparison of standards. In *IEEE PES General Meeting*, pages 1–8. IEEE.

[68] Standardisation Management Board Smart Grid Strategic Group (SG3) (2010). IEC Smart Grid Standardization Roadmap. Technical Report June, Standardisation Management Board Smart Grid Strategic Group (SG3).

[69] State Grid Corporation of China (2010). SGCC Framework and Roadmap to Strong & Smart Grid Standards. Technical report, State Grid Corporation of China.

[70] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2. Technical report, NIST.

[71] Sunyaev, A. (2011). *Health-care telematics in Germany : design and application of a security analysis method*. Gabler.

[72] Symantec Security Response (2016). Destructive Disakil malware linked to Ukraine power outages also used against media organizations.

[73] Tipton, H. (2003). *Information Security Management Handbook*. CRC Press, Inc., Boca Raton, FL, USA.

[74] Von Solms, R. (1999). Information security management : why standards are important. *Information Management & Computer Security*, 7(1):50–57.

[75] Wang, Y., Ruan, D., and Xu, J. (2011a). Analysis of Smart Grid security standards. In *2011 IEEE International Conference on Computer Science and Automation Engineering*, pages 697–701. IEEE.

[76] Wang, Y., Zhang, B., Lin, W., and Zhang, T. (2011b). Smart grid information security - a research on standards. In *2011 International Conference on Advanced Power System Automation and Protection*, pages 1188–1194. IEEE.

[77] Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly*, 26(2):xiii–xxiii.

[78] Wouter Vlegels and Leszczyna (eds.), R. (2012). *Smart Grid Security: Recommendations for Europe and Member States*.

[79] Yilin Mo, Kim, T. H.-J., Brancik, K., Dickinson, D., Heejo Lee, Perrig, A., and Sinopoli, B. (2012). CyberPhysical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, 100(1):195–209.

[80] Zhang, Y., Wang, J., Hu, F., and Wang, Y. (2017). Comparison of evaluation standards for green building in China, Britain, United States. *Renewable and Sustainable Energy Reviews*, 68:262–271.