This is a postprint of the paper published in the *Computer Standards & Interfaces* journal.
DOI: https://doi.org/10.1016/j.csi.2017.09.005.

Cyber Security Standards for Smart Grid – a Comprehensive Survey

Rafał Leszczyna

Gdańsk University of Technology, Narutowicza 11/12, 80-233 Gdańsk, Poland

Abstract

Resilient information and communications technologies are prerequisite for reliable operation of smart grid. In recent years many standards for the new form of electricity network have been proposed which results in the situation that operators and other smart grid stakeholders have difficulties in finding the documents which can be related to their particular problems. To address this challenge a systematic study was conducted that aimed at identification of standards most relevant to the cyber security of smart grid. In result thirty six publications on security and eleven on privacy have been identified that are described and compiled in this paper. The details of the research method and the standards' selection and evaluation criteria are presented.

Keywords: cyber security, privacy, smart grid, standards, critical infrastructures, energy systems, industrial control systems, advanced metering infrastructure, electric substations

1. Introduction

Smart grid brings in multiple benefits stemming from wide application of Information and Communication Technologies (ICT) that include improved power reliability and quality, self-healing and increased resilience to disruption, predictive and automated maintenance, or increased consumer choice [1]. At the same time the dependence on the ICT and interconnection with the Internet results in new security and privacy concerns. Each network connection of the grid constitutes a potential entry for a cyber-attack and every network layer and the technology used may become its possible target. Moreover, because the smart grid is a complex system of distributed and interconnected systems, it presents an exceptionally large attack surface [2].

The new grid is exposed to the whole myriad of cyberthreats which evolve dynamically. Botnets, zero-days, Distributed Denial of Service Attacks (DDoS) or Advanced Persistent Threats (APT), are only few examples of threats which emerged or advanced significantly in the last years. There are also completely new threats inherent to the smart grid domain. These, for instance, include the attacks on the smart grid metering infrastructure. Compromising a smart meter opens a way for reaching other smart grid devices, such as smart thermostats, appliances, charging stations, because they are all interlinked. Furthermore, the location of some of the smart grid components in public places or at the end user facilities exposes them to a nearly 24/7 potential attacker activity [2, 3]. Effective and reliable protection of smart grids is one of the key enablers of their adoption.

To protect the smart grid, various security solutions can be applied, including traditional cyber security technologies such as encryption, access control, anti-malware or firewalls, as well as advanced methods, for instance: Security Information and Event Management (SIEM) systems, trusted computing platforms or Situation Awareness Networks (SANs) [4, 2, 5, 6, 7]. Security experts agree that standardised solutions and practices should be used in the first place [8, 9]. Standards help officers responsible for introducing new security measures to answer the questions regarding the choice of methods, implementation priorities and extent, or the sufficiency of the approach. Solutions based on so called "expert knowledge" of individual company employees may suffer from limitations, depending on the experts' experience and knowledge. The practices recommended in the standards, on the other hand, offer high level of assurance that they are systematic, complete and secure, as they were evaluated by numerous experts in a long-term process.

The reasons for complying to standards are numerous [10, 11, 12, 9]. Among them the fact that they enable certification is worth to note as it constitutes a way for gaining credibility of customers and building a competitive advantage among other organisations in the sector [12, 9]. It is also quoted as one of primary adoption drivers [12]. However it should be borne in mind that standards are not a "silver bullet". They are often generic and deliberately broad in scope, thus not offering detailed instructions on how to resolve certain implementation issues. In result this is the quality of the implementation of recommendations specified in standards which accounts for the effective level of obtained security [13].

In recent years numerous smart grid standards have

Email address: rle@zie.pg.gda.pl (Rafał Leszczyna)

been published. This results in the situation that operators find it difficult to orientate themselves in this plethora of literature, for instance, when choosing a standard applicable to a particular domain or functional area of the grid. Each time they want to choose a standard-recommended solution, they are forced to conduct a time consuming study in order to select the relevant standards. The research presented in this paper aims at addressing this problem by identifying the standards which address the subject of smart grid cyber security. Based on a systematic literature review that comprised three main stages (see Section 2), 36 cyber security publications of relevance were identified. Some of the publications are not standards in the rigorous meaning of this word. Originally they were depicted by their authors as guidelines, technical reports, special publications or regulations. However over time they have become de facto standards[1].

The paper is organised as follows. In Section 2 the method of the research is described, followed by the presentation of standards' selection and evaluation criteria (see Section 3). Section 4 describes standardisation initiatives mentioned in the analysed literature. Many of them comprised stocktaking studies, including security-oriented. The key part of the paper (see Section 5) is dedicated to the demonstration of the 36 identified standards that address security issues in smart grid. Although the study was primarily focused on security, the publications were also analysed with regard to privacy. Section 6 presents the results of this analysis, namely 12 standards are described which to a greater or lesser degree describe privacy questions in smart grids. Finally, after discussion of related work (see Section 7), the paper concludes with closing remarks.

2. Research method

The literature survey was based on the approach of Webster and Watson [14]. A rigorous systematic search process was imposed to identify standards, scientific papers and books, as well as technical reports that describe cyber security standards for smart grids. The strict discipline of the process aimed at assuring its repetitiveness and comprehensiveness, and providing 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*, *literature analysis* and *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, electronic search was performed of the keywords in any descriptive metadata of publications. This led to 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 resulting around 700 records were then analysed manually to elicit 79 publications that seemed relevant to the research. In-depth review of these publications led to 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 [15, 16, 17, 18, 19, 20, 21, 22] 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. [23, 24, 25, 26] were found. The following initiatives related to smart grid standardisation were identified [19, 27, 28, 25]:

- CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) [29, 19],
- European Commission Smart Grid Mandate Standardisation M/490 [30, 27],
- German Standardisation Roadmap E-Energy / Smart Grid [23],
- IEC Strategic Group 3 Smart Grid [31, 32, 33, 26, 27],
- IEEE Smart Grid Standardisation [34, 35, 16, 36],
- ITU-T Smart Grid Focus Group [37],
- Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for Smart Grid [25],
- OpenSG SG Security Working Group [38, 36],
- Smart Grid Interoperability Panel [39, 19, 27],
- The State Grid Corporation of China (SGCC) Framework [40, 27].

These activities were primarily dedicated to development of new standards and guidelines, but the majority of them also indicated already existent standards relevant to the subject. They are briefly described in Section 4. Among them, the work of IEC needs to be noted, as it

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

Table 1: Literature search summary.

Publisher	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
Database						
EBSCOhost	258	4	129	7	16	15
Scopus	5361	5	288	145		
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 absence of all metadata search.

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

plays particular role in this paper. IEC prepared and maintains a very useful website with a Smart Grid Standards Map [33] – an interactive graphical tool that facilitates identification of relationships between standards and smart grid components (see Section 4.4 and Fig. 1). 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 3. 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 search for standards related to smart grid cybersecurity. Additionally, the literature search phase was extended to identify other (possibly all) smart grid cyber security standards' identification initiatives which revealed ongoing or concluded projects that are completely or partially dedicated to smart grid standards' stocktaking [41, 42]. It became evident that these undertakings address the subject from various perspectives and provide different sets of standards.

Standards selection. The selection criteria discussed in Section 3 were applied to the identified standards. As a result 36 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 cyber security were depicted. These publications are described in Section 5. Table 2 shows the standards and standards' series that were referred to more than once in the analysed publications. The standards and guidelines which occurrence number is greater than 3 can be depicted as *most recognised.* These publications include IEC 62351, ISO/IEC 27000, IEEE 1686, NERC CIP, NISTIR 7628 and IEC 62443 (formerly ISA 99).

Table 2: Standards indicated in more than 1 study.

Publication	Type	Occur.
IEC 62351	Standard	15
ISO/IEC 27000	Standards	11
NERC CIP	Regulation	10
IEEE 1686	Standard	9
NISTIR 7628	Guideline	7
IEC 62443 (ISA 99)	Standards	7
GB/T 22239	Standard	3
NIST SP 800-53	Guideline	3
NIST SP 800-82	Guideline	3
ISO/IEC 15408	Standard	3
DHS Catalog	Guideline	2
IEC 62056-5-3	Standard	2
ISO 15118	Standard	2
ISO/IEC 27019	Standard	2
Security Profile for AMI	Guideline	2

3. Standards' selection and evaluation criteria

A literature search analogous to the one described in the previous section was dedicated to identification of attributes that facilitate characterisation and comparison of standards. In result 17 publications related to evaluation of standards [15, 43, 44, 45, 46, 47, 48, 49, 50, 51, 13, 52, 53, 54, 55, 56, 57] were identified. 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 [48] 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 with reference to healthcare and healthcare specific IS security approach characteristics.

Sommestad et al. [50] present a quantitative standards' evaluation method that comprises three phases: selection; grouping of recommendations and threats; quantifying fo-

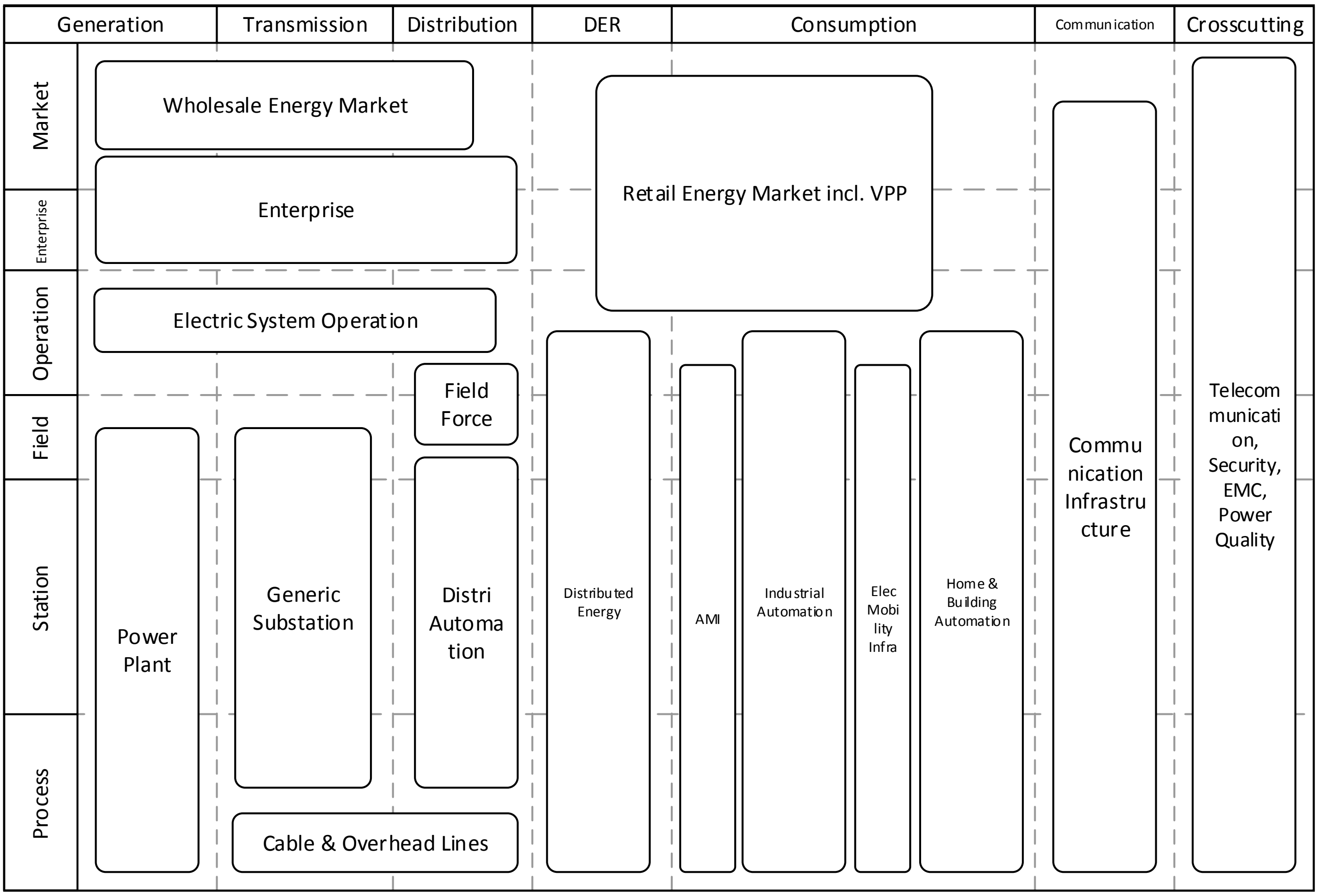

Figure 1: Smart grid components based on the IEC Smart Grid Standards Map [33].

cus of standards. Standard selection criteria are defined which include availability in English, focus on SCADA system security or type of publishing organisation. The comparison of standards is quantitative, based on the normalised value for the number of occurrences of certain keywords in the compared texts.

Beckers et al. [47] developed a structured, conceptual model for analysis of standards and a template that facilitates its application. A common terminology is defined. The paper comprises good discussion of other standards' surveys. Siponen and Wilson [13] 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 defines qualitative criteria. Arora [53] evaluates standards according to their focus, scope, structure, organisational model etc. Phillips et al. [55] compares technical features (including band, range and data) and security features (confidentiality, integrity, availability). ENISA's evaluation of Privacy Enhancing Technologies [46] distinguishes between maturity and stability, privacy policy implementation and usability. Zhang et. al [43] – objective and measures (idea analysis), Gazis [45] – maturity, layers, arrangement, domain, definitions, audience, etc. Eastaughffe et al. [57] focus on the domain-specific features such as safety management agents, integrity levels, human factors, assurance techniques or post-development issues. Kuligowski [51] compares standards' terminology, maps controls and documents, and defines qualitative/quantitative criteria that include effectiveness of security standards, number of certifications, number of privacy data breaches, target organisations etc.

Another approach is presented in NIST SP 800-29 [56] where the content of documents is compared, section by section. Similarly in the works of Kosanke [52] and Metheny [58] who also present domain-specific comparison criteria. While Ruland et al. [15] and Idaho National Laboratory [54] 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 [48] in his study dedicated to the healthcare sector depicts an impressive number of security assessment-related criteria.

Based on the analysis, the following, mutually non exclusive *selection criteria* were chosen. A standard to be selected for a content based evaluation (see previous Section) needed to be: (a) published in English, (b) referenced

Table 3: Standards' evaluation criteria.

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

in smart grid standard identification studies or papers, (c) published by a standardisation body or governmental institution, (d) related to cyber security. The *evaluation criteria* which serve in comparing the selected standards are presented in Table 3.

4. Standards identification initiatives

During the *literature analysis* stage of the research (see Section 2), reports were discovered which describe institutional initiatives carried out mostly by standardisation bodies that aim at identifying smart grid security standards. This chapter provides descriptions of these initiatives. The presentations focus on cyber security related actions.

4.1. European Commission Smart Grid Mandate M/490

Mandate M/490, directed to the European standardisation bodies, was issued by the European Commission on the first of March, 2011. The aim of the mandate is to develop or update a set of standards that foster creation and operation of the European smart grid. The mandate requests the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI) to develop a smart grid standardisation framework that would facilitate continuous standard enhancement and development by European standardisation bodies. The framework should include: 1) specification of a technical reference architecture, 2) a set of standards and 3) definition of standardisation methodology and tools. The mandate explicitly indicates cyber security, information security and privacy, system integrity and data protection and integrity as technical areas that need to be addressed. In fact, a distinct part of the document is dedicated to specification of standardisation activities related to information security and data privacy.

4.2. CEN/CENELEC/ETSI Smart Grid Coordination Group

Smart Grid Coordination Group (SG-CG) is a joint initiative of the three European standardisation bodies: CEN, CENELEC and ETSI launched in response to the Mandate M/490 (see Section 4.1) which aims at providing a unified framework for smart grid standardisation in Europe. At the end of 2014 the group published final versions of the reports that describe components of the standardisation framework: 1) an extended set of standards that fosters smart grids deployment, 2) standardisation methodology, 3) interoperability measures and 4) information security measures.

The report on information security [29] was prepared by the Smart Grid Information Security (SGIS) working group. It describes key elements of smart grid information security, namely the smart grid architecture model, smart grid information security levels and selected use cases. Substantial part of the work is dedicated to the identification of existent standards relevant to smart grid information security and privacy, as well as potential standardisation gaps. 10 standards with security requirements and 7 standards that specify security solutions are presented. Each of the standards is referred to the Smart Grid Reference Architecture (see Figure 1). Security recommendations and a new risk assessment methodology are provided that are in line with the work of the European Network and Information Security Agency (ENISA) [29].

4.3. German Roadmap E-Energy / Smart Grid

E-Energy/Smart Grid Expertise Centre for Standardization within the German Commission for Electrical, Electronic & Information Technologies of DIN and VDE (DKE) performed actions related to the development of a strategic plan of German standardisation activities in the context of European and global developments, which among the others included the analysis of the current situation worldwide. The results of this initiative were presented in two subsequent versions of the *German Roadmap E-Energy / Smart Grid* published in 2010 and 2013 [59, 23]. Both documents include summary tables which compare various studies on smart grid standardisation, but more descriptive contents focused on standards are presented in the earlier report. There recommendations for security and privacy are presented as well [59]. The second report contains a separate chapter dedicated to security aspects of smart grids, which in fact summarises the work of the CEN/CENELEC/ETS SG-CG (see Section 4.2) [23]. 9 standards that address security questions were identified by the initiative.

4.4. IEC Strategic Group 3 Smart Grid

The IEC Strategic Group on Smart Grids (IEC SG3) is responsible for international standardisation activities in the field of smart grid technologies. The group developed a standards framework and released a roadmap which inventories existing, primarily IEC, standards and allocates them to different smart grid applications [26]. In the report, the recommendations for further developments of standards are presented.

Additionally to that the group maintains a website which facilitates access to the most relevant standards [60]. The site facilitates identification of standards based on their topic and smart grid area i.e. the relevant components of the smart grid architecture (see Fig. 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, which were published by standardisation bodies including IEC, ISO, CISPR, EN, ENTSO, ETSI, ITU-T, W3C, IEEE, IETF and other. There are 18 (IEC and ISO) standards identified as relevant to smart grid security.

It is also possible to download a list of smart grid-related IEC standards. The list is presented in an interactive Excel file where standards are classified according to their topic. The topics include various types of energy source (solar voltaic, wind turbines, hydro power etc.), different parts of the infrastructure (electrical relays, power-line, substation automation etc.) and others. There are three topics relevant to its security: "Information Technology security","security" and "security of control systems", for which 13 standards are indicated.

4.5. IEEE Smart Grid Standardisation

The IEEE publishes over 100 standards and standards in development relevant to smart grid, including more than 20 that are recognised by the SGIP (see Section 4.9) and included into its smart grid interoperability roadmap [39]. Currently there are 19 IEEE Working Groups and 37 projects that contain "smart grid" in the name. Among them the IEEE 2030 and IEEE 1547 projects are highly recognised [34, 16, 36]. The former resulted in publication of several standards dedicated to smart grid operability that define the Smart Grid Interoperability Reference Model (SGIRM), the terminology, characteristics, functional performance and evaluation criteria, as well as engineering principles for smart grid interoperability. The latter (IEEE 1547) concluded with specification of requirements for interconnecting distributed energy resources to the distribution segment of the electric power system.

4.6. ITU-T Smart Grid Focus Group

ITU-T Focus Group on Smart Grid (FG Smart) operated between February, 2010 and December, 2011. Its objective was to lay the foundations for development of smart grid standards (recommendations) by the ITU-T. This was achieved by recognising smart grid standardisation actors, preparing a glossary of smart grid terms, identifying prospective directions of research, analysing case studies and developing requirements for network communication, evaluating potential impacts of on standards development for various thematic areas. The group delivered five reports that describe: 1) the use cases, 2) communication requirements, 3) the smart grid architecture, 4) smart grid concepts, 5) and the terminology [61]. The *Smart Grid Architecture* document [62] presents the results of gap analysis between standards and smart grid functions. There several standards are indicated that address subsequent smart grid domains, including two related to security. The report itself directs to NISTIR 7628 for a description and requirements of security functions [62].

4.7. Japanese Industrial Standards Committee

In Japan, under the Japanese Industrial Standards Committee (JISC), two strategic groups were founded: in 2009, the Study Group on International Standardization for Next Generation Energy Systems and in 2012, the Subcommittee on Smart Grid International Standardization, with the aim of promoting Japanese smart grid standardisation activities and developing a roadmap for Japan's contribution to the international smart grid standardisation effort. The groups identified the current status of smart grid developments and initiatives, identified the thematic areas of interest (Wide-Area Awareness in Transmission, Supply-Side Energy Storage, Distribution Grid Management, Demand Response, Demand-Side Energy Storage, Electric Vehicles and AMI Systems), selected the 26 Priority Action Areas of Japanese contribution and analysed possible standardisation strategies. The topics are addressed in cooperation with other international bodies, including IEEE, IEC and CEN/CENELEC [34, 25].

4.8. OpenSG SG Security Working Group

The Utility Communications Architecture (UCA) is a standards-based communication architecture for the electric, gas, and water utilities that facilitates large scale integration at reduced costs. It was designed in the nineties by the IEEE and the Electric Power Research Institute (EPRI). UCA applies to all functional areas including customer interface, distribution, transmission power plant, control center, and corporate information systems [63].

The Open Smart Grid (OpenSG) User's Group is a member group of the UCA International Users Group – a not-for-profit organisation that assists users and vendors in the deployment of standards for real-time applications for several industries and which works closely with the organisations responsible for developing such standards (e.g. the IEC TC 57: Power Systems Management and Associated Information Exchange). The group promotes broad adoption of advanced metering networks and demand response solutions through development of open standards. The Security Working Group of the OpenSG focuses on developing security guidelines, recommendations, and best practices for smart grid and AMI [64].

4.9. Smart Grid Interoperability Panel

In 2014 the National Institute for Standards and Technology released the third version of *NIST Framework and Roadmap for Smart Grid Interoperability Standards* [39] which summarises the results of the seven years work on identifying the standards by NIST Smart Grid Interoperability Panel (SGIP). Among the others the framework includes a list of smart grid standards and specifications identified as important for smart grid and a list of documents applicable to the grid.

In 2009 NIST established the Cyber Security Coordination Task Group (CSCTG) which was later incorporated into SGIP and renamed to the SGIP Cyber Security Working Group (CSWG). The group formed of over five hundred international experts has been continuously working on cyber security issues of smart grid. Since the beginning of 2013 when SGIP was transitioned to a private/public partnership funded by industry stakeholders in cooperation with the federal government, CSWG operates as the Smart Grid Cybersecurity Committee. Among many achievements, publication of *NISTIR 7628 Guidelines for Smart Grid Cyber Security* [65] is one of the most important. The document covers various aspects of smart grid security and provides a roadmap for developing effective cyber security strategies tailored to the specifics of organisations. There are cyber security requirements for smart grid presented in logical interface categories.

Additionally, in February, 2014, NIST published the *Framework for Improving Critical Infrastructure Cybersecurity* [66]. The framework aims at supporting critical infrastructure owners and operators in reducing cyber security risks in industries such as power generation, transportation and telecommunications. It relies on a variety of existing standards, guidelines, and practices and indicates them adequately to each area of critical infrastructure protection in the Framework Core. These references include publications such as: ISO/IEC 27001, NIST SP 800-53, ISA 62443, COBIT and CCS.

4.10. State Grid Corporation of China (SGCC)

In March 2009, the State Grid Corporation of China, the state-owned electric utility, created a working group responsible for studies on smart grid standards. According to [40], the group studied 1550 standards (781 international standards and 769 domestic standards). The study results were compiled into the *SGCC Framework and Roadmap for Strong and Smart Grid Standards* report [40] released in July, 2010.

5. Results of the analysis

The following sections provide characterisation of the standards from the security assessment point of view. The summary of the analysis is presented in Tables 4 – 9. The standards are described in the order of their recognisability by the smart grid standard identification studies or papers described in Section 2.

5.1. IEC 62351

The standards from the *IEC 62351 Power systems management and associated information exchange – Data and communications security* series aim at defining security properties of communication protocols defined by IEC TC 57 (IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970 and IEC 61968). They enable setting various levels of protocol security, depending on the protocol and the parameters selected for a specific implementation. They were designed for backward compatibility and phased implementations. Subsequent documents in the series introduce to the series, define common terms, specify security properties and address end-to-end information security [67]. The two introductory documents – *IEC 62351-1* (introduction) and *IEC 62351-2* (terms and definitions) are general in scope while the remaining 4 valid standards (other 2 were withdrawn) provide specific technical requirements. IEC 62351 standards apply to all components of the smart grid architecture (see Fig. 1) besides physical, cable layer. They have a worldwide range.

5.2. ISO/IEC 27001 and 27002

The *ISO/IEC 27000* series (or *ISO27k* for short) comprises information security standards that present good practices and recommendations on information security management, risks and controls. The standards resolve around the establishment and operation of an Information Security Management System (ISMS) which refers in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). The ISMS' cyclic character responds to the dynamic nature of the information security environment where threats, vulnerabilities or impacts of information security incidents change over time [68, 69, 70]. At present, around thirty standards in the series are published and available, while several more are still under development.

ISO/IEC 27001 [68], the flagship publication in the ISO/IEC 27000 series, is the most fundamental international standard for information security management, applied broadly by organisations of various profiles (commercial, governmental, not-for profit etc.) and sizes [71]. It is general in scope, not orientated towards any particular domain, sector or technology. It specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) within the organisations' business contexts [68, 69, 70]. *ISO/IEC 27002* provides auxiliary, practical guidance on the implementation of ISO/IEC 27001 [69]. The international standards ISO/IEC 27001 and 27002 can be applied to all components of the smart grid architecture (see Fig. 1).

5.3. NERC CIP

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards define requirements for controls and measures to protect the bulk power system from cyber threats. The current, fifth version of the standards, approved by the US Federal Energy Regulatory Commission (FERC) on November 22, 2013, represents visible change in the approach and composition of controls comparing to its predecessor apparent among the others in the focus shift from critical assets to cyber systems and three-level, impact-based classification of the systems. The series comprises 11 documents subject to enforcement. It can be applied to all components of the smart grid architecture (see Fig. 1).

5.4. IEEE 1686

IEEE Std 1686-2007 IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities [72] defines properties, functions, and practices for substations Intelligent Electronic Devices (IEDs) in the domains such as data access, diagnostics, configuration, firmware upgrading or manually forced operation. The standard establishes baseline security requirements for IEDs and defines which safeguards, audit mechanisms, and alarm indications need to be provided by IED' vendors. The standard supports users in defining security programs. It is designed to meet the NERC CIP requirements in the first place, but can be applied to any substation IED [72].

5.5. NISTIR 7628

The National Institute of Standards and Technology (NIST) Internal or Interagency Report (IR) 7628 Guidelines for Smart Grid Cyber Security is a three-volume report which provides a comprehensive framework for smart grid stakeholders that can be used for developing effective cyber security strategies tailored to their particular characteristics, risks, and vulnerabilities [65]. This de-facto standard is applicable to all components of the smart grid architecture (see Fig. 1).

In Volume 1 a logical reference model of smart grid is defined, which distinguishes twenty two logical interface categories of smart grid architecture. In relation to the model, high level security requirements for smart grid are specified. Further on cryptographic and key management issues as well as cyber security strategies are discussed. Volume 2 is dedicated to the privacy of smart grid stakeholders (see Section 6). Volume 3 presents other supplementary material that includes, for instance, classes of potential smart grid vulnerabilities classified by category, research and development themes or key power system use cases that are architecturally significant with respect to security requirements for smart grid [65].

5.6. IEC 62443 (ISA99)

The *ISA99* standards, developed by ISA99 Committee (ISA – the International Society of Automation), address electronic security of Industrial Automation and Control Systems (IACS). Since 2009 these standards have been adopted in the *IEC 62443* series, by the IEC Technical Committee 65 (“Industrial-process measurement, control and automation”) Working Group 10, which proceeds in strong collaboration with ISA99 Committee [73]. Specifications in the standards include security models and concepts, system security compliance metrics, security life cycle and use cases, patch management in the IACS environment, security technologies for IACS, security risk assessment and system design, implementation guidance for an IACS security management system, as well as various requirements that refer to different aspects of IACS (security management system, solution suppliers, product development, IACS system and its components).

5.7. GB/T 22239

GB/T 22239 Information Security Technology – Baseline for Classified Protection of Information System Security [74] 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 levels of security protection ability i.e. ,,the extent to which a system can defend against threat, detect security event and restore to the previous state in case of system damaged”. The requirements are split between technical and managerial.

5.8. NIST SP 800-53

NIST Special Publication (SP) 800-53 Recommended Security Controls for Federal Information Systems and Organizations [75] is a fundamental NIST document devoted to information security management. It guides through the process of selection and specification of security controls for information systems of federal agencies. The instructions are applicable to all components of information systems that are responsible for processing, storing, or transmitting federal information [75].

NIST SP 800-53, after FIPS 199, defines three types of information systems depending on their impact on information confidentiality, integrity, and availability: low impact, moderate impact and high impact systems. For each of the system types – a security control baseline – a set of minimum security controls is defined. The three security control baselines are hierarchical with regard to the security controls employed in those baselines. Each higher baseline comprises all security controls of the lower extended with some new [75].

Security controls defined in NIST SP 800-53 are grouped into seventeen families that cover all areas of information security management (technological, management, operational, legal, etc). NIST SP 800-53 very reasonably refers to security aspects, defining minimum requirements that can be satisfied by various organisations and sufficient to ensure a good level of security [75].

Although NIST SP 800-53 has been originally dedicated to US federal agencies, it raised great international interest, and is perceived as de-facto standard in the area, adopted and implemented by organisations and enterprises worldwide. It is fully compatible with ISO/IEC 27001 and the related ISO/IEC 27000 series. In Table H-1, Appendix H of NIST SP 800-53 [75]) a 1:1 assignment between NIST SP 800-53 and ISO/IEC 27001 is presented. NIST SP 800-53 can be applied to all components of the smart grid architecture (see Fig. 1).

5.9. NIST SP 800-82

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security is the NIST primary publication dedicated to the security of Industrial Control Systems (ICS). The document introduces to the topic and overviews various types of ICS (SCADA, PCS etc.) and typical system topologies. It identifies common ICS threats and vulnerabilities and specifies recommended security controls to mitigate the associated risks [76]. Similarly to other NIST publications it is widely recognised and adopted worldwide.

5.10. ISO/IEC 15408 and 18045 (Common Criteria and CEM)

The *ISO/IEC 15408* set of three standards *Information technology – Security techniques – Evaluation criteria for IT security* [77, 78, 79] describes criteria for security evaluation of IT products (hardware and software). The standards were originally developed in the Common Criteria project that aims at systematic, recognisable product validations and certifications. The members of the project granted ISO/IEC non-exclusive license to use their common criteria specifications in the ISO/IEC 15408 development. The currently available ISO/IEC 15408 standards are from 2008 and 2009, while the newest, freely available, Common Criteria (v3.1 Release 4) [80, 81, 82] were published at the end of 2012. These standards are fully devoted to the security assessment subject as far as security products are concerned. The assessments are performed in testing laboratories.

A separate document *Common Methodology for Information Technology Security Evaluation* (CEM) [83] on 433 pages explains standardised, systematic methodology of the assessments. The document is very detailed and technical. Although it doesn't explicitly mention smart grid, it can be applied to security evaluation of its software/hardware components. An earlier version of this document was adopted as *ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation* standard [84] and published in 2008. ISO/IEC 15408 and 18045 standards are publicly available without a charge[2].

5.11. DHS Catalog

The Department of Homeland Security (DHS)' Catalog of Control Systems Security: Recommendations for Standards Developers presents practices that various industrial organisations have recommended to increase the security of Industrial Control Systems (ICS). The recommendations, grouped into 19 categories, are broad in scope in order to provide a flexibility level that enables developing sound cyber security standards specific to individual security needs. The de-facto standard can be applied to all components the smart grid architecture (see Fig. 1).

5.12. IEC 62056-5-3

IEC 62056 series is dedicated to electric meter data exchange for meter reading, tariffs and load control. The standards specify different aspects of the communication including physical layer services, transport layers and application layers, object identification and interfaces. *IEC 62056-5-3 Electricity metering data exchange – The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer* [85] addresses information security issues of Device Language Message Specification (DLMS) and COmpanion Specification for Energy Metering (COSEM).

5.13. ISO 15118

The three-part international standard *ISO 15118 Road vehicles – Vehicle to grid communication interface* [86] specifies the communication interface between electric vehicles and the charging infrastructure. Part 2 defines network and application protocol requirements, including security [86].

5.14. ISO/IEC 27019

ISO/IEC TR 27019 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 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 [87]. 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 [87].

The structure of ISO/IEC 27019 is similar to ISO/IEC 27002. For the controls specified in ISO/IEC 27002:2005 that require a sector-specific method of implementation, implementation guidelines are provided [87]. Otherwise direct references are made to the specifications in ISO/IEC 27002. The list of the new control objectives and measures for the energy supply sector is provided in Annex A. Supplementary comments and notes are presented in Annex B [87].

[2] from `http://standards.iso.org/ittf/PubliclyAvailable-Standards/index.html`

5.15. Security Profile for Advanced Metering Infrastructure

Security Profile for Advanced Metering Infrastructure [88] is a guideline developed the Advanced Metering Infrastructure Security (AMI-SEC) Task Force and issued in June, 2010. The aim of the document is to provide guidance on building-in and implementing security in the AMI infrastructure. The majority of security controls presented in the standard are adapted from the DHS Catalog of Control Systems Security (see Section 5.11).

5.16. AMI System Security Requirements

AMI System Security Requirements [89] 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 grouped in three categories 1) Primary security services, 2) Supporting security services and 3) Assurance services. *DHS Cyber Security Procurement Language for Control Systems* [90] defines analogous procurement security requirements, but for Industrial Controls Systems.

5.17. IEC 62541

IEC 62541 OPC unified architecture is a series of platform-independent, interoperability standards for the secure and reliable exchange of data in the industrial automation space and in other industries. *IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model* [91] describes complete security model that includes the description of possible threats to the OPC Unified Architecture (UA) and security functions aiming to mitigate them. Important part of the document is dedicated to the analysis of how the OPC-UA security functions meet security objectives and defend from the threats.

5.18. IEEE 2030

IEEE Std 2030 series is also dedicated to smart grid (overall) interoperability. It specifies Smart Grid Interoperability Reference Model (SGIRM) and provides the relevant guidance. Cyber security is an integral part of the standard. *IEEE Std 2030 IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads* describes privacy and security protection techniques, smart grid security principles, security process, security engineering, risk management or security categorisation. *IEEE Std 2030.2-2015 Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure* [92] dedicates its Chapter 8 to the subject of security and privacy in energy storage systems. Also in *IEEE Std 2030.3-2016 IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard* the eight chapter is dedicated to security and privacy in the network communication application layer.

5.19. NRC RG 5.71

The US Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71 Cyber Security Programs for Nuclear Facilities [93] presents a set of security controls and the guidance on their use, that address national regulations regarding protection of nuclear infrastructures. The controls in the standard originate from NIST SP 800-53 and NIST SP 800-82, but they were adapted to the specifics of the nuclear energy sector. They are grouped into a template of a cyber security program presented in Appendix A. The standard introduces the notion of Critical Digital Assets (CDA) which are important from the security and safety point of view and must be obligatorily protected [93].

5.20. Standards on risk management

ISO/IEC 27005 Information technology – Security techniques – Information security risk management [70] is a subsequent very popular publication from the ISO/IEC 27000 series. It is explains the process of risk management, which is particularly suitable for the organisations that comply with ISO/IEC 27001. Another document devoted to risk management is *NIST SP 800-39 Managing Information Security Risk* [94] which explains the process in detail.

A risk management methodology dedicated to the electricity sector is described in *Electricity Subsector Cybersecurity Risk Management Process* [95] collaboratively developed by US DoE, NIST and NERC. The methodology is strongly based on the general-application risk management process described in NIST SP 800-39 [94].

US Department of Energy (DoE) *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities* [96] presents complete checklist-based approach to risk management for small- and medium-scale energy facilities, such as municipal and independent utilities, or rural cooperatives.

5.21. Standards with security requirements

IEEE C37.240 Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems [97] after describing the cyber security problem in the utilities sector, defines baseline cyber security requirements dedicated to electric substations' communication systems (automation, protection and control).

Dutch guideline *Privacy and Security of the Advanced Metering Infrastructure* [98] presents ISO 27001-based security and privacy requirements for AMI. German VGB-Standard *IT Security for Generating Plants* [99] specifies security requirements for power plants.

GB/T 20279 Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products [100] is a national, Chinese standard which presents technical security requirements for network separation devices (firewalls and similar).

NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise [101] defines security requirements for mobile devices and describes complete life cycle of secure management of the devices.

ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules [102] defines prerequisite security characteristics of cryptographic modules used in security systems that protect sensitive information in computer and telecommunication systems.

5.22. Other standards of relevance to smart grid cyber security

IEC 61400-25 Communications for monitoring and control of wind power plants series specifies uniform information model and protocols for communication between wind power plants and Industrial Control Systems. *IEC 61400-25-3* describes selected security aspects.

IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security [103] describes security aspects related to the establishment and operation of electric substations. It describes different types of physical intrusions, methods of protection against and evaluates the effectiveness of the measures. Section 6.2 is dedicated to computer security.

The series *ISO/IEC 14543 Information technology - Home electronic system (HES) architecture* consists of 20 standards that describe different components of home control systems including communication and interoperability aspects. Security aspects are addressed in *ISO/IEC 14543-5-1:2010* and *ISO/IEC 14543-5-7:2015*, where security mechanisms for Intelligent Grouping and Resource Sharing (IGRS) protocols are described.

NIST SP 800-64 Security Considerations in the System Development Life Cycle [104] demonstrates how to incorporate good security practices into the life cycle of IT system development.

RFC 6272 Internet protocols for the smart grid [105] identifies key Internet protocols to be used in smart grid. Several sections of the standard are dedicated to security.

5.23. Summary and comparison of standards

Tables 4 – 9 illustrate main features of the standards according to the criteria described in Section 3.

6. Privacy questions in the analysed standards

Although this study was primarily dedicated to the recognition of standards that address cyber secure operation of smart grid, the identified publications were also analysed with regard to presence of privacy related concepts. In result 12 standards of relevance were recognised that are enlisted in Table 6. This chapter provides descriptions of the standards and the privacy questions which they raise.

6.1. NISTIR 7628

Among the standards, *NISTIR 7628* stands out as from its three extensive volumes, one (177 pages) is completely devoted to privacy in smart grids [65]. The standard introduces basic privacy concepts, describes legal aspects of privacy in the grid, indicates which private information can be potentially disclosed in the smart grid and discusses in detail the privacy concerns that are characteristic to smart grid, such as learning personal behaviour patterns or performing real-time remote surveillance. The problem of inevitable in smart grid transfers of energy usage data to third parties is described as well as privacy issues of the electric vehicle communication. To answer these questions existent privacy protection standards and tools are indicated [65].

Privacy Impact Assessment (PIA) is a structured process that aims at evaluating the risks associated with storing, processing and sharing of personal information in a given context, as well as identifying the measures to mitigate the risks. The Privacy Subgroup of SCIP CSWG (see Section 4.9) performed the PIA for smart grid in 2009 an 2010. The methodology of the study, its findings and resulting recommendations are presented in a separate chapter [65]. The risks which will be evolving together with the development of new technologies are also discussed in the document, NIST actions in the field of privacy and recommendations for protecting privacy in smart grid are described. Additional detailed information is provided in 5 appendices where regulatory frameworks, third party data transfers related privacy practices, privacy use cases, summary of the PIA and privacy related definitions are described [65].

6.2. NIST SP 800-53

Also in *NIST SP 800-53*, which is not smart grid specific, but rather of general application, a considerable amount of content (26 pages) is dedicated to privacy. Namely, the Appendix J, after a brief introduction of the subject, defines 26 privacy controls, based on international standards and best practices, grouped into 8 families (AP - Authority and Purpose, AR - Accountability, Audit, and Risk Management, DI - Data Quality and Integrity, DM - Data Minimization and Retention, IP - Individual Participation and Redress, SE - Security, TR - Transparency and UL - Use Limitation) [75]. The controls, which include e.g. Privacy-Enhanced System Design and Development, Minimization of Personally Identifiable Information (PII) Used in Testing, Training, and Research or Inventory of Personally Identifiable Information [75] can be directly applied to protect privacy in smart grids.

6.3. IEC 62443 and ISO/IEC TR 27019

IEC 62443 addresses some selected privacy aspects series related to the use of IACS. *IEC 62443-2-1* states that “information that is sensitive to disclosure needs to be

Table 4: Smart grid or power systems' standards relevant to cyber security applicable to all smart grid components.

	Standard	Scope	Type	Range	Pub.
1.	IEC 62351	Security of communication protocols	Technical	Worldwide	2007
2.	NERC CIP	Bulk electric system cyber security	General	US	2013
3.	NISTIR 7628	Smart grid cyber security	General	US	2014
4.	NRC RG 5.71	Cyber security of nuclear infrastructures	General	US	2010
5.	EI RM Checklists	Risk management in small/medium energy facilities	General	US	2002
6.	Risk Management Process	Risk management in electric sector	General	US	2012
7.	IEC 62541	OPC UA security model	General	Worldwide	2016
8.	RFC 6272	Identification of Internet protocols for smart grid	Technical	Worldwide	2011

Table 5: Smart grid or power systems' standards relevant to cyber security applicable to substations.

	Standard	Scope	Type	Range	Pub.
9.	IEEE 1686	Cyber security	Technical	Worldwide	2007
10.	IEEE C37.240	Cyber security	Technical	Worldwide	2014
11.	IEEE 1402	Physical and electronic security	General	Worldwide	2008

Table 6: Smart grid or power systems' standards relevant to cyber security applicable to Industrial Automation and Control Systems (IACS).

	Standard	Scope	Type	Range	Pub.
12.	IEC 62443 (ISA 99)	IACS cyber security	Technical	Worldwide	2009
13.	ISO/IEC 27019	IACS cyber security	General	Worldwide	2013
14.	NIST SP 800-82	IACS cyber security	General	US	2013
15.	DHS Catalog	IACS cyber security	General	US	2009
16.	DHS Cyber Security Procurement Language for Control Systems	Cyber security requirements for procurement	Technical	US	2008

Table 7: Smart grid or power systems' standards relevant to cyber security applicable to Advanced Metering Infrastructure (AMI).

	Standard	Scope	Type	Range	Pub.
17.	Security Profile for AMI	Cyber security	General	US	2010
18.	Privacy and Security of AMI	Security and privacy requirements	General	Netherlands	2010
19.	AMI System Security Requirements	Security requirements for procurement	Technical	US	2008
20.	IEC 62056-5-3	AMI data exchange security	Technical	Worldwide	2016

Table 8: Smart grid or power systems' standards relevant to cyber security applicable to selected smart grid components.

No.	Standard	Scope	Applicability	Type	Range	Pub.
21.	VGB R175	Cyber security requirements for power plants	Power plants	Technical	Germany	2014
22.	IEC 61400-25	Wind power plants-IACS communication	Wind power plants	Technical	Worldwide	2015
23.	IEEE 2030	Energy storage systems' interoperability	Storage	Technical	Worldwide	2015
24.	ISO 15118	Vehicle-grid communication	PEV and relevant comm. infr.	Technical	Worldwide	2014
25.	ISO/IEC 14543	Home Electronic System security	Home Electronic System	Technical	Worldwide	2010/2015

Table 9: General application standards and guidelines which can be adopted to smart grid.

No.	Standard	Scope	Type	Range	Pub.
26.	ISO/IEC 27001 and 27002	IS management	General	Worldwide	2013
27.	NIST SP 800-53	IS management	General	US, worldwide	2013
28.	GB/T 22239	IS management	General	China	2008
29.	ISO/IEC 27005	Risk management	General	Worldwide	2011
30.	NIST SP 800-39	Risk management	General	US	2011
31.	ISO/IEC 15408 / Common Criteria	Security assessments	Technical	Worldwide	2008/2012
32.	ISO/IEC 18045 / CEM	Security assessments	Technical	Worldwide	2008/2012
33.	GB/T 20279	Security requirements for network separation devices	General	China	2015
34.	ISO/IEC 19790	Security requirements for cryptographic modules	General	Worldwide	2012
35.	NIST SP 800-64	Security of systems in development	Technical	US	2008
36.	NIST SP 800-124	Security of mobile devices	General	US	2013

Table 10: Standards that address privacy issues. The level of relevance (high, moderate, low) is indicated.

No.	Standard	Relevance
1.	NISTIR 7628	High
2.	NIST SP 800-53	High
3.	IEC 62443	Mod.
4.	ISO/IEC 27019	Mod.
5.	IEEE 2030	Mod.
6.	Privacy and Security of AMI	Mod.
7.	AMI System Security Requirements	Mod.
8.	NIST SP 800-82	Mod.
9.	ISO/IEC 15408	Mod.
10.	NIST SP 800-64	Mod.
11.	ISO/IEC 27001 and 27002	Low
12.	Security Profile for AMI	Low

properly protected both to maintain competitive advantage and to protect employee privacy." *IEC 62443-1-3*, in Chapter 7, defines IACS privacy metrics such as the number of unauthorised disclosures of non-public IACS personnel information, the number of failures to ensure confidentiality and integrity of IACS personnel records or the number of access violations related to fraudulent statements or counterfeit documents that resulted in the disclosure of IACS data which could be used for financial benefit. *IEC 62443-2-1* specifies (after ISO 27001:2005) the 15.1.4 security requirement "Data protection and privacy of personal information" that imposes data protection and privacy assurance according to relevant legislation, regulations, or contractual clauses. Implementation guidance (not IACS specific) is provided, based on ISO 27002:2005. A similar approach is taken in *ISO/IEC TR 27019* [87].

6.4. IEEE 2030

The smart grid interoperability standard *IEEE Std 2030-2011*, in Chapter 4.5.2 briefly overviews the problem of privacy in smart grids. It explains that privacy regards the various modes of use (collecting, accessing, distributing etc.) of the Personally Identifiable Information (PII), and that various interpretations and definitions of privacy exist. Smart grid, with its new technologies, such as smart meters or smart appliances, introduces new privacy risks that need to be addressed by proper measures, including Privacy Impact Assessments (PIA) performed frequently [106]. A similar description is provided in the *IEEE Std 030.2-2015* [92].

6.5. Privacy and Security of the Advanced Metering Infrastructure

The Dutch guideline *Privacy and Security of the Advanced Metering Infrastructure* [98] consistently with its title addresses both, security and privacy of AMI. According to the document the two concepts partially overlap. As far as the the target of protection is concerned, privacy is narrower in scope, because it focuses on personal data. On the other hand, the protection objectives in privacy are broader than in security as they regard the questions of unnecessary further processing of information or unlawful processing, and satisfying legal requirements that concern the sensitive data. At the same time, to be capable of protecting privacy, security must be assured first. The document defines PII and privacy-sensitive information and identify privacy related goals, risks and requirements [98].

6.6. Other standards that refer to privacy

AMI System Security Requirements [89] include the class of 16 requirements that are oriented towards privacy and confidentiality in AMI. In the description of the AMI system, privacy concerns are indicated in all 4 use cases that are related to billing and 2 ("Customer Prepayment" and "Third Party Energy Management") that regard customer activities. According to the guideline, security objectives in smart grid should include prevention of privacy violations, while privacy questions need to be included into the utility worker education [89].

The IACS orientated *NIST SP 800-82* provides guidance and supplementary or enhancing information on application of the NIST SP 800-53 security and privacy controls to IACS. Chapter 6.2.19 explains that the privacy controls from NIST SP 800-53 are directly applicable to IACS [76].

ISO/IEC 15408 which provides criteria for security evaluation of IT products, in its second part [78] "Security functional components" defines class "FPR: Privacy" of functional requirements that regard privacy understood as protecting users against discovery and misuse of their identity by other users. The class contains 4 families: anonymity, pseudonymity, unlinkability and unobservability [78].

NIST SP 800-64 dedicated to security in software development recommends privacy impact assessments performed during the process of building a new system. It should be determined, usually during security categorisation, whether the system would store or process PII, and if it was, the appropriate measures need to be implemented that include privacy information incident handling and reporting [104].

The newest version of *ISO 27001* defines the security objective 18.1.4 "Privacy and protection of personally identifiable information" (earlier – 15.1.4) which regards the implementation of appropriate policy, controls and procedures to protect the privacy of personal information in accordance to relevant legislation, regulations, or contractual clauses [68]. The security objective is described in more detail in *ISO 27002* [69].

Security Profile for Advanced Metering Infrastructures [88] just mentions privacy when explaining the rationale of the DHS-2.8.9 ("Communication Confidentiality") and DHS-2.9.1 ("Information and Document Management Policy and Procedures") security controls. According to the document confidentiality requirements are necessary to ensure the privacy of customer and business information, while document management policies should help avoiding violations of privacy laws [88].

7. Related work

As mentioned in Section 2, during the literature search smart grid standardisation initiatives were identified that indicated already existent standards relevant to cyber security. The studies are based on expert knowledge and don't aim at scientific completeness of their analyses. Thus they don't indicate a systematic method which would serve for this purpose. In result they provide diverse sets of standards and address the subject from various perspectives.

Additionally to that 8 scientific papers were identified (see Section 2) that focus on identifying smart grid cyber security standards [15, 16, 17, 18, 19, 20, 21, 22].

Ruland et al. [15] overview IEC 62351, IEC 62443, IEC 62541-2, ISO/IEC 27019, NISTIR 7628, NERC CIP and Smart Grid Information Security of CEN-CENELEC-ETSI Smart Grid Coordination Group and compare their focus and the scope of application.

Griffin and Langer [16] explains developing a smart grid security architecture. The approach is strongly based on NISTIR 7628, the Smart Grid Coordination Group's Smart Grid Architecture Model (SGAM) and the Microgrid Security Reference Architecture (MSRA) of Sandia, which are described quite extensively. Additionally several IEC and IEEE standards are indicated. Although the paper is not dedicated to identification or evaluation of standards, the references and descriptions it provides can be useful.

Rosinger and Uslar [17] present five standards' sets (IEC 62351, IEC 62443 / ISA 99, NERC CIP and ISO/IEC 27000) and two national (German) standards (BDEW Whitepaper [107] and *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)* [108]). The standards are categorised depending on the value they add to a particular domain of smart grid (generation, trading, retail, transmission, storage, metering, application).

Kanabar et al. [18] briefly describe smart grid standards for protection, control, and monitoring applications in various areas of power transmission and distribution network. As for security – IEC 62351 and IEEE 1686 are shortly described and NERC CIP, NIST SP 800-53 and NIST SP 800-82 are mentioned.

Goraj et al. [19] overview NERC CIP, IEEE 1686, IEC 62351, NISTIR 7628, CIGRE technical brochures on cyber security and some European cyber security initiatives – in the context of a secure remote access to electrical substations.

Falk and Fries [20] summarise smart grid security standardisation and regulation initiatives including NERC CIP, German BDEW, NIST SGIP and European Smart Grid Joint Working Group, as well as standards and guidelines: NIST SP 1108, NISTIR 7628, ISO/IEC 62351, IEC 61850, ISO/IEC 15118, ISA99, IEEE 1686 and RFC 6272.

Wang et al. very briefly describe eight standards or standards' sets (NISTIR 7628, IEC 61850, GB/T 22239, IEC 62351, ISO/IEC 15408, GB18336, ISO 27001, GB/T 22080) and four standardisation bodies (IEC SG3, IEEE PES, NIST and SGCC) [22].

Among the evaluations, the analysis presented by Wang et al. in [21] is the most systematic. In the first step, the authors perform a literature review based on transparent criteria (standard source, relevance to smart grid cyber security 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 [21].

All these studies expose varying levels of completeness and often address the subject from a specific angle. With the exception of [21], 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.

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

- It provides high assurance of completeness due to the application of a repeatable, systematic and rigorous literature search and analysis method with explicitly defined selection and evaluation criteria (see Section 2 and 3).
- The details of the research method are provided (see Section 2).
- It constitutes an extensive guide through smart grid standards that address cyber security problems – 36 standards and guidelines are described from the security perspective, referred to each other and related to evaluation criteria (see Section 5).
- It comprises the search for and the analysis of privacy related contents in the identified standards. 12 standards that address privacy issues were recognised (see Section 6).
- All the standards are referenced to the IEC smart grid architecture (see Fig. 1).

8. Conclusions

The study revealed a relatively large number of standards relevant to the security of smart grids. The publications vary in scope, from general, discussing more high-level issues without providing details on concrete implementation (e.g. ISO/IEC 27019 or ISO/IEC 27001), to strictly technical (e.g. IEC 62443 or IEC 62056-5-3). Part of them is entirely devoted to cyber security aspects, other refer to cyber security when addressing different smart grid problems. In addition, there are standards not dedicated to smart grid, but indicated as applicable to or even recommended to smart grid. 12 standards describe privacy issues in smart grid.

As far as applicability of the standards is concerned, 19 documents can be applied to all smart grid components (see Table 4. 8 of them are smart grid-oriented standards and 11 of general application. 3 publications regard substations (see Table 5), 5 – Industrial Automation and Control Systems (IACS) (see Table 6), 4 – Advanced Metering Infrastructure (AMI) (see Table 7) and 5 – other selected smart grid components (see Table 8).

References

[1] NIST, NIST Special Publication 1108R2 NIST Framework and Roadmap for Smart Grid Interoperability Standards, Tech. rep., National Institute of Standards and Technology (2012).
URL http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf

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

[3] I. Ghansah, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks, Tech. rep., Sacramento (2012).

[4] R. Leszczyna, M. R. Wrobel, Evaluation of open source SIEM for situation awareness platform in the smart grid environment, in: 2015 IEEE World Conference on Factory Communication Systems (WFCS), IEEE, 2015, pp. 1–4. doi:10.1109/WFCS.2015.7160577.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7160577

[5] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, Cyber Security and Privacy Issues in Smart Grids, IEEE Communications Surveys & Tutorials 14 (4) (2012) 981–997. doi:10.1109/SURV.2011.122111.00145.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6129371

[6] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, A. Trombetta, A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems, Industrial Informatics, IEEE Transactions on 7 (2) (2011) 179–186. doi:10.1109/TII.2010.2099234.

[7] H. Khurana, M. Hadley, D. Frincke, Smart-grid security issues, IEEE Security & Privacy Magazine 8 (1) (2010) 81–85. doi:10.1109/MSP.2010.49.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5403159

[8] H. F. Tipton, M. Krause, Information Security Management Handbook, Sixth Edition, no. c, 2007. doi:10.1201/9781439833032.
URL http://www.amazon.com/Information-Security-Management-Handbook-Sixth/dp/1420090925

[9] R. Von Solms, Information security management : why standards are important, Information Management & Computer Security 7 (1) (1999) 50–57. doi:10.1108/09685229910255223.

[10] S. Purser, Standards for Cyber Security, in: NATO Science for Peace and Security Series - D: Information and Communication Security, IOS Press, 2014, pp. 97–106. doi:10.3233/978-1-61499-372-8-97.
URL http://ebooks.iospress.nl/volumearticle/35722

[11] ETSI, Why we need standards.
URL http://www.etsi.org/standards/why-we-need-standards

[12] J.-N. Ezingeard, D. Birchall, Information Security Standards: Adoption Drivers (Invited Paper), in: P. Dowland, S. Furnell, B. Thuraisingham, X. S. Wang (Eds.), Security Management, Integrity, and Internal Control in Information Systems, Vol. 193 of IFIP International Federation for Information Processing, Springer US, Boston, MA, 2006, pp. 1–20. doi:10.1007/0-387-31167-X.
URL http://www.springerlink.com/index/10.1007/0-387-31167-X

[13] M. Siponen, R. Willison, Information security management standards: Problems and solutions, Information & Management 46 (5) (2009) 267–270. doi:10.1016/j.im.2008.12.007.
URL http://www.sciencedirect.com/science/article/pii/S0378720609000561

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

[15] K. C. Ruland, J. Sassmannshausen, K. Waedt, N. Zivic, Smart grid security an overview of standards and guidelines, Elektrotechnik und Informationstechnik 134 (1) (2017) 19–25. doi:10.1007/s00502-017-0472-8.
URL http://link.springer.com/10.1007/s00502-017-0472-8

[16] R. W. Griffin, L. Langer, Chapter 7 Establishing a Smart Grid Security Architecture, in: Smart Grid Security, 2015, pp. 185–218. doi:10.1016/B978-0-12-802122-4.00007-9.

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

URL http://www.springer.com/us/book/9783642349157#

[18] M. G. Kanabar, I. Voloh, D. McGinn, Reviewing smart grid standards for protection, control, and monitoring applications, in: 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), IEEE, 2012, pp. 1–8. doi:10.1109/ISGT.2012.6175811.
URL http://ieeexplore.ieee.org/document/6175811/

[19] M. Goraj, J. Gill, S. Mann, 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), IET, 2012, pp. 161–161. doi:10.1049/cp.2012.0064.
URL http://digital-library.theiet.org/content/conferences/10.1049/cp.2012.0064

[20] R. Falk, S. Fries, Smart Grid Cyber Security - An Overview of Selected Scenarios and Their Security Implications, PIK - Praxis der Informationsverarbeitung und Kommunikation 34 (4) (2011) 168–175.
URL http://10.0.5.235/piko.2011.037http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=77830990&lang=pl&site=ehost-live&scope=site

[21] Y. Wang, B. Zhang, W. Lin, T. Zhang, Smart grid information security - a research on standards, in: 2011 International Conference on Advanced Power System Automation and Protection, Vol. 2, IEEE, 2011, pp. 1188–1194. doi:10.1109/APAP.2011.6180558.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6180558

[22] Y. Wang, D. Ruan, J. Xu, Analysis of Smart Grid security standards, in: 2011 IEEE International Conference on Computer Science and Automation Engineering, Vol. 4, IEEE, 2011, pp. 697–701. doi:10.1109/CSAE.2011.5952941.
URL http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5952941

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

[24] ENISA, Smart Grid Security: Recommendations for Europe and Member States, Tech. rep., ENISA (2012).

[25] CEN-CENELEC-ETSI JWG, Final report Standards for Smart Grids (2011).
URL ftp://ftp.cen.eu/CEN/Sectors/List/Energy/SmartGrids/SmartGridFinalReport.pdf

[26] Standardisation Management Board Smart Grid Strategic Group (SG3), IEC Smart Grid Standardization Roadmap, Tech. Rep. June, Standardisation Management Board Smart Grid Strategic Group (SG3) (2010).
URL http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf

[27] I. Hauer, Z. A. Styczynski, P. Komarnicki, M. Stotzer, J. Stein, Smart grid in critical situations. Do we need some standards for this? A german perspective, in: 2012 IEEE Power and Energy Society General Meeting, IEEE, 2012, pp. 1–8. doi:10.1109/PESGM.2012.6344975.
URL http://ieeexplore.ieee.org/document/6344975/

[28] M. G. Kanabar, I. Voloh, D. McGinn, A review of smart grid standards for protection, control, and monitoring applications, in: 2012 65th Annual Conference for Protective Relay Engineers, IEEE, 2012, pp. 281–289. doi:10.1109/CPRE.2012.6201239.
URL http://ieeexplore.ieee.org/document/6201239/

[29] CEN-CENELEC-ETSI Smart Grid Coordination Group, SG-CG/M490/H_Smart Grid Information Security, Tech. rep. (2014).

[30] European Commission, M/490 Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment, Tech. rep. (2011).

[31] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Set of Standards Version 3.1, Tech. rep. (2014).

[32] IEC, Smart Grid (2017).
URL http://www.iec.ch/smartgrid/

[33] IEC, Smart Grid Standards Map (2017).
URL http://smartgridstandardsmap.com/

[34] I. Gomez, J. E. Rodriguez, S. Stomff, J. Jimeno, C. Nolle, D2.1 – Smart Grid Standardization Documentation Map, Tech. rep. (2013).

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

[36] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W. H. Chin, Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities, IEEE Communications Surveys & Tutorials 15 (1) (2013) 21–38. doi:10.1109/SURV.2011.122211.00021.
URL http://ieeexplore.ieee.org/document/6129368/

[37] ITU-T, Focus Group on Smart Grid (FG Smart) (2011).

[38] OpenSG, Security Working Group, Tech. rep. (2017).
URL http://osgug.ucaiug.org/utilisec

[39] NIST, NIST SP 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, Tech. rep., Na (2014). arXiv:CODEN: NSPUE2, doi:10.6028/NIST.SP.1108r3.
URL http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf

[40] State Grid Corporation of China, SGCC Framework and Roadmap to Strong & Smart Grid Standards, Tech. rep., State Grid Corporation of China (2010).

[41] SoES – Security of Energy Systems (2017).
URL http://www.soes-project.eu

[42] STARGRID – STandard Analysis supporting smart eneRgy GRID developmen (2017).
URL http://stargrid.eu

[43] Y. Zhang, J. Wang, F. Hu, Y. Wang, Comparison of evaluation standards for green building in China, Britain, United States, Renewable and Sustainable Energy Reviews 68 (2017) 262–271. doi:10.1016/j.rser.2016.09.139.
URL http://linkinghub.elsevier.com/retrieve/pii/S1364032116306499

[44] M. Metheny, Comparison of federal and international security certification standards, in: Federal Cloud Computing, Elsevier, 2017, pp. 211–237. doi:10.1016/B978-0-12-809710-6.00007-X.
URL http://linkinghub.elsevier.com/retrieve/pii/B978012809710600007X

[45] V. Gazis, A Survey of Standards for Machine-to-Machine and the Internet of Things, IEEE Communications Surveys & Tutorials 19 (1) (2017) 482–511. doi:10.1109/COMST.2016.2592948.
URL http://ieeexplore.ieee.org/document/7516570/

[46] ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, Tech. rep. (2016).

[47] K. Beckers, I. Côté, S. Fenz, D. Hatebur, M. Heisel, A Structured Comparison of Security Standards, Springer International Publishing, 2014, pp. 1–34. doi:10.1007/978-3-319-07452-8_1.
URL http://link.springer.com/10.1007/978-3-319-07452-8%7B%5C_%7D1

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

[49] T. M. Overman, T. L. Davis, R. W. Sackman, High assurance smart grid, in: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10, ACM Press, New York, New York, USA, 2010, p. 1. doi:10.1145/1852666.1852734.
URL http://portal.acm.org/citation.cfm?doid=1852666.1852734

[50] T. Sommestad, G. N. Ericsson, J. Nordlander, SCADA system cyber security A comparison of standards, in: IEEE PES General Meeting, IEEE, 2010, pp. 1–8. doi:10.1109/PES.2010.5590215.
URL http://ieeexplore.ieee.org/document/5590215/

[51] C. Kuligowski, Comparison of IT Security Standards, Ph.D. thesis (2009).
URL http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf

[52] K. Kosanke, ISO Standards for Interoperability: a Comparison, in: Interoperability of Enterprise Software and Applications, Springer-Verlag, London, 2006, pp. 55–64. doi:10.1007/1-84628-152-0_6.
URL http://link.springer.com/10.1007/1-84628-152-0%7B%5C_%7D6

[53] V. Arora, Comparing different information security standards : COBIT v s . ISO 27001, Carnegie Mellon University, Qatar (2005) 7–9.
URL https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf

[54] Idaho National Laboratory, A Comparison of Cross-Sector Cyber Security Standards, Tech. rep. (2005).

[55] T. Phillips, T. Karygiannis, R. Huhn, Security Standards for the RFID Market, IEEE Security and Privacy Magazine 3 (6) (2005) 85–89. doi:10.1109/MSP.2005.157.
URL http://ieeexplore.ieee.org/document/1556544/

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

[57] K. Eastaughffe, A. Cant, M. Ozols, 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', IEEE Comput. Soc, 1999, pp. 33–44. doi:10.1109/SESS.1999.766576.
URL http://ieeexplore.ieee.org/document/766576/

[58] M. Metheny, Comparison of Federal and International Security Certification Standards, in: Federal Cloud Computing, Elsevier, 2013, pp. 195–216. doi:10.1016/B978-1-59-749737-4.00007-1.
URL http://linkinghub.elsevier.com/retrieve/pii/B9781597497374000071

[59] DKE, German Roadmap E-Energy / Smart Grid, Tech. rep. (2010).

[60] IEC, Smart Grid.
URL http://www.iec.ch/smartgrid/

[61] ITU-T, Terms of Reference of ITU-T Focus Group on Smart Grid (2010).

[62] ITU-T, Smart Grid Architecture, Tech. rep. (2011).

[63] K. Schwarz, IEEE Utility Communications Architecture (UCA) applies mainstream standard Ethernet, in: Fieldbus Technology, Springer Vienna, Vienna, 1999, pp. 268–275. doi:10.1007/978-3-7091-6421-1_35.
URL http://link.springer.com/10.1007/978-3-7091-6421-1_35

[64] OpenSG Users Group, Open Smart Grid.
URL http://osgug.ucaiug.org/default.aspx

[65] NIST, NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity, Tech. rep., NIST (2014).

[66] NIST, Framework for Improving Critical Infrastructure Cybersecurity (2014). doi:10.1109/JPROC.2011.2165269.
URL papers2://publication/uuid/DD40979D-D391-4678-9601-F14CF1CB8BF5

[67] IEC, IEC/TS 62351-1: Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues (2007).

[68] ISO/IEC, ISO/IEC 27001:2013: Information technology Security techniques Information security management systems Requirements (2013).
URL http://shop.bsigroup.com/ProductDetail/?pid=000000000030313534

[69] ISO/IEC, ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls (2013).

[70] ISO/IEC, ISO/IEC 27005:2011: Information technology Security techniques Information security risk management, Tech. rep., ISO/IEC (2011).

[71] E. Humphreys, Information security management system standards, Datenschutz und Datensicherheit - DuD 35 (1) (2011) 7–11. doi:10.1007/s11623-011-0004-3.
URL http://link.springer.com/10.1007/s11623-011-0004-3

[72] IEEE, IEEE 1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (2007).

[73] ISA, ISA99, Industrial Automation and Control Systems Security (2017).
URL https://www.isa.org/isa99/

[74] GB/T 22239:2008 – Information Security Technology – Baseline for Classified Protection of Information System Security, Tech. rep. (2008).

[75] National Institute of Standards and Technology (NIST), NIST SP 800-53 Rev. 4 Recommended Security Controls for Federal Information Systems and Organizations, U.S. Government Printing Office, 2013.
URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdfhttp://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

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

[77] ISO/IEC, ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, Tech. rep. (2009).
URL http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[78] ISO/IEC, ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components, Tech. rep. (2008).
URL http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[79] ISO/IEC, ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components, Tech. rep. (2008).
URL http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[80] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model Version 3.1 Revision 4, Tech. rep. (2012).

[81] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components Version 3.1 Revision 4 (2012).

[82] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components Version 3.1 Revision 4 (2012).

[83] Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4, Tech. Rep. September (2012).
URL http://www.commoncriteriaportal.org/

[84] ISO/IEC, ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation, Tech. rep. (2008).
URL http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

[85] IEC, IEC 62056-5-3:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer, Tech. rep. (2016).

[86] ISO, ISO 15118-2:2014 Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements, Tech. rep. (2014).

[87] ISO/IEC, 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 (2013).

URL http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759

[88] Advanced Security Acceleration Project, Security Profile for Advanced Metering Infrastructure, Tech. rep. (2010).

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

[90] DHS, Cyber Security Procurement Language for Control Systems Version 1.8, Tech. rep. (2008).

[91] IEC, IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model (2016).

[92] IEEE Standards Coordinating Committee 21, IEEE guide for the interoperability of energy storage systems integrated with the electric power infrastructure, Tech. rep. (2015).
URL http://ieeexplore.ieee.org/document/7140715/

[93] NRC, NRC RG 5.71 Cyber Security Programs for Nuclear Facilities, Tech. rep. (2010).

[94] NIST, NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View, Tech. Rep. March (2011).
URL http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[95] DOE, NIST, NERC, Electricity Subsector Cybersecurity Risk Management Process, Tech. Rep. May (2012).
URL https://www.federalregister.gov/articles/2012/05/23/2012-12484/electricity-subsector-cybersecurity-risk-management-process

[96] DoE, Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, Tech. rep. (2002).

[97] IEEE Power & Energy Society. Power System Relaying Committee., IEEE Power & Energy Society. Substations Committee., Institute of Electrical and Electronics Engineers., IEEE-SA Standards Board., C37.240-2014 – IEEE standard cybersecurity requirements for substation automation, protection, and control systems, Tech. rep. (2014).
URL http://ieeexplore.ieee.org/document/7024885/

[98] Netbeheer Nederland, Privacy and Security of the Advanced Metering Infrastructure, Tech. rep. (2010).

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

[100] GB/T 20279-2015 – Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products, Tech. rep. (2015).

[101] M. Souppaya, K. Scarfone, NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise, NIST special publication (2013) 30doi:10.6028/NIST.SP.800-124r1.

[102] ISO/IEC, ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules, Tech. rep. (2012).

[103] IEEE-SA Standards Board, IEEE 1402 (R2008) – IEEE Guide for Electric Power Substation Physical and Electronic Security, Tech. rep. (2008).

[104] R. Kissel, K. M. Stine, M. A. Scholl, H. Rossman, J. Fahlsing, J. Gulick, NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle, Tech. rep. (2008).
URL http://dl.acm.org/citation.cfm?id=2206279%5Cnpapers2://publication/uuid/D524BF13-D081-4554-AB83-6A82E77E6EC8

[105] F. Baker, D. Meyer, RFC 6272 – Internet protocols for the smart grid, Tech. rep. (2011). doi:ISSN: 2070-1721.
URL http://www.hjp.at/doc/rfc/rfc6272.html

[106] IEEE Standards Coordinating Committee 21, IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, Institute of Electrical and Electronics Engineers, 2011.

[107] BDEW, Requirements for Secure Control and Telecommunication Systems (2015).

[108] H. Kreutzmann, S. Vollmer, Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP) (2014).