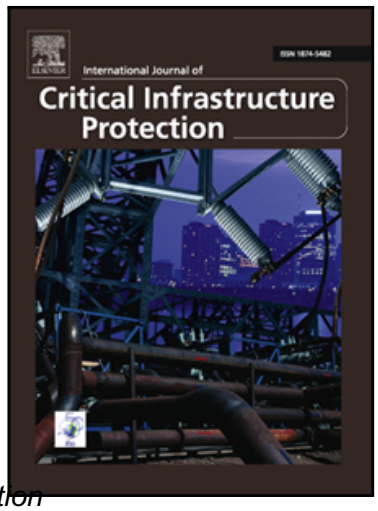

Standards on Cyber Security Assessment of Smart Grid

Rafał Leszczyna

PII: S1874-5482(16)30142-1
DOI: 10.1016/j.ijcip.2018.05.006
Reference: IJCIP 252

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 21 October 2016
Revised date: 21 May 2017
Accepted date: 27 May 2018

Please cite this article as: Rafał Leszczyna, Standards on Cyber Security Assessment of Smart Grid, *International Journal of Critical Infrastructure Protection* (2018), doi: 10.1016/j.ijcip.2018.05.006

Standards on Cyber Security Assessment of Smart Grid

Rafał Leszczyna*

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

Abstract

Security evaluation of communication systems in smart grid poses a great challenge to the developers and operators. In recent years many new smart grid standards were proposed, which paradoxically results in the difficulty in finding a relevant publication in this plethora of literature. This paper presents the results of a systematic analysis which aimed at addressing this issue by identifying standards that present sound security assessment guidance. This should help practitioners in choosing the standards that are applicable to their area. Additionally the contents extracted from the standards can serve as a useful guidance on security assessments of smart grid components.

Keywords: cyber security, security assessment, critical infrastructures, smart grid

1. Introduction

The transformation from traditional power infrastructure to a new form of electricity network called *smart grid* should result in many significant social and technological benefits connected to the decentralised nature of the grid and the utilisation of Information and Communication Technologies (ICT) to enable two-way power and information flows.

From the users' point of view, the smart grid gives the opportunity of actively controlling their energy usage, taking advantage of flexible energy plans and even becoming small-scale electricity suppliers. As for energy providers, it enables time-based pricing, better capacity and energy utilisation planning, and more flexible adjustment to the market demands. The grid enhances energy transmission management and increases resilience to control-system failures [96, 145].

At the same time the intense use of Information and Communication Technologies brings in many new concerns. Smart grid is a collection of different legacy systems surrounded with new technologies and architectural approaches, compliant to different standards and regulations that all need to be combined into one communication network. The interlinked smart grid communication systems have many vulnerabilities that differ across networks [145].

The smart grid interconnection with the Internet exposes the grid to new types of risks, including Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets and zero-days [26, 141, 145, 10]. Stuxnet, Duqu, Red October, or Black Energy are just few examples of modern threats that appeared since 2010 [118, 41, 126, 125, 139, 57]. The new variant of Black Energy threat, called Disakil is being linked to the Ukrainian power outages in December, 2015 [135]. Sophistication of these attacks raises very quickly.

Securing the smart grid requires a multidisciplinary approach that combines various technologies and incorporates managerial, policy, legal aspects and more. The crucial part of this process is formed by security assessment [26, 47, 94] i.e. evaluating the level of security and identifying potential vulnerabilities that can be exploited by attackers.

There is a strong need for the assurance that information technologies embedded in the smart grid will not induce failures or facilitate the intrusion by malicious agents (e.g. hackers, virus). It is also important to understand what is the impact of cyber attacks on power facilities in the smart grid [46].

Operators and security officers seek for systematic security assessment methodologies that can provide the assurance of reliable and secure operation of the grid [92]. Security experts agree that standardised solutions and practices should be used in the first place [137, 140].

In recent years numerous smart grid standards were 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 study presented in this paper aims at addressing this problem by identifying the standards that can be applied to security assessments of smart grid components. Based on a systematic literature review that comprised three main stages, 35 cyber security publications of relevance were identified. To the best of the author's knowl-

*Corresponding author

edge 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 majority of these documents have become *de facto* standards. A de facto standard is a custom, convention, company product, corporate standard, etc. that becomes generally accepted and dominant and is widely used and applied.

In the following sections the concepts of smart grid and security assessments are discussed, the method of the research is described and the results presented. The key part of the paper (see Section: *Results of the analysis*) is dedicated to the demonstration of smart grid standards from the security assessment point of view. There the standards are shortly characterised and the results are summarised in Tables 5 – 8. In Section 7 the topic of industry implementation of the identified standards is discussed. Finally, after the presentation of related work, the paper concludes with closing remarks.

2. Smart grid

The European Commission describes a smart grid as *"an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added"* [24]. The European Smart Grid Task Force defines 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"* [24].

According to the American Department of Energy (DoE) smart grid is 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 smart grid is a new form of electricity network that intensively employs the Information and Communication Technologies (ICT) to enable two-way power and information flows and to create an automated and distributed advanced energy delivery network [96, 145, 43].

In traditional grid, power generation is centralised, while electric infrastructure is built mostly on electromechanical solutions. Monitoring and potential restorations are performed manually, giving the operators only a limited control. In smart grid, on the other hand, power generation centres are distributed and interconnected with a power and communication network based on digital solutions and sensors [43]. The components of the smart grid architecture are illustrated in Fig. 1.

The benefits of smart grid include [106]:

- higher power reliability and quality,
- self-monitoring, self-healing and increased resilience to disruption,
- predictive and automated maintenance and operation,
- facilitated deployment of distributed energy sources including renewable sources,
- wider consumer choice.

However there are also challenges linked to the development of the new domain. Because a smart grid is highly dependent on ICT and interconnected with the Internet, cyber security and privacy concerns arise [96]. Each network connection of the grid opens a potential entry for an attacker, every network layer and the technology used may become his or her possible target. Moreover, as a smart grid is a complex system of systems, it presents a vast attack surface [10].

The new grid is exposed to a large number of cyber-threats which, to make the situation even worse, evolve dynamically. Advanced Persistent Threats (APT), botnets, zero-days or Distributed Denial of Service Attacks (DDoS'es) are examples of threats that emerged or advanced significantly in the last years. Additionally to that, there are completely new threats exclusive to the smart grid domain. These, for instance, include attacks on smart metering systems. Compromising a smart meter opens a way for accessing other smart grid devices, such as smart appliances, smart thermostats, or charging stations – because they are all connected to a communication network. Furthermore, deploying smart grid components at the end user's facilities or in public places exposes them to a nearly 24/7 potential attacker activity [10, 48].

Effective and reliable protection of smart grid is one of the key enablers of its adoption.

3. Security assessment

3.1. Concepts and definitions

Multiple definitions of security assessment can be found in the literature. This section presents the definitions from the analysed standards. Theses definitions are the most acknowledged among the experts of information security.

IEC TS 62351-1 defines security assessment as *"a circular process of assessing assets for their security requirements, based on probable risks of attack, liability related to*

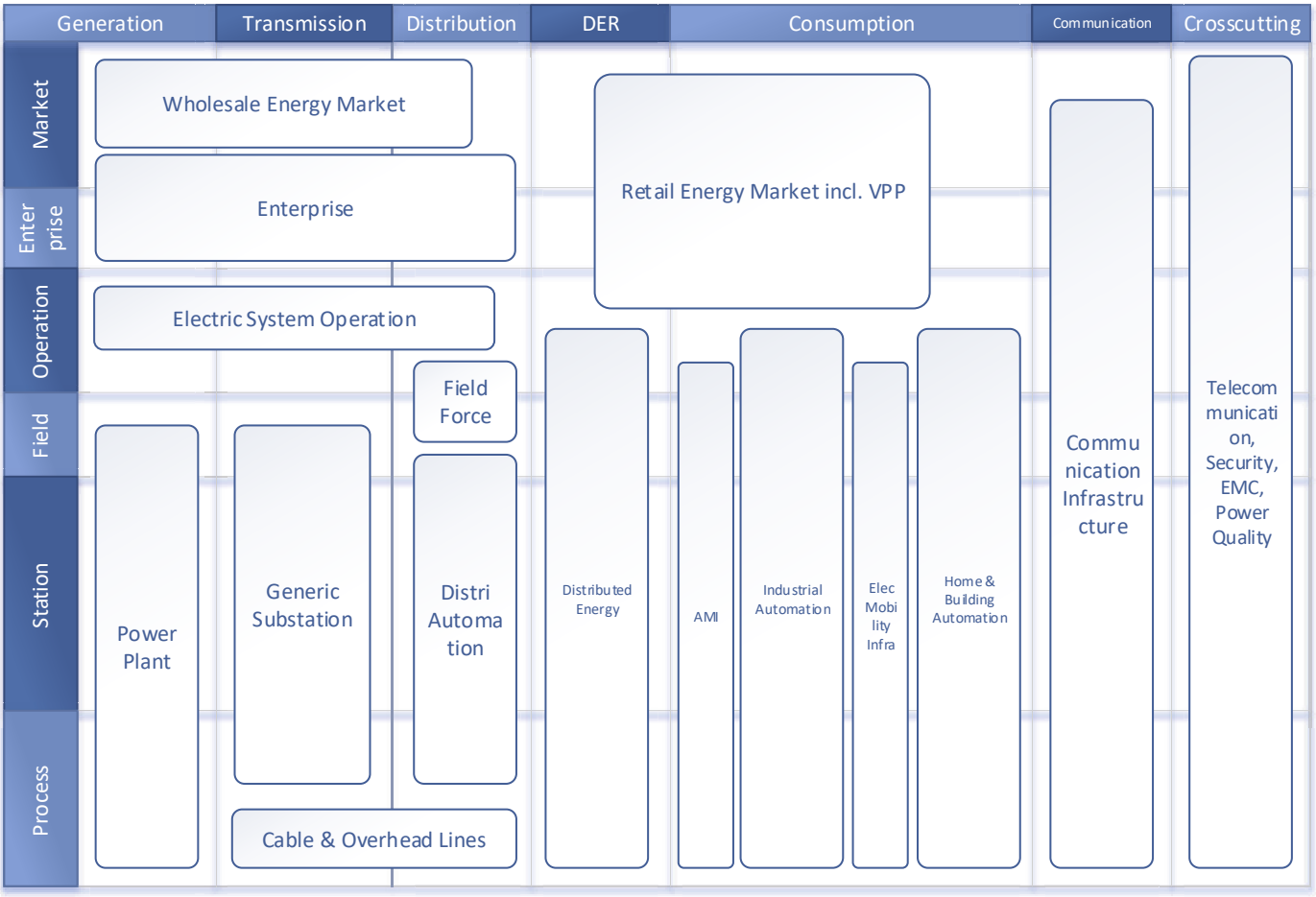

Figure 1: Smart grid components based on the IEC Smart Grid Standards Map [66].

successful attacks, and costs for ameliorating the risks and liabilities." [59]. NIST SP 800-53 equates Security Assessment with Security Control Assessment and defines it as *"the testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system"* [100].

According to the US Department of Homeland Security (DHS), security assessments are based on analysing security controls in the system to *"determine the extent the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system"* [30].

NIST SP 800-115 defines an information security assessment as *"the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, personknown as the assessment object) meets specific security objectives."* The standard distinguishes three types of assessment methods that can be used to accomplish this [123]:

- testing – analysing assessment objects under defined conditions to compare actual and expected behaviours,
- examination – checking, inspecting, reviewing, observing, studying, or analysing assessment objects to clarify, understand or gather required evidence,
- interviewing – discussing with individuals or groups within an organisation to clarify, understand or to identify the location of evidence.

The definitions are very similar. Their common denominator is the understanding of security assessment as a process based on analysis of assets in order to determine if they meet security requirements (or security objectives). NIST SP 800-115 extends the definition with enlisting the methods for security assessment.

Summarising, security assessment is the process of determining how effectively an entity being assessed meets specific security objectives or security requirements. This can be done using three types of methods: testing, examination and interviewing.

3.2. Techniques

Security assessment techniques can be classified into one of the following groups [123]:

- *Reviews* – passive, usually manual, examinations performed to discover security vulnerabilities. They include documentation, log, rules, and configurations reviews, compliance checking, formal analysis, network sniffing and file integrity checking [123, 80, 34, 138].
- *Vulnerability identification* – manual or automated (usually) searches for systems' flaws. Identification techniques include network discovery, port scanning, vulnerability scanning, wireless scanning, and application security examination.
- *Vulnerability analysis* – manual or automated explorations of identified vulnerabilities to ultimately confirm their existence and to elaborate further consequences of their exploitation. Techniques include password cracking, penetration testing, social engineering and application security testing.

Compliance checking determines if systems meet their security objectives or satisfy security requirements. *Network sniffing* is a tool-aided, passive monitoring of network communication and examination of its content to validate whether it is sufficiently protected. *File integrity checking* detects file modifications based on computing of checksums [123, 80].

Formal analysis uses formal logic, discrete mathematics and other mathematically-grounded methods to evaluate security of information systems. The evaluation requires preparing formal specifications of analysed systems, which can be subsequently verified, similarly to verification of mathematical formulae. Formal methods are often equipped with a logical calculus which may be checked systematically by an automated tool [11, 34].

Network discovery is a recognition of network structure usually performed from the outside of its boundary. *Port scanning* enables identifying open communication ports, which are most often the first target of attackers. *Vulnerability scanning* searches for (usually known) software vulnerabilities. It helps in noticing outdated software versions, missing patches or incorrect configurations. *Wireless scanning* examines if wireless networks or communications can be accessed by an unauthorised person [123].

Password cracking aims at discovering passwords based on available data in order to identify weak passwords and password policies. *Penetration testing*, *red teaming* or *white-hat hacking*, or other so-called 'ethical hacking' procedures use hackers' approaches to analyse system vulnerabilities. There is a bottom-up initiative of a group of information security practitioners who developed a penetration testing standard called PTES [102]. A sample description of smart grid cyber security penetration testing performed in a testbed can be found in [25, 95]. *Social engineering* relies on influencing people to take actions that would result in exposing a system to attackers, to verify security procedures and system users' behaviour (user awareness) [123].

Application security examination and testing validates if software applications contain vulnerabilities, operate securely, interact securely with users, other applications and its execution environment [123, 116, 92].

The study presented in this paper aimed at identification of standards and their contents that refer to these questions.

4. Research method

Based on a systematic review of existing literature, the research described in this paper aimed at identification of standards that address the subject of security assessment. The literature survey was based on the approach of Webster and Watson [144]. 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 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 an 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 [121, 53, 120, 85, 52, 40, 143, 142] presented more comprehensive studies.

Literature analysis. The publications identified during 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. [31, 37, 21, 130] were found. The following

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	30 249 (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.

initiatives related to smart grid standardisation were identified [52, 54, 84, 21]:

- CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG) [22, 52],
- European Commission Smart Grid Mandate Standardization M/490 [39, 54],
- German Standardization Roadmap E-Energy / Smart Grid [31],
- IEC Strategic Group 3 Smart Grid [23, 65, 66, 130, 54],
- IEEE 2030 [70, 53, 42, 54],
- ITU-T Smart Grid Focus Group,
- Japanese Industrial Standards Committee (JISC) Roadmap to International Standardization for Smart Grid [21],
- OpenSG SG Security Working Group [114, 42],
- Smart Grid Interoperability Panel [107, 52, 54],
- The State Grid Corporation of China (SGCC) Framework [131, 54].

These activities were primarily dedicated to the development of new standards and guidelines, but also indicated already existing standards relevant to the subject.

From the above initiatives, 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 a Smart Grid Standards Map [66] – an interactive graphical tool that facilitates identification of relationships between standards and smart grid components (see Fig. 1). At the moment as much as 512 standards published by standardisation bodies including IEC, ISO, CISPR, EN, ENTSO, ETSI, ITU-T, W3C, IEEE, IETF and other are registered. The map allowed for indicating to which smart grid components the standards described in this paper are relevant. This is illustrated by the *applicability* criterion described in Section 5. 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.

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
IEC 61850	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

To avoid any duplication of work, first the initiatives and the 8 scientific studies mentioned earlier were analysed in search for standards related to smart grid cyber security. 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 [7, 8]. It became evident that these undertakings address the subject from various perspectives and provide different sets of standards.

Standards selection. Selection criteria described in Section 5 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

cyber security were depicted. These standards were analysed in search of security assessment related contents, such as definitions, guidance, recommendations, requirements and descriptions or references to security assessment techniques (see Section 3.2).

Table 2 presents 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).

5. 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 [121, 146, 98, 45, 38, 18, 133, 115, 128, 90, 127, 88, 12, 58, 117, 91, 36] 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 [133] describes complete literature analysis approach and defines as many 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. [128] 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 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. [18] 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 [127] 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 [12] evaluates standards according to their focus, scope, structure, organisational model etc. Phillips et al. [117] compares technical features (including band, range and data) and security features (confidentiality, integrity, availability). ENISA's evaluation of Privacy Enhancing Technologies [38] distinguishes between maturity and stability, privacy policy implementation and usability. Zhang et. al [146] – objective and measures (idea analysis), Gazis [45] – maturity, layers, arrangement, domain, definitions, audience, etc. Eastaughffe et al. [36] focus on the domain-specific features such as safety management agents, integrity levels, human factors, assurance techniques or post-development issues. Kuligowski [90] 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.

Table 3: Area-specific standards' evaluation criteria.

Criterion	Description
Details	Does the standard describe details of security assessments?
References	Does the standard indicate security assessment methods, techniques, additional guidance?
CT	Does the standard specify security requirements, objectives which can be used in compliance testing?

Another approach is presented in NIST SP 800-29 [91] where the content of documents is compared, section by section. Similarly in the works of Kosanke [88] and Metheny [97] who also present domain-specific comparison criteria. While Ruland et al. [121] and Idaho National Laboratory [58] 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 [133] in his study dedicated to the healthcare sector depicts an impressive number of 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 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 assessments or cyber security.

The area-specific and area-independent *evaluation criteria* which serve in comparing the selected standards are presented in Table 3 and 4.

6. Results of the analysis

The following sections provide a characterisation of the standards from the security assessment point of view. The summary of the analysis is presented in Tables 5 – 8. The standards are described in the order of their recognisability by the smart grid standard identification studies or papers described in Section 4.

Table 4: Area-independent standards' evaluation criteria.

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

6.1. IEC 62351

IEC 62351 ,,Power systems management and associated information exchange – Data and communications security" series is dedicated to information security in power system control operations and in particular to communication protocols defined by IEC TC 57.

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 (2 were withdrawn) provide specific technical requirements.

In IEC 62351-1 the subject of security assessment is shortly introduced, without providing any details or references. According to the standard, security assessment is ''the process of assessing assets for their security requirements, based on probable risks of attack, liability related to successful attacks, and costs for ameliorating the risks and liabilities. The recommendations stemming from the security requirements analysis lead to the creation of security policies, the procurement of security-related products and services, and the implementation of security procedures." [59]

TS 62351-1 perceives security assessment as a circular process which imposes periodical evaluations. The relevant policy must define the re-evaluation period. Besides that, technological and political changes need to be continuously monitored in case an immediate re-assessment was necessary [59].

Other standards in the series don't provide any security assessment guidance. Since they specify requirements related to security, they can be applied in compliance-type of assessments, where protocols are verified if they match the specifications defined there.

IEC TS 62351-1 applies to all components of the smart grid architecture (see Fig. 1) except physical, cable layer. It has a worldwide reach.

6.2. ISO/IEC 27001 and 27002

ISO/IEC 27001 [80] is the most fundamental standard for information security management, acknowledged worldwide and applied by organisations of various profiles (commercial, governmental, not-for profit etc.) and sizes [56]. It is broad in scope, not orientated towards any particular domain, sector or technology. ISO/IEC 27002 provides auxiliary, practical guidance on the implementation of ISO/IEC 27001 [81].

The following ISO 27001 controls refer to security assessments:

- A.14.2.8 System security testing,
- A.18.2.2 Compliance with security policies and standards,
- A.18.2.3 Technical compliance review.

A.18.2.3 requires regular checks of information systems to confirm that information security objectives are achieved. Further implementation guidance regards the way of performing the compliance checking (manual or automated-tools-aided) and the responsible person (a system engineer or a competent and authorised person). Technical compliance review involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented and may include penetration testing and vulnerability assessments, which register the state of a system in a specific time. They might be carried out by independent experts specifically contracted for this purpose. The conditions of penetration tests or vulnerability assessments are outlined [81].

A.18.2.2 imposes periodical checks of compliance with policies and standards. These verifications should be performed by managers. A.14.2.8 requires testing of security functions during software development.

The international standards ISO/IEC 27001 and 27002 can be applied to all components of the smart grid architecture (see Fig. 1). The security controls and objectives defined in the standards can be subject to compliance-based security assessment.

6.3. 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. The series comprises 11 documents subject to enforcement.

NERC CIP-003-6 ,,Cyber Security – Security Management Controls" imposes vulnerability assessments as part of cyber security programs in energy infrastructures [111]. CIP-010-2 [112] ,,Cyber Security – Configuration Change Management and Vulnerability Assessments" specifies requirements for the assessments. According to them the paper or active evaluations need to be conducted at least once every 15 calendar months, the method of assessment should be documented as well as all outcomes. Every 3

years an active assessment should be performed in a production environment in a manner that minimises adverse effects. The choice of assessment method is left to the operator. The standard doesn't indicate any particular methods either.

All 11 NERC CIP standards can be applied to compliance testing. In fact, at the end of each document, compliance monitoring and assessment processes are enlisted such as compliance audits, self-certifications, spot checking, compliance violation investigations, self-reporting and complaints.

NERC CIP can be applied to all components of the smart grid architecture (see Fig. 1).

6.4. 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 [109]. This de-facto standard is applicable to all components of the smart grid architecture (see Fig. 1).

NISTIR 7628 defines the objective of security assessments as verifying *"that the implementers and operators of smart grid information systems are meeting their stated objectives"*. According to the standard, security assessments include monitoring and reviewing the performance of smart grid information systems. To evaluate the effectiveness of the security program internal checking methods, such as compliance audits and incident investigations, should be applied. Additionally, continuous monitoring enables organisations reviewing compliance of their smart grid information systems. If irregularities are identified, corrective actions should be implemented [109].

The standard dedicates a separate family of security requirements to the subject of security assessments, namely – SG.CA family: Security Assessment and Authorisation, which includes the following 6 requirements [109]:

- SG.CA-1 Security Assessment and Authorization Policy and Procedures,
- SG.CA-2 Security Assessments,
- SG.CA-3 Continuous Improvement,
- SG.CA-4 Smart Grid Information System Connections,
- SG.CA-5 Security Authorization to Operate,
- SG.CA-6 Continuous Monitoring.

During security assessments both sides – the assessor's and the organisation's – need to be represented. Key organisation parties are [124]:

- senior management,
- smart grid information system and Industrial Control System (ICS) owners,
- Chief Information Security Officer (CISO).

The outcome of the assessment should provide information about risks related to organisation information which constitutes the basis for the decisions regarding its operation.

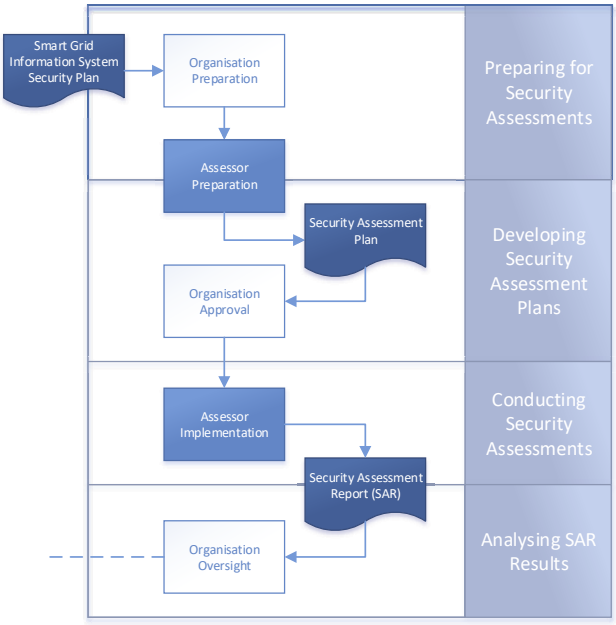

Figure 2: Smart Grid Security Assessment Process defined in [124].

SGIP-CSWG (Smart Grid Interoperability Panel – Cyber Security Working Group) developed the Guide for Assessing the High-Level Security Requirements in NISTIR 7628, Guidelines for Smart Grid Cyber Security [124] and Companion Spreadsheet which constitute a very detailed guideline and a toolbox for evaluating the compliance with NISTIR 7628. The guideline includes [124]:

- explanation of basic concepts,
- description of the security assessment process (see Fig. 2),
- definitions of assessment methods,
- catalogue of assessment procedures,
- an outline of a sample security assessment report.

Additionally a companion spreadsheet tool was developed which covers the catalogue of assessment procedures and enables assessors registering their findings [124].

6.5. IEEE 1686

IEEE Std 1686-2007 ,,IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities" [67] does not include descriptions of or references to security assessments or a security assessment methodology.

6.6. IEC 62443 (ISA99)

IEC 62443 (formerly ISA99) is a set of international standards devoted to the security of Industrial Automation and Control Systems (IACS) which constitute a vital component of smart grids.

IEC/TR 62443-3-1 specifies that IT security personnel should typically scan networks and devices as part of routine vulnerability testing and security assessments [60]. ISA-62443-4-1-WD defines the requirement 14.3 SDSA-SPV-1 – Security Assessment (14.3.1): *"One or more persons shall be appointed to carry out a security assessment in order to arrive at a judgement of the security achieved by the product"* [72]. There are no details on how the security assessment should be executed.

IEC TR 62443-2-3 requires vulnerability assessments performed by suppliers of software patches [62].

The set of standards can be applied to compliance testing of all components of the smart grid architecture (see Fig. 1).

6.7. GB/T 22239

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 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. The security assessment-related content is limited to the requirement of periodical network vulnerability scans. There is no additional guidance on this requirement. The standard can be applied to compliance testing of all components of the smart grid architecture (see Fig. 1).

6.8. NIST SP 800-53

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 ,,Recommended Security Controls for Federal Information Systems and Organizations" [100] is a fundamental NIST document devoted to information security management. Although it has been originally dedicated to US federal agencies, it raised great international interest, and is perceived as defacto standard in the area, adopted and implemented by organisations and enterprises worldwide. It can be applied to all components of the smart grid architecture (see Fig. 1).

NIST SP 800-53 equates Security Assessment with Security Control Assessment and defines it as *"the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization."* [100].

The standard dedicates a separate family of security controls to the subject of security assessments, namely – CA family: Security Assessment and Authorisation [100]. These controls, among others, specify that organisations should periodically evaluate the security controls implemented in their information systems (CA-2) based on earlier defined security assessment plans. This must be done in reference to the security requirements specified for the system and the results need to be documented into a security assessment report. Besides that, the security controls should be monitored on an ongoing basis [100].

Organisations should develop, disseminate, and periodically review/update formal, documented security assessment and authorisation policies and procedures (CA-1). They must define and document remedial actions to correct weaknesses or deficiencies identified during the assessments [100].

Security assessments should be performed already at the stage of software and firmware development (SA family). For that security assessment plans should be defined. Control SA-11 specifies that security assessment plans define the specific activities that developers plan to perform, such as analyses, testing and evaluation, or software reviews. The definitions cover the types of analyses, their depth, accuracy, and coverage, as well as the types of artefacts (by-products) produced during those processes.

Acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been properly applied should be included in contracts. Methods for reviewing and protecting assessment plans, evidence and documentation should correspond with the security category or classification level of the information system [100].

For high-criticality systems (otherwise optional) penetration testing is required to be performed (CA-8). According to the document a common method for penetration testing includes:

- preliminary analysis based on full knowledge of the target system,
- identification of potential vulnerabilities based on the preliminary analysis,
- testing designed to determine the extent to which the identified vulnerabilities can be exploited.

The descriptions of security assessment issues are detailed in NIST SP 800-53 and include enhancements of proposed controls. Moreover references to further publications are provided, namely to (listed in order of relevance) [100]:

- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment [123],
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [28],

- NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans [108],
- NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach [104].

It is worth to note that Revision 4 of NIST SP 800-82 introduces the concept of reciprocity [CNSSI 4009], defined as *"a mutual agreement among participating organisations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information"* [100].

6.9. 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. Like other NIST publications it is widely recognised and adopted worldwide.

Similarly to NIST SP 800-53 the standard dedicates a separate family of security controls to the subject of security assessments, namely – CA family: Security Assessment and Authorisation, which forms a basis for validating and certifying that specified security controls are implemented correctly, operating as intended, and producing the desired outcome [132]. NIST SP 800-82 introduces ICS-specific guidance on (among others) security assessments-related security controls, which was moved from NIST SP 800-53 [132].

Particular recommendations are provided with regard to vulnerability and penetration testing tools. It is advised to carefully evaluate the impacts of these tools on the operation of an ICS, because there have been cases when the additional traffic and exploits used during active vulnerability and penetration testing, combined with the limited resources of many ICS, caused the ICS to malfunction (examples are provided). For this reason a list of recommended vulnerability and penetration testing techniques for ICS has been developed by Sandia National Laboratories (SNL) [35]. The methods on the list are less intrusive, passive instead of active.

The evaluators who perform vulnerability and penetration testing must be informed by the ICS owners about the criticality of continuous operation of the ICS and the risks involved with performing the tests. Another possible risk mitigation strategy is performing the tests in a laboratory setting using the same ICS components as those applied to the industrial processes. However even with very good configuration management to assure that the lab system is highly representative, tests on the actual system are likely to uncover flaws not represented in the laboratory. Certainly the lab tests might be applied to eliminate test procedures potentially harmful to the operational system [132].

Two assessment tools are introduced, namely the Cyber Security Evaluation Tool (CSET) developed by the Department of Homeland Security (DHS) and Samurai Projects Security Testing Framework for Utilities (SamuraiSTFU). CSET aims at helping organisations in protecting their key national cyber assets, by providing a systematic and repeatable approach for checklist-based assessments. SamuraiSTFU is a traditional network penetration testing toolbox. Besides typical testing applications it also includes emulators for ICS, smart meters, and other types of energy sector systems that can be used to perform comprehensive lab tests [132].

For further guidance references to NIST SP 800-115, NIST SP 800-53A, NIST SP 800-37 (see Section 6.8) and NIST SP 800-100 ,,Information Security Handbook: A Guide for Managers" are provided. The de-facto standard can be applied to all components of the smart grid architecture (see Fig. 1) that use IACS.

6.10. 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, 74, 75] 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) [2, 3, 4] 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) [5] on 433 pages explains a 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 [76] and published in 2008. ISO/IEC 15408 and 18045 standards are publicly available without a charge from `http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html`.

6.11. IEC 61850

IEC 61850 ,,Communication networks and systems for power utility automation – Part 10: Conformance testing" [61] does not include descriptions of- or references to- security assessments or a security assessment methodology.

6.12. 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.

DHS recommends that ICS should be authorised for processing before starting their operation and after that – periodically or following any substantial change. According to the guideline each authorisation needs to be accompanied by an assessment of implemented security measures (certification). Security certificates should be renewed on an annual basis. Security assessments need to be also performed before certifications. [30].

In particular, the recommended control 2.18.4: Security Assessments specifies that the security controls should be assessed repeatedly on an organisation-defined frequency (annually – at minimum), to determine the extent of correct implementation of the controls, their intended operation, and whether they produce the desired outcome with respect to meeting the security requirements for the system. The results of the assessment should be registered in a security assessment report. The assessments may include periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises [30].

To satisfy the annual assessment requirement, organisations can use the results from any of the following sources [30]:

- security assessments conducted as part of a system authorisation or reauthorisation process,
- continuous monitoring, or
- testing and evaluation of the system as part of the ongoing system development life-cycle process.

If existing security assessment results are valid they can be reused and supplemented with additional assessments as needed [30].

The selection of security controls for the assessment should be based on [30]:

- the security categorisation of the system (the criticality of the system),
- the specific security controls selected and employed by the organisation, and
- the level of assurance that the organisation must have in determining the effectiveness of the security controls.

Critical controls are assessed annually, other security controls are assessed at least once every three years. Assessments should be performed and documented by qualified and authorised assessors, who understand the information security policies and procedures implemented in the organisation, and the risks associated with a particular facility and/or process. Organisations should assure that assessments do not interfere with ICS functions. In certain cases an ICS may need to be replicated or put into off-line mode to enable an assessment. If a live assessment of an ICS cannot be performed, the organisation should employ compensating controls such as providing a replicated system [30].

Organisations may employ an independent assessor or certification agent, or a team of assessors/certification agents to conduct an impartial assessment of the security controls in the system. Impartiality implies that the assessors are not involved in any conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the control system or to the determination of security control effectiveness. The required level of certifier independence should be decided by the authorising official based on the criticality and sensitivity of the system and the related risks. [30].

In certain situations, for instance if an organisation is small, the assessment cannot be performed by independent experts. In this case the independence of the assessment can be ensured by carefully reviewing and analysing the assessment results by an independent team of experts to validate the completeness, consistency, and veracity of the results [30].

DHS recommended control – 2.18.3: Certification, Accreditation, and Security Assessment Policies requires organisations to develop, disseminate, and periodically review and update formal and documented:

- security assessment and certification and accreditation policies that specify purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance,
- procedures to facilitate the implementation of security assessments and certification and accreditation policies and associated assessment, certification, and accreditation controls [30].

The de-facto standard can be applied to all components the smart grid architecture (see Fig. 1).

6.13. IEC 62056-5-3

IEC 62056-5-3 ,,Electricity metering data exchange – The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer" [63] does not include descriptions of or references to security assessments or a security assessment methodology.

6.14. ISO 15118

The three-part international standard ISO 15118 ,,Road vehicles – Vehicle to grid communication interface" [73] doesn't provide security assessment guidance. Part 2 which defines network and application protocol requirements, including security, can be applied to compliance checking-based assessments of the interfaces between electric vehicles and Electric Vehicle Supply Equipment [73].

6.15. ISO/IEC 27019

ISO/IEC 27019 [82] ,,Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry" aims at assisting organisations from the energy utility industry interpret and apply ISO/IEC 27002 to protect their Industrial Control Systems (ICS). The standard is highly based on ISO/IEC 27002.

The control 15.2 Compliance with security policies and standards, and technical compliance, where in ISO/IEC 27002 penetration tests and vulnerability assessments are mentioned (see section ISO/IEC 27001 and 27002), includes direct reference to the original. Additionally in the Annex B ,,Requirements for Secure Control Systems" it is advised to perform tests of systems, updates, enhancements and security patches in the environments separated from production systems.

All the requirements specified in Annex B can be used for ICS-specific compliance checking in all components of the smart grid architecture (see Fig. 1) that use IACS.

6.16. Security Profile for Advanced Metering Infrastructure

Security Profile for Advanced Metering Infrastructure [9] is a guideline developed by 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 DHS Catalog).

Control DHS-2.10.3 System Monitoring and Evaluation advises regular evaluations of all components of the AMI system for security vulnerabilities and for compliance with its maintenance and security policies. The frequency of evaluations should depend on the organisation's risk management strategy. All vulnerabilities or incompatibilities with security requirements identified during the analyses should result in updates or replacements of the relevant AMI system components [9].

The guideline recommends security analysis of all cryptographic modules applied in the AMI system against the requirements of FIPS 140-2 (Federal Information Processing Standard ,,Security Requirements for Cryptographic Modules"). The most advised solution is to use cryptographic modules validated by the Cryptographic Module Validation Program [110].

6.17. NRC RG 5.71

The US Nuclear Regulatory Commission (NRC) Regulatory Guide 5.71 ,,Cyber Security Programs for Nuclear Facilities" [113] 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 [113].

According to the document, security assessments policies and implementation procedures should be an integral part of the cyber security program. They need to be reviewed annually [113].

Periodical, at least annual, evaluations of security controls conducted as a part of continuous monitoring process aim at validating the existence, correct functioning and effectiveness of security controls required to protect CDA. The effectiveness of security controls is subject to continuous changes due to the volatile threat landscape and system environment. Detected gaps should result in modifications of the cyber security program. Component flaws and malfunctions should be removed [113].

Additionally, all CDA must be scanned for vulnerabilities at minimum once every 3 months or when weaknesses in security controls were detected. Interoperable tools and techniques should be used that automate elements of the vulnerability management process [113].

The standard can be applied to all components of the smart grid architecture (see Fig. 1). It provides reference to a regulatory guide on cyber security self-assessment method for US nuclear power plants (NUREG/CR-6847) [49], however the document is not avaliable publicly [113].

6.18. NIST SP 800-64

NIST SP 800-64 ,,Security Considerations in the System Development Life Cycle" [86] is a guideline dedicated to the US federal agencies which explains how to incorporate good security practices into the life cycle of IT system development.

According to the standard, one of the major activities performed during implementation/assessment phase of the system development is system security assessment (activity 3.3.3.3). Newly developed systems or modifications to existent software/hardware should be formally evaluated before they are authorised for operation. The evaluation is based on compliance checking with functional and security requirements and should follow the assessment procedures described in NIST SP 800-53A ,,Guide for Assessing the Security Controls in Federal Information Systems" [108]. All security controls need to be validated whether they are functional and operating effectively.

NIST SP 800-64 specifies expected deliverables from the process: a security assessment report, plan of action

and milestones, and the updated system security plan. Some implementation advice is provided [86].

6.19. IEEE 1402

IEEE 1402 ,,Guide for Electric Power Substation Physical and Electronic Security" [69] describes security aspects related to the establishment and operation of electric substations. Section 8.5 refers to security assessments, but is dedicated to physical security. The sample security assessment form presented there can be useful as a reference in other types of checklist-based evaluations [69].

6.20. IEEE C37.240

IEEE C37.240 ,,Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems" [68] presents baseline cyber security requirements dedicated to electric substations' communication systems (automation, protection and control). The requirements are moderately technical (present technical solutions but without detailed specifications).

Requirement 6.8 imposes security testing as an integral part of a substation cyber security strategy. The aim of testing is to verify effectiveness of applied security controls in defending against known attacks, but also yet undetected attacks. Indicated testing methods include: reviews of security policies and procedures, penetration testing, physical security audits, vulnerability scanning and reviews of firewall rules. These actions should be performed periodically.

6.21. ISO/IEC 27005

ISO/IEC 27005 ,,Information technology – Security techniques – Information security risk management" [78] is another flagship document from the very popular ISO/IEC 27000 series. It explains the process of risk management, which is particularly suitable for the organisations that comply with ISO/IEC 27001. Though the standard is risk-centric, the guidance on identification of vulnerabilities (part of risk analysis) can be useful in any security assessment. In particular, Annex D ,,Vulnerabilities and methods for vulnerability assessment" provides a list of sample vulnerabilities which can be used in checklist-based assessments, as well as suggests and describes vulnerability assessment methods: automated vulnerability scanning, security testing and evaluation, penetration testing and code review [78]. The standard can be applied to all components of the smart grid architecture (see Fig. 1).

6.22. NIST SP 800-115

NIST SP 800-115 ,,Technical Guide to Information Security Testing and Assessment" [123] provides a systematic and repeatable methodology for performing security assessments which comprises three obligatory phases: planning, execution and post-execution. The document contains comprehensive, detailed descriptions and numerous references to other supportive documents. For this reason this document could be a first choice when seeking for guidance on cyber security assessments in smart grid information systems [123].

The standard describes technical testing and examination techniques that can be used to identify, validate, and assess technical vulnerabilities and assist organisations in understanding and improving the security posture of their systems and networks. In Appendix A references to other security assessment methodologies are provided, including [123]:

- Information Design Assurance Red Team (IDART) [122],
- National Security Agency (NSA) Information Assessment Methodology (IAM) [83],
- NIST security assessment methodology described in NIST SP 800-53A [108],
- Open Source Security Testing Methodology Manual (OSSTMM) [55],
- Open Web Application Security Project (OWASP) Testing Project [99].

The de-facto standard can be applied to all components of the smart grid architecture (see Fig. 1).

6.23. Other standards of relevance to smart grid cyber security assessment

AMI System Security Requirements [20] provides the utility industry and vendors with a set of security requirements for Advanced Metering Infrastructure (AMI) to be used in the procurement process. DHS Cyber Security Procurement Language for Control Systems [29] defines analogous procurement security requirements, but for Industrial Controls Systems.

GB/T 20279 Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products [6] is a national standard which presents technical security requirements for firewalls and similar devices. Dutch guideline ,,Privacy and Security of the Advanced Metering Infrastructure" [101] presents ISO 27001-based security and privacy requirements for AMI. It imposes periodical assessments of security policies based on risk analysis. VGB-Standard ,,IT Security for Generating Plants" [16] specifies security requirements for power plants.

IEC TR 62541-2:2016 ,,OPC unified architecture - Part 2: Security Model" [64] describes the whole security model that includes the description of possible threats to the OPC Unified Architecture (UA) and security functions aiming to mitigate them. An 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.

Table 5: Smart grid or power systems' standards with assessment details. All of them provide general, not technical guidance.

	Standard	Scope	App.	Range	Pub.	Ref.	CT
1.	NISTIR 7628	Smart grid cyber security	All components	US*	2014	[124]	Yes
2.	NIST SP 800-82	IACS security	IACS (SCADA)	US*	2013	CSET, Samurai	Yes
3.	DHS Catalog	IACS security	IACS (SCADA)	US	2009	No	Yes
4.	IEEE 1402	Physical and electronic security	Substations	Worldwide	2008	No	Yes
5.	Energy Infrastructure Risk Management Checklists	Risk management in small/medium facilities	All components	US	2002	No	No
6.	E.S. Cybersecurity Risk Management Process	Risk management in electric sector	All components	US	2012	No	No

* The standard originally aims at US recipients but it is recognised and voluntarily applied worldwide.

Table 6: General application standards and guidelines with assessment details that can be adopted to smart grid.

	Standard	Scope	Applicability	Type	Range	Date	Ref.	CT
7.	NIST SP 800-53	Information security management	Enterprise	General	US*	2013	[123, 28, 108, 104]	Yes
8.	ISO/IEC 15408 *(Common Criteria)*	Security evaluation criteria	IT products (hardware and software)	Technical	Worldwide	2008 *(2012)*	[5]	No
9.	ISO/IEC 18045 *(CEM)*	Security evaluation method	IT products (hardware and software)	Technical	Worldwide	2008 *(2012)*	[77, 74, 75]	No
10.	ISO/IEC 27005	Risk management	Enterprise	General	Worldwide	2011	No	Yes
11.	NIST SP 800-39	Risk management	Enterprise	General	US	2011	No	No
12.	NIST SP 800-64	Cyber security	Systems in development	Technical	US	2008	[108]	Yes
13.	NIST SP 800-115	Cyber security testing and assessment	All components	Technical	US	2008	[122, 83, 108, 55, 99]	Yes

* The standard originally aims at US recipients but it is recognised and voluntarily applied worldwide.

ISO/IEC 19790:2012 ,,Information technology – Security techniques – Security requirements for cryptographic modules" [79] defines security prerequisites for cryptographic modules used in security systems that protect sensitive information in computer and telecommunication systems.

RFC 6272 ,,Internet protocols for the smart grid" [13] identifies key Internet protocols to be used in a smart grid. It contains references to the security assessment documents of TCP and IP protocols.

NIST SP 800-124 ,,Guidelines for Managing the Security of Mobile Devices in the Enterprise" [129] points out to NIST SP 800-115 for security assessment guidance. It recommends periodical validations whether passive (e.g. reviewing logs), or active (e.g. vulnerability scans or penetration testing).

IEEE Std 2030.2-2015 ,,Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure" [71] dedicates its Chapter 8 to the subject of security and security in energy storage systems. It advises periodical tests of all security controls, mechanisms, and procedures by performing analyses of technology implemented in systems or devices, their security features and capabilities as well as penetration testing. The latter is recommended to be conducted in a timeframe when there is possibly the least impact on industrial processes.

6.24. Other standards of relevance to smart grid cyber security

US Department of Energy (DoE) ,,Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities" [32] presents complete checklist-based approach to risk management for small- and medium-scale energy facilities, such as municipal and independent utilities, or rural cooperatives.

A risk management methodology dedicated to the electricity sector is described in ,,Electricity Subsector Cybersecurity Risk Management Process" [33] collaboratively developed by US DoE, NIST and NERC. The methodology is highly based on the 'general-purpose' risk man-

Table 7: Smart grid, power systems or IACS standards that include some security assessment content, but no details.

	Standard	Scope	Applicability	Type	Range	Pub.	Ref.	CT
14.	IEC 62443 (ISA 99)	Security of IACS	All components	Technical	World-wide	2009	No	Yes
15.	Cyber Security Procurement Language	IACS security requirements for procurement	IACS (SCADA)	Techn.	US	2008	No	Yes
16.	NRC RG 5.71	Cyber security of nuclear infrastructures	All components	General	US	2010	[49]*	Yes
17.	VGB R175	Cyber security requirements for power plants	All components	Technical	Germany	2014	No	Yes
18.	Privacy and Security of AMI	AMI security and privacy requirements	AMI	General	Netherlands	2010	No	Yes
19.	NERC CIP	Bulk power system cyber security	All components	General	US	2013	No	Yes
20.	AMI System Security Requirements	cyber security requirements for procurement	AMI	Technical	US	2008	No	Yes
21.	IEEE 2030	Energy storage systems' interoperability	Storage	Technical	World-wide	2015	No	No
22.	IEEE C37.240	Cyber security of communication systems	Substations	Technical	World-wide	2014	No	Yes
23.	IEC 62351	Security of communication protocols	All components	Technical	World-wide	2007	No	Yes
24.	Security Profile for AMI	Power systems' AMI security	AMI	General	US	2010	[103, 110]	Yes
25.	ISO/IEC 27019	power systems' IACS security	Operation, enterprise, market	General	World-wide	2013	No	Yes
26.	ISO 15118	Vehicle-grid communication	PEV and relevant comm. infr.	Technical	World-wide	2014	No	Yes
27.	RFC 6272	Identification of Internet protocols for s. grid	Smart grid communication	Technical	World-wide	2011	[50, 51]	Yes
28.	IEEE 1686	Cyber security	Substations	Technical	World-wide	2007	no	Yes

Table 8: General application standards and guidelines which can be adopted to smart grid that include some security assessment content, but no details.

29.	Standard	Scope	Range	Pub.	Ref.	CT
30.	ISO/IEC 27001 and 27002	IS management	Worldwide	2013	No	Yes
31.	GB/T 22239	IS management	China	2008	No	Yes
32.	GB/T 20279	Security requirements for firewalls and similar devices	China	2015	No	Yes
33.	ISO/IEC 19790	Security requirements for cryptographic modules	Worldwide	2012	No	Yes
34.	NIST SP 800-124	Cyber security of mobile devices	US	2013	[123]	Yes
35.	IEC 62541	OPC UA security model	Worldwide	2016	No	Yes

agement process described in NIST SP 800-39 ,,Managing Information Security Risk" [105].

6.25. Summary and comparison of standards

Tables 5 – 8 illustrate main features of the standards according to the criteria described in Section 5.

7. Industry adoption of the standards

An interesting question regarding the identified standards is the status of their actual implementation by the industry. This regards such factors as the level of standards' adoption, time of the implementation process, costs and perceived benefits, as well as which standards are implemented or which barriers in the implementation process

are encountered by organisations etc.

To answer these questions a literature analysis was performed for the 13 most relevant standards (see Table 5 and 6). The same scientific databases as in the main part of the survey (see Table 1) and the Internet public resources were searched for keywords "NISTIR 7628 implementation", "NISTIR 7628 adoption", "NIST SP 800-82 implementation" etc. as well as "smart grid standards implementation" and "smart grid standards adoption". The results show that the available data on this subject are very scarce.

NERC CIP standards are applied by electric utilities in the U.S. due to the legal obligation imposed by the Federal Energy Regulatory Commission (FERC) [14, 44, 87]. Das et al. [27] indicate however that this process concerns only the bulk power system (electricity generation and transmission) as FERC does not have authority to regulate other participants of the electricity sector. In consequence the others do not feel obligated to improve cyber security of their systems.

Bartnes Line et al. [15] analysed the status of cyber security management practices in small and large Norwegian distribution system operators (DSOs). According to the interviews-based survey, the perception of cyber security risk among the operators and preparedness is low. This in particular concerns small electricity distribution system operators, who declare the ability of withstanding the worst-case cyber threat scenarios, despite being highly dependent on their suppliers when experiencing cyber security incidents. They do not perceive themselves as a possible target of an attack, because in their opinion, larger operators are more attractive for attackers. Although the study does not research the standards' adoption level per se, it indicates the factors that could influence it.

Wiander [19] conducted a study, based on semi-structured interviews, to determine implementation experiences of ISO/IEC 17799 (the predecessor of ISO/ IEC 27002) in 4 organisations (profile not specified in the paper). One of the findings was that employees had a positive attitude towards introducing information security management system as long as the change did not affect them personally. From that moment their attitude changed to reluctance, which according to the study, resulted from uncertainty and lack of information. Similarly, Sussy et al. [134] describe the status of ISO/IEC 27001 implementation in Peruvian public organisations and identify critical success factors. The results are validated by case studies in 5 organisations. These studies are not, however, oriented towards the electricity sector.

Some surveys non-specific to the electricity sector are available [136, 119]. According to the survey of Tenable Network Security which covered 338 IT and security professionals in the U.S. [136], 84% of all organisations adopt a cyber security framework. The most popular frameworks include ISO/IEC 27001/27002 and NIST Framework for Improving Critical Infrastructure Cybersecurity. As far as the utilities sector is concerned, only 5% of respondents declared the use of a cyber security framework. A similar survey conducted in the U.K. (243 respondents) [119] again indicates ISO/IEC 27001 as the most commonly adopted standard (≈22%). Also in the scientific literature a common view that ISO/IEC 27001 is a "widely adopted" standard is shared [87, 143, 93].

The analysis shows that the topic is not adequately elaborated in the existing literature despite its undoubted significance. The need for further research is evident.

8. Related work

As mentioned in Section 4, during 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 4) that focus on identifying smart grid cyber security standards [121, 53, 120, 85, 52, 40, 143, 142].

Ruland et al. [121] 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 [53] explain 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 [120] present five standards' sets (IEC 62351, IEC 62443 / ISA 99, NERC CIP and ISO/IEC 27000) and two national (German) standards (BDEW Whitepaper [17] and *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)* [89]). 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. [85] 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. [52] 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 [40] 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) [142].

Among the evaluations, the analysis presented by Wang et al. in [143] 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 [143].

All these studies expose varying levels of completeness and often address the subject from a specific angle. With the exception of [143], 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 cyber security assessment of smart grid components.

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

- It is dedicated to cyber security assessment – 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 explicitly defined selection and evaluation criteria (see Section 5).
- The details of the research method are provided (see Section 4).
- It provides comprehensive guidance on security assessments in smart grid standards – 35 standards and guidelines are described from the security assessment perspective, referred to each other and related to evaluation criteria.
- All the standards are referenced to the IEC smart grid architecture (see Fig. 1).

9. Conclusions

The study shows that a smart grid standard on cyber security assessments has not been specified so far. Cyber security related standards for smart grid address the issue to various extent and in different ways.

There are 6 smart grid or power systems' standards that provide more information on security assessment processes which can be applied to IACS, substations or all smart grid components (see Table 5). The standards provide rather general guidance, without technical specifications. They can be used as a point of reference for higher-level activities, such as deriving security assessment policies, assigning responsibilities or scheduling security assessment actions. Four of them can be used in compliance testing. Refere CSET, Samurai and [124].

More detailed, general and technical information is provided in 7 standards of wide applicability (enterprises, IT products), not particularly intended for smart grid (see Table 6). These standards can be applied to the enterprise level of smart grid as well as to all its components that use communication technologies and process information. Besides the guidance provided in the standards, multiple references to further literature, which describes additional methods and tools are included. Among them NIST SP 800-115 stands out as the most comprehensive source of security assessment guidance. It defines a three-tier security assessment methodology, describes several assessment techniques, and provides references to further literature and approaches [122, 83, 108, 55, 99]. This document could be a first choice when seeking for guidance on cyber security assessments in smart grid information systems.

The remaining 21 publications which to lesser or greater extent refer to security assessments don't provide details on that subject. Again they can be used for high-level decisions that regard, for instance, type or frequency of assessments. The majority of them can be used in compliance testing.

References

[1] (2008). GB/T 22239:2008 – Information Security Technology – Baseline for Classified Protection of Information System Security. Technical report.
[2] (2012). Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model Version 3.1 Revision 4. Technical report.
[3] (2012). Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components Version 3.1 Revision 4.
[4] (2012). Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components Version 3.1 Revision 4.
[5] (2012). Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4. Technical Report September.
[6] (2015). GB/T 20279-2015 – Information Security Technology – Security Technical Requirements of Network and Terminal Separation Products. Technical report.
[7] (2017a). SoES – Security of Energy Systems.
[8] (2017b). STARGRID – STandard Analysis supporting smart eneRgy GRID developmen.
[9] Advanced Security Acceleration Project (2010). Security Profile for Advanced Metering Infrastructure. Technical report.
[10] Aillerie, Y., Kayal, S., Mennella, J.-p., Samani, R., Sauty, S., and Schmitt, L. (2013). Smart Grid Cyber Security.

[11] Anwar, Z. and Campbell, R. (2008). Automated Assessment Of Compliance With Security Best Practices. pages 173–187. Springer, Boston, MA.

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

[13] Baker, F. and Meyer, D. (2011). RFC 6272 – Internet protocols for the smart grid. Technical report.

[14] Bao Le and Jenkins, B. (2012). Progress in electric utilities risk management - emerging guidance. In *2012 Rural Electric Power Conference*, pages C5–1–C5–4. IEEE.

[15] Bartnes Line, M., Anne Tøndel, I., and Jaatun, M. G. (2016). Current practices and challenges in industrial control organizations regarding information security incident management Does size matter? Information security incident management in large and small industrial control organizations. *International Journal of Critical Infrastructure Protection*, 12:12–26.

[16] 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.

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

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

[19] Wiander T., Association for Computing Machinery., Australian Computer Society., and Australasian Computer Science Week (2008 : Wollongong, N. (2008). Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. In *Proceedings of the sixth Australasian conference on Information security - Volume 81*, page 121. Australian Computer Society, published in association with the ACM Digital Library.

[20] 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.

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

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

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

[24] 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.

[25] Coppolino, L., D'Antonio, S., Elia, I. A., and Romano, L. (2011). Security Analysis of Smart Grid Data Collection Technologies. pages 143–156. Springer, Berlin, Heidelberg.

[26] Coppolino, L., D?Antonio, S., and Romano, L. (2014). Exposing vulnerabilities in electric power grids: An experimental approach. *International Journal of Critical Infrastructure Protection*, 7(1):51–60.

[27] Das, S. K., Kant, K., Zhang, N., Cárdenas, A. A., and Safavi-Naini, R. (2012). Chapter 25 Security and Privacy in the Smart Grid. In *Handbook on Securing Cyber-Physical Critical Infrastructure*, pages 637–654.

[28] Dempsey, K., Chawla, N. S., Johnson, A., Johnston, R., Jones, A. C., Orebaugh, A., Scholl, M., and Stine, K. (2011). NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Technical report.

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

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

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

[32] DoE (2002). Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities. Technical report.

[33] DOE, NIST, and NERC (2012). Electricity Subsector Cybersecurity Risk Management Process. Technical Report May.

[34] Dondossola, G. (1999). *Formal Methods for the engineering and certification of safety-critical Knowledge Based Systems*, pages 113–130. Springer US, Boston, MA.

[35] Duggan, D. P. (2005). Penetration Testing of Industrial Control Systems. Technical report, Sandia National Laboratories, Albuquerque.

[36] 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.

[37] ENISA (2012). *Smart Grid Security: Recommendations for Europe and Member States*.

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

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

[40] 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.

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

[42] 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.

[43] 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.

[44] Flick, T., Morehouse, J., Flick, T., and Morehouse, J. (2011). Chapter 4 Federal Effort to Secure Smart Grids. In *Securing the Smart Grid*, pages 49–72.

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

[46] Genge, B., Kiss, I., and Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, 10:3–17.

[47] Genge, B., Siaterlis, C., Nai Fovino, I., and Masera, M. (2012). A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers & Electrical Engineering*, 38(5):1146–1161.

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

[49] Glantz, C. S., Coles, G. A., and Bass, R. B. (2004). NUREG/CR-6847 – Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants. Technical report.

[50] Gont, F. (2009). Security Assessment of the Transmission Control Protocol (TCP).

[51] Gont, F. (2011). RFC 6274 – Security Assessment of the Internet Protocol Version 4.

[52] 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.

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

[54] 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.

[55] Herzog, P. (2010). OSSTMM 3 - The Open Source Security Testing Methodology Manual. Technical report, ISECOM.

[56] Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit - DuD*, 35(1):7–11.

[57] ICS-CERT (2014). Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (Update B).

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

[59] IEC (2007). 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.

[60] IEC (2009). IEC/TR 62443-3-1: Industrial communication networks Network and system security Part 3-1: Security technologies for industrial automation and control systems.

[61] IEC (2012). IEC 61850-10 Ed. 2.0 b:2012 Communication networks and systems for power utility automation – Part 10: Conformance testing. Technical report.

[62] IEC (2015). IEC TR 62443-2-3: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment.

[63] IEC (2016a). IEC 62056-5-3:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer. Technical report.

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

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

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

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

[68] 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.

[69] IEEE-SA Standards Board (2008). IEEE 1402 (R2008) – IEEE Guide for Electric Power Substation Physical and Electronic Security. Technical report.

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

[71] IEEE Standards Coordinating Committee 21 (2015). IEEE guide for the interoperability of energy storage systems integrated with the electric power infrastructure. Technical report.

[72] ISA (2013). ISA-62443-4-1: Security for industrial automation and control systems Part 4-1: Product Development Requirements, Draft 1.

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

[74] ISO/IEC (2008a). ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components. Technical report.

[75] ISO/IEC (2008b). ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components. Technical report.

[76] ISO/IEC (2008c). ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation. Technical report.

[77] ISO/IEC (2009). ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. Technical report.

[78] ISO/IEC (2011). ISO/IEC 27005:2011: Information technology Security techniques Information security risk management. Technical report, ISO/IEC.

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

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

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

[82] ISO/IEC (2013c). 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.

[83] Johnson, B. C. (2004). National Security Agency (NSA) INFOSEC Assessment Methodology (IAM). Technical report, SystemExperts Corporation.

[84] 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.

[85] 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.

[86] Kissel, R., Stine, K. M., Scholl, M. A., Rossman, H., Fahlsing, J., and Gulick, J. (2008). NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle. Technical report.

[87] Knapp, E. D., Langill, J. T., Knapp, E. D., and Langill, J. T. (2015). Chapter 13 Standards and Regulations. In *Industrial Network Security*, pages 387–407.

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

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

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

[91] 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.

[92] Leszczyna, R., Fovino, I. N., and Masera, M. (2011). Approach to security assessment of critical infrastructures' information systems. *IET Information Security*, 5(3):135.

[93] Line, M. B., Tondel, I. A., and Jaatun, M. G. (2014). Information Security Incident Management: Planning for Failure. In *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, pages 47–61. IEEE.

[94] Liu, N., Zhang, J., Zhang, H., and Liu, W. (2010). Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM. *IEEE Transactions on Power Delivery*, 25(3):1492–1500.

[95] Masera, M., Fovino, I. N., and Leszczyna, R. (2008). Security Assessment Of A Turbo-Gas Power Plant. pages 31–40. Springer, Boston, MA.

[96] McDaniel, P. and McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy Magazine*, 7(3):75–77.

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

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

[99] Meucci, M. (2008). OWASP Testing Guide. Technical report, OWASP Foundation.

[100] 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.

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

[102] Nickerson, C., Kennedy, D., Riley, C. J., Smith, E., Amit, I. I., Rabie, A., Friedli, S., Searle, J., Knight, B., Gates, C., McCray, J., Perez, C., Strand, J., Tornio, S., Percoco, N., Shackelford, D., Smith, V., Wood, R., and Remes, W. (2017). Penetration Testing Execution Standard.

[103] NIST (2001). FIPS 140-2, Security Requirements for Cryptographic Modules. Technical Report 2.

[104] NIST (2010). NIST SP 800-37 Rev. 1 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach. Technical report.

[105] NIST (2011). NIST SP 800-39 Managing Information Security Risk Organization, Mission, and Information System View. Technical Report March.

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

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

[108] NIST (2014b). NIST SP 800-53A Rev. 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans. Technical Report December 2014.

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

[110] NIST (2017). Cryptographic Module Validation Program (CMVP).

[111] North American Electric Reliability Corporation (2013a). CIP-003-6 Cyber Security Security Management Controls. Technical report, North American Electric Reliability Corporation.

[112] North American Electric Reliability Corporation (2013b). CIP-010-2 Cyber Security Configuration Change Management and Vulnerability Assessments. Technical report, North American Electric Reliability Corporation.

[113] NRC (2010). NRC RG 5.71 Cyber Security Programs for Nuclear Facilities. Technical report.

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

[115] 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.

[116] Peake, C. (2003). Red Teaming: The Art of Ethical Hacking. Technical report.

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

[118] Piggin, R. (2016). Cyber security trends: What should keep CEOs awake at night.

[119] PwC (2013). UK Cyber Security Standards. Technical report.

[120] 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.

[121] 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.

[122] Sandia National Laboratories. The IDART Methodology.

[123] Scarfone, K., Souppaya, M., Cody, A., and Orebaugh, A. (2008). NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

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

[125] Shakarian, P., Shakarian, J., and Ruef, A. (2013). *Introduction to Cyber-warfare*. Elsevier.

[126] Shi, X., Li, Y., Cao, Y., and Tan, Y. (2015). Cyber-physical electrical energy systems: challenges and issues. *CSEE Journal of Power and Energy Systems*, 1(2):36–42.

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

[128] 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.

[129] Souppaya, M. and Scarfone, K. (2013). NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST special publication*, page 30.

[130] 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).

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

[132] 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.

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

[134] Sussy, B., Wilber, C., Milagros, L., and Carlos, M. (2015). ISO/IEC 27001 implementation in public organizations: A case study. In *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE.

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

[136] Tenable (2016). Trends in Security Framework Adoption: A Survey of IT and Security Professionals. Technical report.

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

[138] Vaidya, B., Makrakis, D., and Mouftah, H. (2013). Secure communication mechanism for ubiquitous Smart grid infrastructure. *The Journal of Supercomputing*, 64(2):435–455.

[139] Virvilis, N. and Gritzalis, D. (2013). The Big Four - What We Did Wrong in Advanced Persistent Threat Detection? In *2013 International Conference on Availability, Reliability and Security*, pages 248–254. IEEE.

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

[141] Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371.

[142] 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.

[143] 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.

[144] 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.

[145] Yan, Y., Qian, Y., Sharif, H., and Tipper, D. (2012). A Survey on Cyber Security for Smart Grid Communications. *IEEE Communications Surveys & Tutorials*, 14(4):998–1010.

[146] 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.