Standards with Cybersecurity Controls for Smart Grid – a Systematic Analysis

Rafał Leszczyna

Faculty of Management and Economics, Gdańsk University of Technology, Gdańsk, Poland

Correspondence
Rafał Leszczyna, Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland.
Email: rle@zie.pg.gda.pl

Summary

In recent years numerous standards related to the cybersecurity of smart grids have been published, which led to the challenge for operators in obtaining indications that match their specific objectives and contexts. Although several studies approached this problem by providing more or less comprehensive surveys and overviews of smart grid cybersecurity standards, none of them was dedicated to the actual and important subject of cybersecurity controls. This paper aims at filling this gap. A systematic literature analysis was conducted which resulted in the identification of nineteen broadly recognised standards that specify cybersecurity controls applicable to the smart grid infrastructure. The publications are described in respect to the con-trols they define and referred to evaluation criteria. In result this paper constitutes a guideline on standardised cybersecurity controls for smart grids, where (criteria-based) indications help to select standards for a particular smart grid area or specific goals. The method of the research as well as the standards' selection and evaluation criteria are presented.

KEYWORDS:
cybersecurity, security controls and measures, smart grid, standards, industrial control systems, industrial automation, substations, AMI, critical infrastructures

1 | INTRODUCTION

Assuring smart grid cybersecurity requires novel, multidisciplinary approaches that combine traditional and pioneering technologies and address non-technical aspects including managerial, policy or legal[1,2]. It is recommended to apply standardised solutions and practices in the first place[3,4] as they were elaborated during a systematic, multiple-stage standard development process and elected by consensus of numerous domain-experts coming from various environments and often different parts of the world. In comparison to proprietary, "expert knowledge"-based solutions, standards offer the advantage of high assurance of completeness and maturity, as well as other quality-related characteristics.

During the last decade a large number of smart grid standards have been published, which leads to the situation that operators lose orientation in this abundance of literature. Especially if they are at the beginning of standard-based improvement process. The research described in this paper contributes to resolving this problem by identifying standards that define controls for protecting cyber-physical and information systems in the smart grid. *Cybersecurity controls* are the (technical and non-technical) safeguards or countermeasures (processes, policies, devices, practices, or other actions) that aim at protecting a system or assets from cyberattacks and modify cybersecurity risks[5,6]. This paper brings in all the standards that describe cybersecurity controls applicable to smart grids into one place and characterises them in regard to the controls. This is based on a structured

TABLE 1 The summary of literature identification.

Source	All metadata	Title	Abstract	Keywords	In-depth review	Relevant
ACM DL	26	0	16	1	8	6
Elsevier SD	7,114	0	37	4	10	10
IEEE Xplore	602	3	184	17	37	27
Springer	3,190	0	n.a.	n.a.	17	5
Wiley	3,683	3	34	3	8	4
EBSCOhost	265	5	123	6	22[1]	20[1]
Scopus	7,054	5	338	178	35	16
WoS	258[2]	3	n.a.	n.a.	39[1]	23[1]
Total	22,192	19	732	209	176	112

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

[2] Only *Topic* was analysed due to unavailability of *all metadata* option.

analysis that follows up the approach and the findings of the author's earlier studies, which addressed smart grid cybersecurity-related standards in general[7], specifications of cybersecurity requirements[8] and cybersecurity assessments for smart grids[9]. Also (criteria-based) indications are provided that aim at helping the operators to choose the standards which are applicable to their area and that address their individual goals. This is to altogether constitute a comprehensive guideline on standardised cybersecurity controls for smart grids. As an outcome of systematic, three-stage literature analysis, 19 relevant standards or de-facto standards were identified.

In the following sections, the method of the research together with standards' selection and evaluation criteria are described. Section 3 presents the standards that operators can take as a reference when establishing protection measures in the smart grid. Section 4 is dedicated to the multilateral analysis that embraces the relationships between the controls in the identified standards, covered smart grid areas and cybersecurity domains. Finally, after discussing related studies, concluding remarks are brought in.

2 | RESEARCH METHOD

The analysis followed the systematic method of Webster and Watson[10], which aims at completeness and repetitiveness of the review process. In the approach, a literature search begins with the analysis of the most established literature sources, article databases and proceedings. After that, citations in the identified documents are reviewed to determine earlier publications of relevance. This step is called *backward analysis*. In the following stage, i.e. *forward analysis*, the documents that refer to the main articles recognised in the previous steps are searched for, using a scientific database. The approach is concept-centric – concepts determine the organisation of a literature analysis as well as its closure (no new concepts are found)[10]. The study comprised three key stages – the *literature identification*, *literature analysis* and *standards' selection*.

Literature identification. At this stage, a search for the key phrases: "smart grid", "security" and "standard" was performed in the resources of the most recognised publishers in the area of computer science, cybersecurity, electric power systems etc. as well as in cumulative databases that store information from various publishers. In the first attempt, 22,192 documents were found for which any of metadata matched the key phrases. To delimit the number of results, in the second attempt, the searching concerned only publications' titles, keywords and abstracts. This resulted in around 700 documents. Reading the descriptions of these publications allowed for distinguishing 176 publications that appeared relevant to the study. Further analysis, which included browsing the documents' contents, ended with the designation of 112 papers that describe standards related to smart grid cybersecurity (see Table 1). Among them, 10 studies[11,12,13,14,15,16,17,18,19,20] included more comprehensive results, while the majority only referred to some standardisation initiatives or standards.

Literature analysis. This stage aimed at identification of smart grid standards and standardisation actions and consisted of reading (entirely or partially) the 112 papers recognised in the previous step. Also references included in the papers were analysed and traced. In effect, several standardisation actions were distinguished [17,21,22,23,24] as well as some supplementary reports (e.g. [25,26,23,27]).

The standardisation actions concentrated mostly on providing new specifications, but often they also pointed to related undertakings in the field. The work of IEC proves particularly useful, with the Smart Grid Standards Map [28], that enables interactive analysis of relationships between standards and electric power grid elements, as well as facilitated access to information on the norms (see Figure 1). In this research, the map is used for illustrating the relations between the identified standards and the elements of smart grid infrastructure (see the *applicability* criterion, Table 2). The relationships of NIST, NERC, DHS and other US standards, which are missed in the IEC map, were supplemented by the author. When searching for smart grid standards that refer to cybersecurity issues, the standardisation actions and the 10 more comprehensive scientific studies on standards [11,12,13,14,15,16,17,18,19,20] spotted during the literature identification phase, were analysed in the first place, in order to avoid any duplication of work.

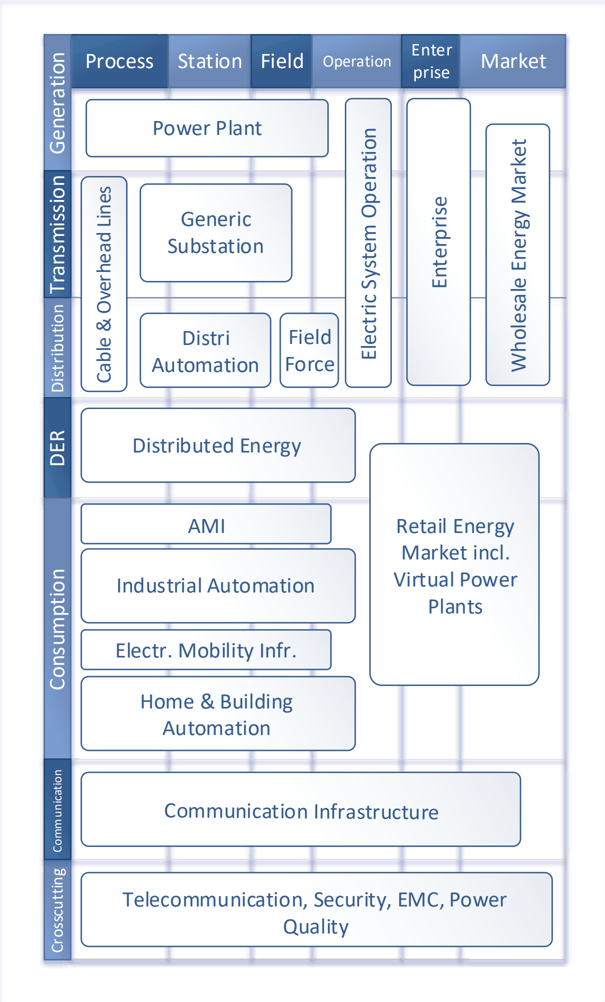


FIGURE 1 Smart grid components based on the IEC Smart Grid Standards Map [28].

Standards selection. To systematically select the standards that describe cybersecurity controls applicable to the smart grid, the *selection criteria* were formulated based on the analysis of the literature dedicated to the evaluation of standards [11,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44]. Namely, the standards should satisfy the following requirements:

(a) being referenced in smart grid standard identification studies or papers,

TABLE 2 Standards' evaluation criteria.

Criterion	Description
Scope	The thematic area addressed by the standard.
Type	The level of technical detail or more higher-level guidance.
Applicability	The elements of the smart grid infrastructure to which the standard can be applied.
Range	The geographical coverage of the standard (national or international).
Publication	The publication date of the standard.
Relevance	The level of relevance to *cybersecurity controls*. Standards that are directly dedicated to cybersecurity measures or practices, focus on them or contain detailed descriptions of the controls, are depicted as *highly*-relevant. The *low* level of relevance is associated with standards that only mention some cybersecurity controls.

(b) being developed by a standardisation body or a governmental institution,

(c) including definitions and descriptions of cybersecurity controls that can be utilised in smart grids, and

(d) being available in the English version.

The third (c) criterion requires particular attention as it specifically distinguishes the norms that are in the scope of this study. Namely, the standards need to define and describe cybersecurity controls which can be directly applied or adapted to the smart grid environment. The application of this criterion results in that important documents, such as IEEE C37.240[45], Protection Profile for the Gateway of a Smart Metering System[46] or Privacy and Security of the Advanced Metering Infrastructure[47], are excluded from the focus of this analysis. The first two publications concentrate on cybersecurity requirements, while the third defines a Common Criteria-based cybersecurity profile for AMI gateways.

After applying the criteria to the standards recognised during the literature analysis, 19 standards or standards' series were distinguished. (An example of a standards' series is IEC 62443 or AMI C12, while the singled standards that are part of the series, are IEC 62443-3-3 or AMI C12.12.) The documents are presented in Tables 3 – 5 . To facilitate the comparison of standards, the *evaluation criteria* demonstrated in Table 2 were introduced, in an analogous way as for the selection criteria. Moreover, the descriptions of the norms that focus on the security controls-related contents are provided in Section 3.

3 | RESULTS

The standards identified during the analysis are presented in Tables 3 – 5 . There, the main features of the standards according to the criteria described in Section 2 are illustrated. Additional details on the documents are provided in the following subsections.

3.1 | Smart grid or power systems' standards that describe security controls and practices

This section presents norms devised for the electricity sector or the smart grid, in particular, that contain descriptions of cybersecurity controls. The first three standards, i.e. NRC RG 5.71, IEEE 1686 and Security Profile for AMI, are depicted highly-relevant (see Table 3) because they are focused on cybersecurity measures that apply either to the entire power system or to its specific area (e.g. substations). The next two publications, i.e. NISTIR 7628 and IEC 62351 are not cybersecurity controls-centric. However, they contain sections dedicated to the controls. The remaining standards (see Section 3.1.6) describe only selected cybersecurity practices that can be applied to protect the smart grid.

3.1.1 | NRC RG 5.71

The US Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 5.71 Cyber Security Programs for Nuclear Facilities[48] guides through the life cycle of a cybersecurity programme for nuclear infrastructures. According to the standard establishing the programme requires 1) the analysis of computer systems and networks; 2) identification and documentation of critical digital assets (CDAs); 3) deployment of security controls and 4) implementation of the activities that enable sustaining of the

TABLE 3 Smart grid or power systems' standards that describe security controls and practices.

No.	Standard	Scope	Applicability	Type	Range	Pub.	Relevance
1	NRC RG 5.71	Cybersecurity of nuclear infrastructures	All components	General	US	2010	High
2	IEEE 1686	Cybersecurity	Substations	Technical	World-wide	2007	High
3	Security Profile for AMI	Cybersecurity	AMI	General	US	2010	High
4	NISTIR 7628	Smart grid cybersecurity	All components	General	US	2014	Moderate
5	IEC 62351	Security of communication protocols	All components	Technical	World-wide	2007-2016	Moderate
6	IEEE 2030	Smart grid interoperability	All components	Technical	World-wide	2011-2016	Low
7	IEC 62541	OPC UA security model	All components	General	World-wide	2015-2016	Low
8	IEC 61400-25	Wind power plants-IACS communication	Wind power plants	Technical	World-wide	2006-2016	Low
9	IEEE 1402	Physical and electronic security	Substations	General	World-wide	2008	Low
10	IEC 62056-5-3	AMI data exchange security	AMI	Technical	World-wide	2016	Low
11	ISO/IEC 14543	Home electronic system security	Home Electronic System	Technical	World-wide	2006-2016	Low

TABLE 4 Standards that describe security controls and practices applicable to IACS.

No.	Standard	Scope	Type	Range	Published	Relevance
12	IEC 62443 (ISA 99)	IACS cybersecurity	Technical	Worldwide	2008-2015	High
13	ISO/IEC 27019	IACS cybersecurity	General	Worldwide	2013	High
14	NIST SP 800-82	IACS cybersecurity	Technical	US	2015	High
15	DHS Catalog	IACS cybersecurity	General	US	2009	High

TABLE 5 General application standards that describe security controls and practices which can be adopted to smart grid.

No.	Standard	Scope	Type	Range	Published	Relevance
16	ISO/IEC 27001 and 27002	IS management	General	Worldwide	2013	High
17	NIST SP 800-53	IS management	General	US	2013	High
18	NIST SP 800-64	Security of systems in development	Technical	US	2008	High
19	NIST SP 800-124	Security of mobile devices	General	US	2013	High

programme. All these steps are explained in detail in the main chapters of the standard and additionally compiled into a security programme template presented in Appendix A. The security measures that address the third step of the process are presented in Appendices B and C. They are based on high impact baseline controls from NIST SP 800-53 and NIST SP 800-82 adapted to the characteristics of the nuclear energy sector. Appendix B includes technical security measures, while Appendix C – operational and management[48].

3.1.2 | IEEE 1686

IEEE Std 1686-2013 IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities describes security controls for IEDs. The measures respond to critical infrastructure protection programmes (e.g. NERC CIP). They are primarily dedicated to protecting the activities related to access, operation, configuration, firmware revision, and data retrieval from IEDs. In Annex A, a sample table of compliance is presented[49].

3.1.3 | Security Profile for AMI

Security Profile for Advanced Metering Infrastructure provides a set of baseline controls for protecting the Advanced Metering Infrastructure (AMI) components. The controls are an outcome of a four-step process which included: 1) the analysis of smart grid use cases; 2) risk assessment; 3) domain analysis; and 4) the analysis and adaptation of the controls specified in the DHS Catalog (see Section 3.2.4). These steps are explained in Chapter 4. The set of security controls is relatively extensive. For each measure, besides its description, a rationale of application is provided, and when applicable – potential enhancements or supplemental guidance. The document can be used to support the procurement process by serving as reference material for utilities and vendors[50].

3.1.4 | NISTIR 7628

The *NIST Internal or Interagency Report (IR) 7628 Guidelines for Smart Grid Cyber Security* approach for building cybersecurity includes determining the logical interface categories to which belongs the analysed system, and based on that to identify the security requirements that are associated with the interfaces. The standard is focused on security requirements, however in Annex B also cybersecurity measures are presented which respond to them. They fall into seven areas including power system configurations and engineering strategies, local equipment monitoring, analysis, and control, or centralized monitoring and control (see Table A2). In addition, a table is provided which gives examples of controls that respond to particular cybersecurity requirements defined in the standard.

A separate document *NISTIR 7628 User's Guide, A White Paper* published in February 2014 describes in detail the process of establishing cybersecurity in a smart grid organisation. The document distinguishes 8 major activities that constitute the process. All of them are related to risk management based on the *DOE Electricity Subsector Cybersecurity Risk Management Process (RMP)*[51]. The guide is delayed to its companion NISTIR 7628 as it refers to its previous release from 2010. NISTIR 7628 addresses the entire smart grid, with its all components, but it can also be tailored to smart grid specific elements[52].

3.1.5 | IEC 62351

IEC 62351 Power systems management and associated information exchange is a group of standards dedicated to the information security of power systems' control equipment, including EMS (Energy Management Systems), IACS, distribution automation, and others. Currently, the IEC 62351 group comprises 12 publications. The standards are detailed and technically oriented. IEC 62351-3 to 62351-6 focus on the security of communication protocols[53]. IEC 62351-7 defines abstract data object for network system management (NSM) that can be mapped to any communications protocol. The NSM is a means to assure high level security in information infrastructures. IEC 62351-8 is a detailed specification of RBAC in the context of power systems, while IEC 62351-9 is dedicated to key management and IEC 62351-14 to security event logging. IEC 62351-10 describes the security architecture for power systems based on fundamental security controls and provides a mapping of security-related standards to the components of power system[54].

3.1.6 | Smart grid or power systems' standards with lower relevance to cybersecurity controls

IEEE Std 2030 series is dedicated to smart grid interoperability. Privacy and security techniques and principles are briefly described in *IEEE Std 2030 IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*, *IEEE Std 2030.2-2015 Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure*[55] and *IEEE Std 2030.3-2016 IEEE Adoption of Smart Energy Profile 2.0 Application Protocol Standard*[55].

IEC 62541 OPC unified architecture is a series of platform-independent, interoperability standards for secure communication of IACS. *IEC TR 62541-2:2016 OPC unified architecture – Part 2: Security Model* describes a complete security model for the architecture, which includes possible threats and security functions aiming to mitigate them. These functions are evaluated in regard to their effectiveness[56]. *IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security* is a type of a straightforward manual devoted to electric substations physical and electronic security. It contains brief descriptions of different types of intrusions as well as security methods to eliminate them. An interesting and useful part of the standard is Chapter 7 on the evaluation of the methods where the results of surveys regarding the effectiveness of the security measures are provided. In Chapter 8 preparation of a security plan as well as its basic elements are explained. A sample security assessment form is presented[57].

IEC 62056 series specifies data exchange for electric meter reading, tariffs and load control. *IEC 62056-5-3 Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer* describes security techniques in Device Language Message Specification (DLMS) and COmpanion Specification for Energy Metering (COSEM)[58]. *ISO/IEC 14543 Information technology – Home electronic system (HES) architecture* consists of 20 standards dedicated to different components of home control systems, as well as to communication and interoperability aspects. In *ISO/IEC 14543-5-1:2010* and *ISO/IEC 14543-5-7:2015* security mechanisms for Intelligent Grouping and Resource Sharing (IGRS) protocols are described. *IEC 61400-25 Communications for monitoring and control of wind power plants* series specifies the uniform information model and protocols for communication between wind power plants and Industrial Control Systems. *IEC 61400-25-3* describes selected security aspects.

3.2 | Standards that describe security controls and practices applicable to IACS

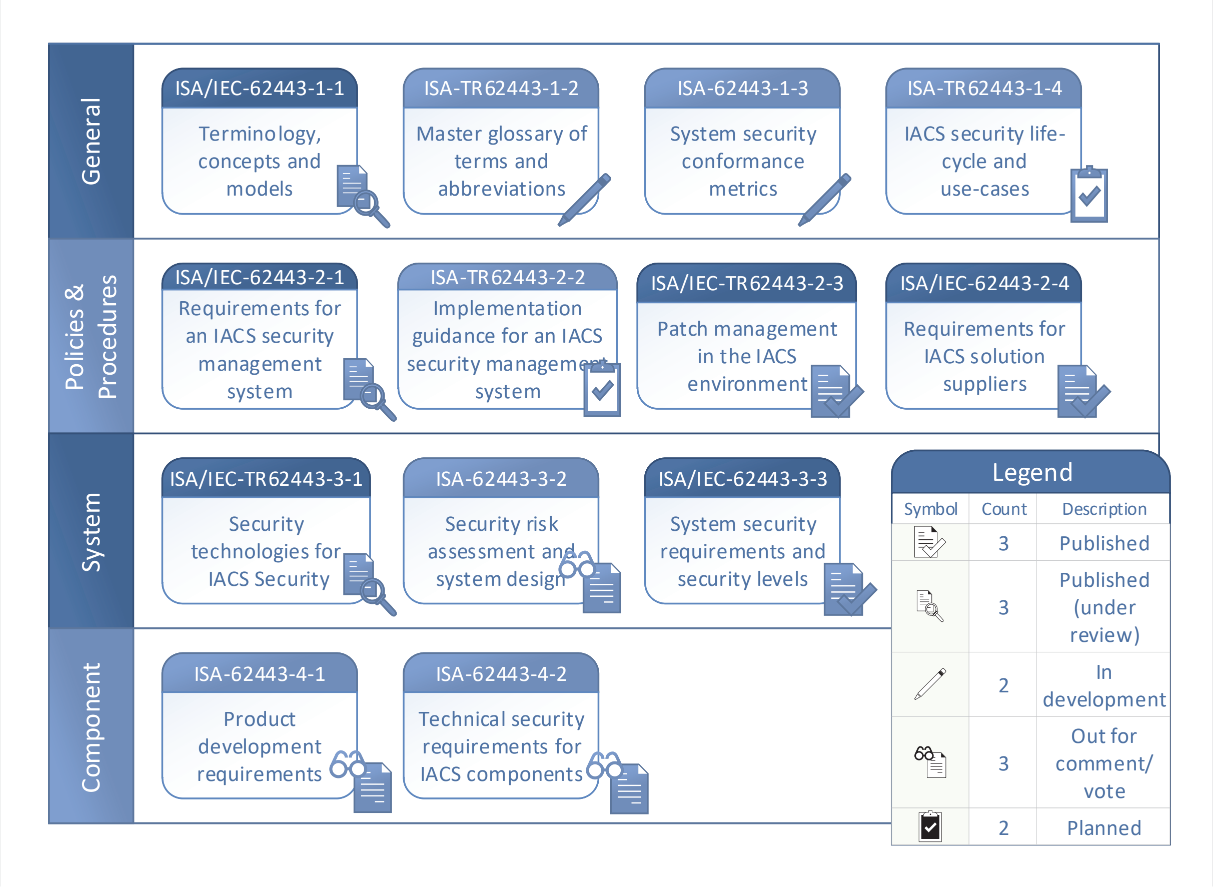
This section presents standards that specify security controls for industrial control and automation systems (IACS). IACS constitute an essential part of the smart grid responsible for monitoring and control of industrial processes involved in the entire energy supply chain, from generation to distribution. Their protection is indispensable for the proper functioning of the electricity grid.

3.2.1 | IEC 62443 (ISA99)

The *ISA99* standards, developed by ISA99 Committee (ISA – the International Society of Automation), address the electronic security of Industrial Automation and Control Systems (IACS). Since 2009 these standards have been adopted in the *IEC 62443* series, by the IEC Technical Committee 65 *Industrial-process measurement, control and automation* Working Group 10, which proceeds in strong collaboration with ISA99 Committee[59]. A drawback of this situation is some compatibility issues as the standards published by the IEC are based on older versions of ISA99 documents. For instance, various publications (e.g. NIST SP 800-82[60]) refer to ISA-62443-2-1 as to the standard which guides through the process of developing an IACS security programme, while the current version of the publication is focused on IACS-ISMS requirements and it has another title. At the same time, the IEC version (IEC-62443-2-1) is still concentrated on the IACS security programme. The standards and the status of their development are presented in Table 2 . IEC-62443-2-1, ISA-62443-2-2, ISA-62443-2-3 and ISA-62443-3-1 include descriptions of controls and practices for protecting IACS[61].

IEC 62443-2-1 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program describes the foundational elements of a Cybersecurity Management System (CSMS) for industrial communication networks (see Figure 3) and guides through the process of their development. These elements are primarily related to policies and procedures, and they are personnel-oriented. The publication introduces necessary background, discusses various types of IACS and the differences between IACS and classical ICT. It explains the process of performing risks assessment for IACS indicating specific problems, such as for instance the mandatory inclusion of non-cyber assets or safety. Chapter 4 describes the development of IACS security programme. The publication is general in scope and relatively extensive (164 pages). A substantial amount of informative guidance is located in Annexes. Published in 2010, the standard is based on the guidance in ISO/IEC 27001 and ISO/IEC 17799 which renders it slightly outdated. Also the title can be misleading as in reality the standard is CSMS-centric, directed toward describing the CSMS. These issues are addressed by the companion ISA 62443-2-1 document (the most recent version dated November 2015). However, it is still in a draft version intended for the only internal use of ISA99 and associated parties[61,63,64,65].

ISA 62443-2-2 Security for industrial automation and control systems – Implementation Guidance for and IACS Security Management System has a “planned” status (see Figure 2). There is a draft version available (from April, 2013) where some controls are left undefined. The standard, similarly to ISO 27019, follows the convention of ISO 27002. The security approach in these standards is to identify assets, perform risk analysis, accommodate relevant requirements (legal and other) and to select security controls. In ISA-62443-2-2 security requirements are described and security controls are mapped to them[63].


General
ISA/IEC-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security life-cycle and use-cases
Policies & Procedures
ISA/IEC-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA/IEC-TR62443-2-3
Patch management in the IACS environment
ISA/IEC-62443-2-4
Requirements for IACS solution suppliers
System
ISA/IEC-TR62443-3-1
Security technologies for IACS Security
ISA-62443-3-2
Security risk assessment and system design
ISA/IEC-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components
Legend

Symbol	Count	Description
✓	3	Published
🔍	3	Published (under review)
✎	2	In development
👓	3	Out for comment/ vote
☑	2	Planned

FIGURE 2 IEC 62443 standards and the status of their development[62].

IEC/TR 62443-2-3:2015 Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment provides extensive guidance on secure software patching which is particularly critical and specific to IACS. In Annex B the complete life cycle of secure patching is described[64].

IEC/TR 62443-3-1:2009 Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems is entirely dedicated to the extensive presentation of current security technologies that can be applied to protect IACS. Each control is discussed in regard to the threats it mitigates, its deployment, limitations and further development directions, as well as the particularities of applying the control to the IACS environment. The existence of IACS-specific implementations is evaluated, references to supplementary literature and other recommendations and indications are provided. The categories of controls include authentication and authorisation, communication filtering and network separation, encryption and data validation, logging, vulnerability analysis, malware detection, security management, or physical security controls[65].

3.2.2 | ISO/IEC 27019

ISO/IEC TR 27019 Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry, similarly to ISA-62443-2-2 adapts ISO/IEC 27002 (guidance on the implementation of the information security management system, see Section 3.3.1) to IACS. It also follows the structure of ISO/IEC 27002. Both standards refer to the older version of ISO 27002 which was published in 2005, while the current (subsequent) edition of the norm was released in 2013 (ISO/IEC 27002:2013). For the security controls which can be directly applied to IACS, ISO/IEC 27019 sends to the original for further guidance. For other controls, additional IACS-specific indications are provided. Moreover, there are new controls defined particularly for IACS. These controls are described in line with other measures and additionally enlisted in Annex A 3.3.1[66].

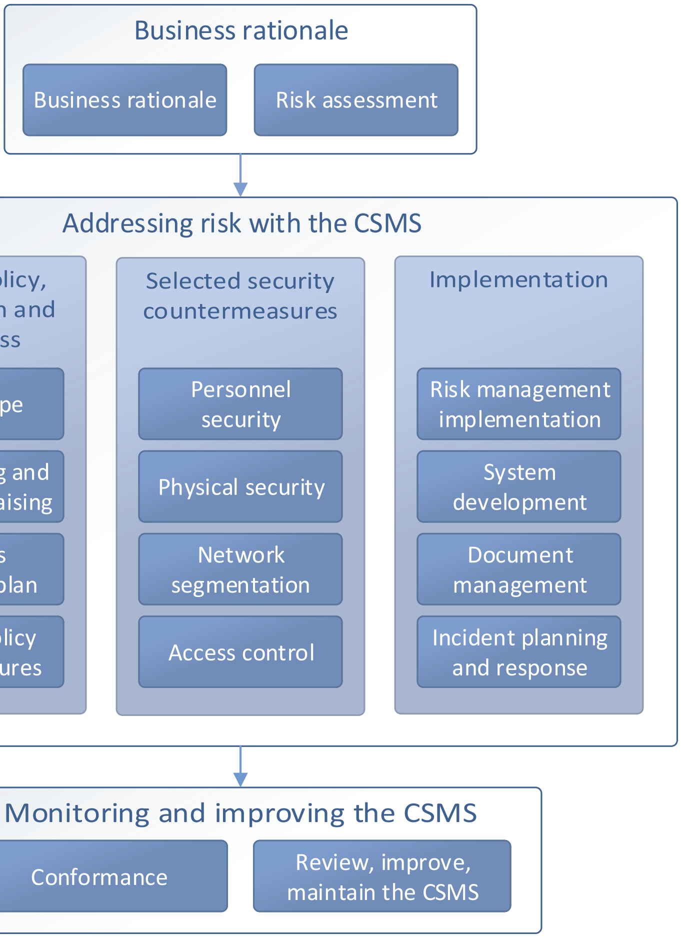

Business rationale
Business rationale
Risk assessment
Addressing risk with the CSMS
Security policy, organisation and awareness
CSMS Scope
Staff training and awareness raising
Business continuity plan
Security policy and procedures
Selected security countermeasures
Personnel security
Physical security
Network segmentation
Access control
Implementation
Risk management implementation
System development
Document management
Incident planning and response
Monitoring and improving the CSMS
Conformance
Review, improve, maintain the CSMS

FIGURE 3 The elements of IACS Cybersecurity Management System specified in IEC 62443-2-1.

Although ISO/IEC 27019 presents some similarities to ISA-62443-2-2 (mainly regarding the structure and the approach), these standards need to be distinguished as they differ substantially. The IACS-specific descriptions of controls are different. Selected controls are extended in one standard while left unchanged in the other. ISO/IEC 27019 defines new controls while ISA-62443-2-2 adheres to the controls of ISO/IEC 27002. Finally, the ISA-62443-2-2 is still in a draft version, and its IEC counterpart does not exist[66].

3.2.3 | NIST SP 800-82

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security is another publication dedicated to protecting IACS. Similarly to the IEC 62443-3-1, the document addresses various IACS architectures (DCS, SCADA, PLCs and other) and has a diverse readership, from control engineers, integrators, and architects, to researchers and vendors. According to the authors, it is technical in nature[60].

Key security objectives defined in NIST SP 800-82 include reducing the access to IACS networks (e.g. through network separation, DMZ, multilayer, access control) and limiting physical access to IACS, protecting against exploits, detecting security incidents, establishing a multidisciplinary security team, effective communication and information sharing, fault tolerance, graceful degradation, system restoration and defence-in-depth. Consequently, an IACS protection strategy should comprise IACS-centric policies and procedures, awareness and training, security through the whole life cycle (from design to disposal) of IACS components, multi-layered network with critical operations occurring in the most secure subnetwork and other which are directly derived from the security objectives. All these elements are thoroughly explained in the document[60].

The development process of a security programme specified in NIST SP 800-82 (see Figure 4) reflects the approach presented in IEC 62443-2-1 (see Section 3.2.1) and comprises similar elements. In fact, NIST SP 800-82 directs to IEC 62443-2-1 for further details on the activities which constitute the overall process. Additional guidance on IACS security measures is presented in Appendix G, where an extensive description of security controls is provided. The controls are based on NIST SP 800-53, however, for each of them, the IACS-specific indications and enhancements are provided. Choosing the controls for a particular IACS should be based on risk assessment[60].

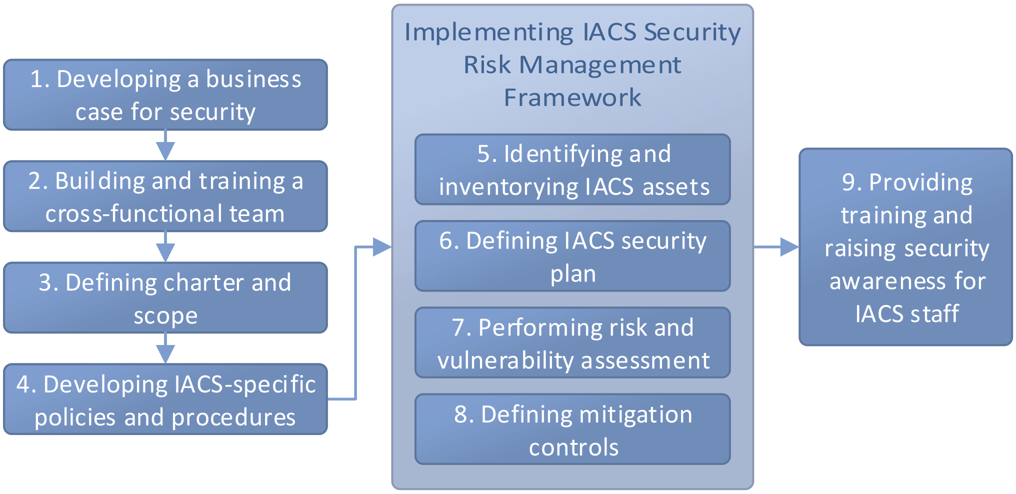

1. Developing a business case for security
2. Building and training a cross-functional team
3. Defining charter and scope
4. Developing IACS-specific policies and procedures
Implementing IACS Security Risk Management Framework
5. Identifying and inventorying IACS assets
6. Defining IACS security plan
7. Performing risk and vulnerability assessment
8. Defining mitigation controls
9. Providing training and raising security awareness for IACS staff

FIGURE 4 The elements of IACS security programme development according to NIST SP 800-82.

3.2.4 | DHS Catalog

The Department of Homeland Security (DHS)' Catalog of Control Systems Security: Recommendations for Standards Developers defines an extensive set of 250 controls that can be applied to protect IACS used in various industries. For each control, (under a perhaps misleading heading – "Requirement"), the description of recommended security practices and mechanisms is provided. In addition, supplementary guidance and control enhancements are presented when applicable. The controls originate from various sources, and their organisation follows the structure of NIST SP 800-53, which results in a 19 categories classification of controls. The sources of controls are not indicated explicitly, however, Appendix A contains a cross-referencing table where all the controls from the DHS Catalog are referred to 15 other standards. The standards include AGA, FIPS, IEC 62351, ISA99, ISO 27001, ISO 17799, NER CIP, NIST SP 800-53 and other. DHS Catalog is focused on the presentation of the controls. The standard does not present additional guidance on selecting the controls to a particular system configuration or industry[67].

3.3 | General application standards that describe security controls and practices which can be adopted to smart grid

In this section universal cybersecurity standards that contain descriptions of cybersecurity controls are presented. These publications are not the electricity sector or the smart grid-oriented. However, the presented protection measures and practices can be successfully adapted to protect the smart grid.

3.3.1 | ISO/IEC 27001 and 27002

The *ISO/IEC 27000* series (or *ISO27k* for short) is a long-recognised set of standards dedicated to the protection of information assets in organisations through establishing and operating an information security management system (ISMS). ISO/IEC 27001 specifies the requirements for a correct realisation of an ISMS through its complete life cycle. The process is risk management-centric and its essential part constitute risk assessments performed periodically. To mitigate the risks identified during the assessments a list of 114 security controls that address 35 security objectives is presented in a table in Annex A. A detailed guidance on implementation of these controls is provided in ISO/IEC 27002 (*code of practice*)[68,69].

The ISO/IEC standards not only are widely recognised and applied by thousands of organisations worldwide but also constitute a foundation for other security standards, guides, regulations and frameworks. For instance, IACS-specific ISO/IEC 27019 or ISA 62443-2-2 (see Section 3.2.2 and 3.2.1) are directly based on ISO/IEC 27002, while NIST SP 800-53 and its followers (e.g. NIST SP 800-82) or the DHS Catalog refer to them broadly. Many of these derivative standards are based on ISO/IEC 27001:2005 and ISO/IEC 27002:2005 while in 2013 new versions of these publications have been published which entail specific changes. The 2013 standards not any longer refer to the Plan-Do-Check-Act model, direct more attention to evaluating the performance of an ISMS based on metrics and redefine several concepts including risk assessment, controls' selection or continual improvement[68,69].

3.3.2 | NIST SP 800-53

NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations specifies baseline sets of controls for protecting information systems in the US public administration that have been derived from various types of legislative and regulatory documents, standards and business requirements. The controls, grouped into 18 families which reflect distinctive security topics, address various aspects of security, including policy development and management, awareness and training, contingency planning, incident response, personnel security, systems acquisition and more. Although the publication is dedicated to federal institutions, it has been widely recognised worldwide and applied by various organisations (not only governmental)[70].

The control baselines are specified in a way that enables their high customisation, which facilitates the development of cost-effective protection strategies and systems. Controls' definitions include organisation-specific parameters and control enhancements. Three baseline sets of controls are specified that respond to the three levels of systems' criticality (low, moderate and high) defined in the Federal Information Processing Standard (FIPS) 199. Extending from a lower baseline set to higher is based on implementing additional controls and control enhancements. Additionally, the concept of *overlays* was introduced in the newest (fourth) standard release. The overlays enable designating control baselines tailored to particular organisation's needs, mission or business functions, technologies or environments. At the same time the IACS-specific guidance present in the earlier releases was moved to NIST SP 800-82 (see Section 3.2.3). An important part of NIST SP 800-53 is dedicated to the explanation of the control selection process which should be part of an organisational risk management[70].

3.3.3 | NIST SP 800-64

NIST SP 800-64 Security Considerations in the System Development Life Cycle guides through the process of incorporating cybersecurity principles and practices into the life cycle of IT system development. The guidelines are based on the classical software development model – the waterfall model, in which five stages are distinguished in the standards. These include initiation, development or acquisition, implementation or assessment, operations and maintenance, and disposal. There security controls are defined by means of security activities associated with each phase. The descriptions are detailed and accompanied by implementation tips. Although the standard uses the waterfall model as a reference, it should apply to other software development approaches[71]. However, supplementing the norm with indications on security in agile development might be, perhaps, of a value.

3.3.4 | NIST SP 800-124

NIST SP 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise provides specific guidance on security of mobile devices. The standard describes technologies for mobile devices management together with the required security capabilities and explains their application through the entire life cycle of mobile solutions. Analogously to NIST SP 800-64 (see Section 3.3.3), the five-stages waterfall model of a system life cycle is taken as a reference[72].

4 | STANDARDS' ANALYSIS

This section presents the results of the analysis of the standards and cybersecurity controls they define. Specifically, the relationships between the controls have been investigated as well as the coverage of smart grid domains and cybersecurity areas. These topics are described in Sections 4.1, 4.2 and 4.3.

4.1 | Relationships between cybersecurity controls in the standards

The relationships between cybersecurity controls in the identified standards are presented in Figure 5 . Unidirectional solid arrows indicate which norms served as an input during the development of other specifications of cybersecurity measures and practices. For instance, the controls defined in NRC RG 5.71 are derived from NIST SP 800-53 and NIST SP 800-82 (see Section 3.1.1. Dashed bidirectional arrows show congruence between standards as far as cybersecurity controls are concerned. NIST SP 800-53 is highly convergent with ISO 27001 in the sense that practically for all the controls defined in ISO 27001 its NIST SP 800-53 equivalents can be found. Moreover, in Appendix H, NIST SP 800-53 provides mapping tables where the relationships between the individual controls in the two documents are presented. Dashed unidirectional arrows indicate that a standard refers to cybersecurity measures or practices defined in another publication. As an example, IEEE 2030 advises consideration of ISO 27000 standards when developing a security programme.

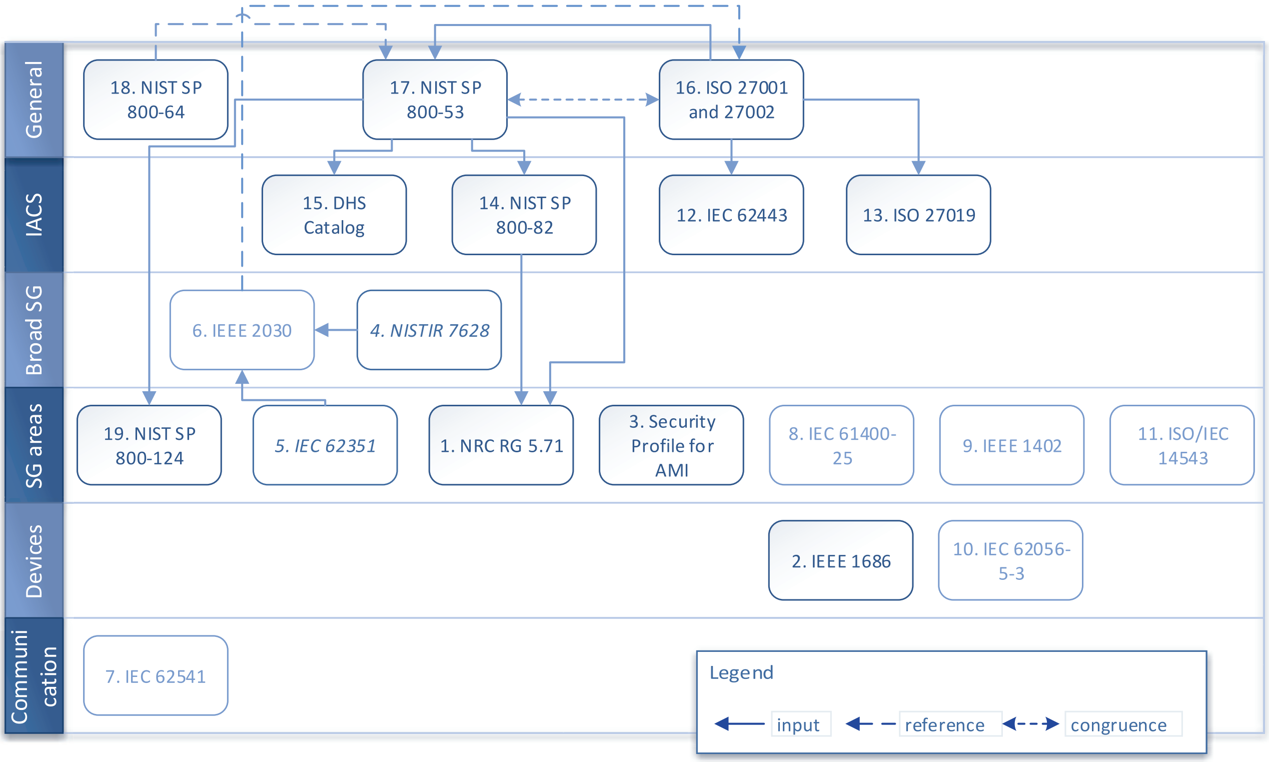
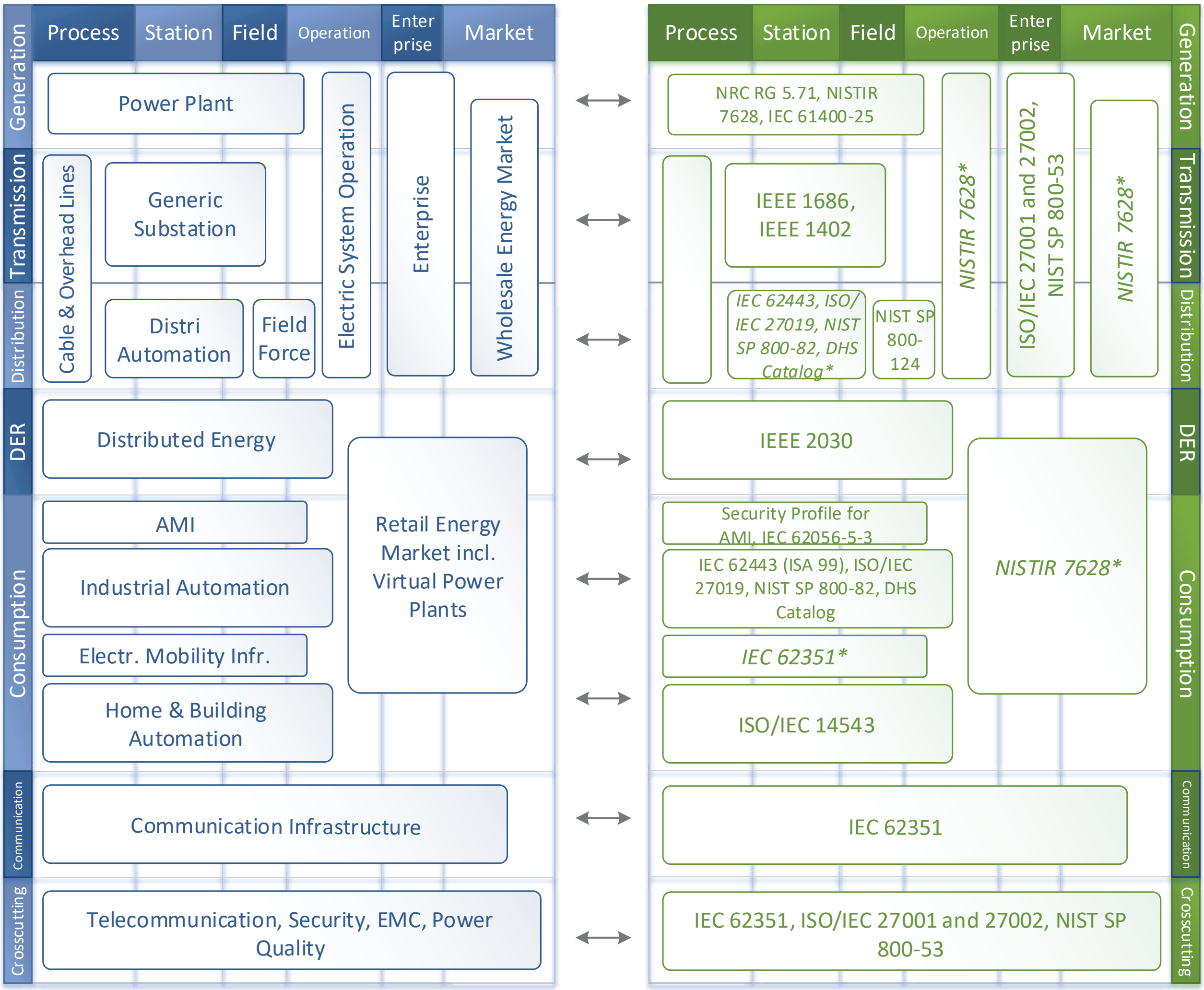


FIGURE 5 Relationships between cybersecurity controls in the identified standards. Unidirectional solid arrows indicate which standards served as an input during the development of other specifications of cybersecurity measures and practices. Dashed bidirectional arrows show congruence between standards as far as cybersecurity controls are concerned. Dashed unidirectional arrows indicate that a standard refers to cybersecurity measures or practices defined in another publication. Horizontal lanes depict the scope of the standards in regard to cybersecurity requirements, their level of generality and/or thematic coverage.

Horizontal lanes depict the scope of the standards in relation to cybersecurity controls, their level of abstraction and the coverage of smart grid areas. E.g. the cybersecurity measures specified in ISO 27001 and 27002 are universal, applicable to organisations of various types and size. The controls defined in IEC 62351, on the other hand, are dedicated to concrete communication protocols in the smart grid. IEEE 1686 specifies measures for particular smart grid components (IEDs), while the measures from NIST SP 800-124, NRC RG 5.71 or IEEE 1402 are more suitable for specific smart grid areas (field operations, power plants, substations).

4.2 | Smart grid areas addressed by controls

A mapping between smart grid areas and standards that define cybersecurity controls for them is presented in Figure 6 . The smart grid areas follow the smart grid reference architecture specified by the IEC (see Section 2). All smart grid domains are covered with control specification to a lesser or greater extent. The only exception is “Cable and overhead lines” which has entirely physical character. Standards such as IEEE 1686, NRC RG 5.71 or IEC 62443 (ISA 99) propose cybersecurity controls specifically dedicated to the indicated areas (substations, power plants and IACS – respectively). NISTIR 7628, on the other hand, is a broad scope publication on smart grid security, which coverage spans over multiple smart grid domains. However, some of them (e.g. energy markets or electric system operation) are addressed only limitedly.



Process
Station
Field
Operation
Enterprise
Market
Generation
Transmission
Distribution
DER
Consumption
Communication
Crosscutting
Power Plant
Cable & Overhead Lines
Generic Substation
Distri Automation
Field Force
Electric System Operation
Enterprise
Wholesale Energy Market
Distributed Energy
AMI
Industrial Automation
Electr. Mobility Infr.
Home & Building Automation
Retail Energy Market incl. Virtual Power Plants
Communication Infrastructure
Telecommunication, Security, EMC, Power Quality
NRC RG 5.71, NISTIR 7628, IEC 61400-25
IEEE 1686, IEEE 1402
IEC 62443, ISO/ IEC 27019, NIST SP 800-82, DHS Catalog*
NIST SP 800-124
NISTIR 7628*
ISO/IEC 27001 and 27002, NIST SP 800-53
NISTIR 7628*
IEEE 2030
Security Profile for AMI, IEC 62056-5-3
IEC 62443 (ISA 99), ISO/IEC 27019, NIST SP 800-82, DHS Catalog
IEC 62351*
ISO/IEC 14543
NISTIR 7628*
IEC 62351
IEC 62351, ISO/IEC 27001 and 27002, NIST SP 800-53

FIGURE 6 Mapping between smart grid areas and standards that specify controls to protect them. Standards marked with asterisk and italic letters cover the indicated smart grid area only to a small extent.

4.3 | Cybersecurity areas addressed by controls

Cybersecurity areas addressed by the controls specified in the analysed standards are presented in Tables A1 – A4 in Appendix A. It becomes evident that standards with a common root, such as NIST SP 800-82 and DHS Catalog, which have been developed in reference to NIST SP 800-53 (see Section 4.1), cover similar cybersecurity areas.

5 | RELATED WORK

The smart grid stocktaking actions associated with standardisation initiatives described in Section 2, that aimed at recognising existent standards relevant to cybersecurity, aimed at achieving a general overview of the situation, rather than achieving scientific completeness or correctness of the conduct. Consequently, they did not require applying and demonstrating a systematic method of the research. As a result the studies bring in various standards and present them from different perspectives[73,28,74,75,15,76,77,78,79,25,24,22,17,21,23,80,27,81].

Also, scientific reviews that concentrate on identifying smart grid cybersecurity standards[11,12,13,14,15,16,17,18,19,20] exhibit different levels of exploration-depth, completeness and objectiveness, in the majority being just unconstrained overviews of standards and specifications connected to smart grid cybersecurity. None of them is devoted to the topic of cybersecurity measures that can be utilised in smart grids.

Among the studies, the work of Wang et al. in[12] stands out, as it is well-based on transparent criteria (standard source, relevance to smart grid cybersecurity and representativeness). As a result 17 publications were recognised, including NERC CIP, NISTIR 7628, IEEE 1686-2007, NIST SP 800-82 as well as DHS Catalog[12]. It is the only study that provides details of a systematic method used in the evaluation, nor selection/evaluation criteria.

The research described in this paper follows up the earlier author's studies on standards dedicated to cybersecurity aspects of smart grids[7], cybersecurity requirements for smart grids[8], and security assessments in smart grids[9]. It applies the same systematic and repeatable research method (details of which are openly provided), based on transparently stated selection and evaluation criteria, in order to achieve the highest possible degree of completeness.

The current study is devoted to cybersecurity controls, i.e. the technical and non-technical measures of protecting a system or assets from cyberattacks, that can be utilised in the smart grid infrastructure. To the best of author's knowledge, there are no concurrent works that address this topic, despite its significance and validity. As a result, this review provides a form of a guide through smart grid standards that specify cybersecurity controls – 19 standards and guidelines are described from the security controls perspective, referred to each other and related to evaluation criteria. All of them have been referred to the IEC smart grid architecture (see Fig. 1) to depict the relationships between standards and smart grid components.

6 | CONCLUSIONS

Several standards exist that define cybersecurity controls applicable to smart grids. Some of them, such as NRC RG 5.71 or IEEE 1686 are directly dedicated to this topic, other address it as one of the covered areas. Norms such as ISO 27001 or NIST SP 800-53, on the other hand, while not devoted to smart grids, can be straightforwardly adapted to them, especially as far as their corporate part is concerned. Certain standards (NIST SP 800-82 and DHS Catalog) highly overlap regarding the controls which they define, other, although also are derived from a common origin, are complementary to each other (IEC 62443 (ISA 99) and ISO/IEC 27019).

It becomes evident that ISO 27001, ISO 27002 and NIST SP 800-53, while highly congruent, they are also complementary to each other. They have similar coverage of cybersecurity measures and areas, but they group cybersecurity controls in different categories (see Table A4) and describe them with varying levels of details. Certification processes are available and established for ISO standards. NIST SP 800-53, on the other hand, provides more detailed descriptions of controls. A possible control implementation approach could be to aim at satisfying ISO compliance requirements, using the NIST's publication for guidance.

Among the standards with cybersecurity measures and practices dedicated to IACS, DHS Catalog and NIST SP 800-82 represent visible convergence as they both originate from NIST SP 800-53 and cover practically the same control areas. DHS Catalog is entirely focused on controls, while NIST SP 800-82 additionally explains the process of development and establishment a cybersecurity programme for IACS. Moreover, NIST SP 800-82 is periodically reviewed and updated. Its most recent version was issued in 2015, and this is a second revision to the original release from 2011. DHS Catalog, on the other hand, is dated 2009 and since that time no modifications or amendments have been done to it.

Similarly, IEC 62443 (ISA 99) and ISO/IEC 27019, which are also IACS-oriented, contain intersecting parts, as the standards centre around ISO/IEC 27001. In particular, ISO 27019 and ISA-62443-2-2 follow the structure of ISO/IEC 27001, while IEC 62443-2-1 is based on its guidance. It must be noted though, that the latter has not been officially published, while the available draft version is incomplete. IEC/TR 62443-3-1:2009, on the other hand, provides an extensive explanation of IACS-specific security technologies independent from ISO 27001.

Other smart grid areas that are well covered by standards, as far as cybersecurity controls are concerned, are the AMI infrastructure and nuclear power plants, for which security measures are defined in Security Profile for AMI and NRC RG 5.71, consequently. For power plants of lesser criticality than nuclear power plants, NRC RG 5.71, NIST SP 800-53 and NIST SP 800-82 can be used together as a reference, with the approach of replacing the high-impact controls from NRC RG 5.71 with lower impact controls.

IEEE 1402 is dedicated to the physical security of electric substations, but it also shortly describes selected cybersecurity controls. In regard to the in-the-field operation of technical personnel, NIST SP 800-124 explains in detail the measures for protecting the use of mobile devices. Specific areas of the home electronic system (HES) and wind power plants are covered by specifications in IEC 61400-25-3 and SO/IEC 14543. As far as electric power devices are concerned, IEEE 1686 specifies cybersecurity controls for IEDs and IEC 62056-5-3 addresses selected control areas of electric meters. IEC 62351 and IEC 6254 centre around power grid and IACS communications.

NISTIR 7628 and IEEE 2030 embrace the elements of the entire smart grid architecture, with a strong focus on their interoperability. The former focuses on cybersecurity, but it is predominately devoted to requirements and privacy aspects, depicting only selected cybersecurity controls. The latter is not dedicated to cybersecurity but contains cybersecurity-related contents. It refers to ISO 27001 and NISTIR 7628, but includes additional explanations or the implementation process (in Annex B) or security engineering.

Certain disproportions can be observed in relation to the smart grid domains coverage by cybersecurity controls. IACS and corporate parts of smart grids are particularly well covered. Nuclear power plants and substations operators will also find useful guidance on controls in NRC RG 5.71, IEEE 1686. Operators of other types of power plants can tailor the guidance from NRC RG 5.71, with the aid of NIST SP 800-53 and NIST 800-82.

The areas that require further standardisation developments in regard to cybersecurity controls are:

- markets,
- the operation of the entire power system,
- electric vehicles.

APPENDIX

A CYBERSECURITY AREAS ADDRESSED BY CONTROLS

Tables A1 – A4 depict the areas of cybersecurity which are addressed by the controls specified in the analysed standards.

TABLE A1 Cybersecurity areas addressed by controls specified in smart grid or power systems' standards highly focused on cybersecurity measures and practices.

NRC RG 5.71	IEEE 1686-2013	Security Profile for AMI
Access controls	Audit trail	Access control
Audit and accountability	Communications port access	Audit and accountability
Awareness and training	Electronic access control	Incident response
Configuration management	Firmware quality control	Information and document management
Contingency planning/continuity of safety, security, and emergency preparedness	IED configuration software	Survivability
Critical digital asset and communications protection	IED cyber security features	System and communication protection
Defense-in-depth	Supervisory monitoring and control	System and information integrity
Defensive strategy		System development and maintenance
Functions		
Identification and authentication		
Incident response		
Maintenance		
Media protection		
Personnel security		
Physical and environmental protection		
Security assessment and risk management		
System and information integrity		
System and service acquisition		
System hardening		

TABLE A2 Cybersecurity areas addressed by controls specified in smart grid or power systems' standards moderately relevant to cybersecurity measures and practices.

NISTIR 7628	IEC 62351
Centralized monitoring and control	Event logging
Centralized power system analysis and control	Intrusion detection systems
Local equipment monitoring, analysis, and control	Key management
Power system configurations and engineering strategies	Monitoring and control of networks and protocols
Testing	Monitoring and management of end systems
Training	Role-based access control
	Security of communication protocols

References

1. Yilin Mo , Kim Tiffany Hyun-Jin, Brancik K., et al. CyberâĂŞPhysical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE.* 2012;100(1):195–209.

2. Pearson Ivan L.G.. Smart grid cyber security for Europe. *Energy Policy.* 2011;39(9):5211–5218.

3. Tipton Harold F, Krause Micki. *Information Security Management Handbook, Sixth Edition.* No. c2007.

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

TABLE A3 Cybersecurity areas addressed by controls specified in the standards that describe measures and practices applicable to IACS.

IEC 62443	ISO/IEC 27019	NIST SP 800-82	DHS Catalog
Auditing	Access control	Access control	Access control
Authentication and authorization	Asset management	Audit and accountability	Audit and accountability
Data validation	Business continuity management	Awareness and training	Configuration management
Encryption and data validation	Communications and operations management	Configuration management	Incident response
Filtering, blocking, and access control	Compliance	Contingency planning	Information and document management
Management,	Human resources	Identification and authentication	Media protection
Measurement	Information security incident management	Incident response	Monitoring and reviewing control system security policy
Monitoring and detection tools	Information systems acquisition, development and maintenance	Maintenance	Organizational security
Operating systems	Organisation of information security	Media protection	Personnel security
Physical security control	Physical and environmental security	Personnel security	Physical and environmental security
	Security policy	Physical and environmental protection	Risk management and assessment
		Planning	Security awareness and training
		Program management	Security policy
		Risk assessment	Security program management
		Security assessment and authorization	Strategic planning
		System and communications protection	System and communication
		System and information integrity	System and information integrity
		System and services acquisition	System and services acquisition
			System development and maintenance

5. Kissel Richard. *NISTIR 7298 Revision 2 Glossary of Key Information Security Terms.* : NIST; 2013.

6. ISO/IEC . *ISO/IEC 27000:2016 Information technology âĂŤ Security techniques âĂŤ Information security management systems âĂŤ Overview and vocabulary.* 2016.

7. Leszczyna Rafał. Cybersecurity and privacy in standards for smart grids âĂŞ A comprehensive survey. *Computer Standards and Interfaces.* 2018;56(April 2017):62–73.

8. Leszczyna Rafał. A Review of Standards with Cybersecurity Requirements for Smart Grid. *Computers & Security.* 2018;.

TABLE A4 Cybersecurity areas addressed by controls specified in general application standards that describe cybersecurity measures and practices which can be adopted to smart grid.

ISO 27001 and 27002	NIST SP 800-53	NIST SP 800-64	NIST SP 800-124
Access control	Access control	Business impact assessment	Access control
Asset management	Audit and accountability	Configuration management	Applications' security
Business continuity management	Awareness and training	Continuous monitoring	Audit
Communications and operations management	Configuration management	Detailed plan for certification and accreditation	Configuration settings
Compliance	Contingency planning	Developmental, functional, and security testing	Continuous monitoring
Human resources	Identification and authentication	Disposal or transition plan development	Media sanitization
Information security incident management	Incident response	Hardware and software disposal	Secure data communication and storage
Information systems acquisition, development and maintenance	Maintenance	Information preservation	Security awareness training
Organisation of information security	Media protection	Information system authorisation	Security policy
Physical and environmental security	Personnel security	Information system categorisation	System and communications protection
Security policy	Physical and environmental protection	Media sanitisation	System and information integrity
	Planning	Operational readiness review	User and device authentication
	Program management	Privacy impact assessment	
	Risk assessment	Risk assessment	
	Security assessment and authorization	Secure information system development	
	System and communications protection	Security architecture definition	
	System and information integrity	Security assessment	
	System and services acquisition	Security controls selection and documentation	
		Security documentation	
		Security integration	
		Security planning	
		System closure	

9. Leszczyna Rafał. Standards on Cyber Security Assessment of Smart Grid. *International Journal of Critical Infrastructure Protection.* 2018;.

10. Webster Jane, Watson Richard T.. Analyzing the past to prepare for the future: writing a literature review. *MIS Quarterly.* 2002;26(2):xiii–xxiii.

11. Ruland Karl Christoph, Sassmannshausen Jochen, Waedt Karl, Zivic Natasa. Smart grid security âĂŞ an overview of standards and guidelines. *Elektrotechnik und Informationstechnik.* 2017;134(1):19–25.

12. Wang YuFei, Zhang Bo, Lin WeiMin, Zhang Tao. Smart grid information security - a research on standards. In: :1188–1194IEEE; 2011.

13. Lam Jonathan. Protecting Large and Complex Networks. *IET Cyber Security in Modern Power Systems.* 2016;(June).

14. Kanabar Mitalkumar G., Voloh Ilia, McGinn David. Reviewing smart grid standards for protection, control, and monitoring applications. In: :1–8IEEE; 2012.

15. Griffin Robert W., Langer Lucie. Chapter 7 âĂŞ Establishing a Smart Grid Security Architecture. In: 2015 (pp. 185–218).

16. Rosinger Christine, Uslar Mathias. Smart Grid Security: IEC 62351 and Other Relevant Standards. In: Springer, Berlin, Heidelberg 2013 (pp. 129–146).

17. Goraj M., Gill J., Mann S.. Recent developments in standards and industry solutions for cyber security and secure remote access to electrical substations. In: :161–161IET; 2012.

18. Falk Rainer, Fries Steffen. Smart Grid Cyber Security - An Overview of Selected Scenarios and Their Security Implications. *PIK - Praxis der Informationsverarbeitung und Kommunikation.* 2011;34(4):168–175.

19. Wang Yong, Ruan Da, Xu Jianping. Analysis of Smart Grid security standards. In: :697–701IEEE; 2011.

20. Kuzlu M., Pipattanasompom M., Rahman S.. A comprehensive review of smart grid related standards and protocols. In: :12–16IEEE; 2017.

21. Hauer I., Styczynski Z. A., Komarnicki P., Stotzer M., Stein J.. Smart grid in critical situations. Do we need some standards for this? A german perspective. In: :1–8IEEE; 2012.

22. Kanabar Mitalkumar G., Voloh Ilia, McGinn David. A review of smart grid standards for protection, control, and monitoring applications. In: :281–289IEEE; 2012.

23. CEN-CENELEC-ETSI JWG . *Final report Standards for Smart Grids.* 2011.

24. Fan Zhong, Kulkarni Parag, Gormus Sedat, et al. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. *IEEE Communications Surveys & Tutorials.* 2013;15(1):21–38.

25. DKE . *German Roadmap E-Energy/Smart Grid 2.0.* : German Commission for Electrical, Electronic & Information Technologies of DIN and VDE; 2013.

26. Wouter Vlegels , Leszczyna (eds.) Rafal. *Smart Grid Security: Recommendations for Europe and Member States.* 2012.

27. Standardisation Management Board Smart Grid Strategic Group (SG3) . *IEC Smart Grid Standardization Roadmap.* June: Standardisation Management Board Smart Grid Strategic Group (SG3); 2010.

28. IEC . *Smart Grid Standards Map.* 2017.

29. Zhang Yurong, Wang Jingjing, Hu Fangfang, Wang Yuanfeng. Comparison of evaluation standards for green building in China, Britain, United States. *Renewable and Sustainable Energy Reviews.* 2017;68:262–271.

30. Metheny Matthew. Comparison of federal and international security certification standards. In: Elsevier 2017 (pp. 211–237).

31. Gazis Vangelis. A Survey of Standards for Machine-to-Machine and the Internet of Things. *IEEE Communications Surveys & Tutorials.* 2017;19(1):482–511.

32. ENISA . *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools.* : ; 2016.

33. Beckers Kristian, Côté Isabelle, Fenz Stefan, Hatebur Denis, Heisel Maritta. A Structured Comparison of Security Standards. In: Springer International Publishing 2014 (pp. 1–34).

34. Sunyaev Ali.. Design and application of a security analysis method. In: Gabler 2011 (pp. 117–166).

35. Overman Thomas M., Davis Terry L., Sackman Ronald W.. High assurance smart grid. In: :1ACM Press; 2010; New York, USA.

36. Sommestad Teodor, Ericsson GoÌĹran N, Nordlander Jakob. SCADA system cyber security âĂŤ A comparison of standards. In: :1–8IEEE; 2010.

37. Kuligowski Christine. Comparison of IT Security Standards. PhD thesis2009.

38. Siponen Mikko, Willison Robert. Information security management standards: Problems and solutions. *Information & Management.* 2009;46(5):267–270.

39. Kosanke Kurt. ISO Standards for Interoperability: a Comparison. In: London: Springer-Verlag 2006 (pp. 55–64).

40. Arora Varun. Comparing different information security standards : COBIT v s . ISO 27001. *Carnegie Mellon University, Qatar.* 2005;:7–9.

41. Idaho National Laboratory . *A Comparison of Cross-Sector Cyber Security Standards.* : ; 2005.

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

43. Lee Annabelle, Snouffer Stanley R., Easter Randall J., Foti James, Casar Tom. *NIST SP 800-29 A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2.* : ; 2001.

44. Eastaughffe K.A., Cant A., Ozols M.A.. A framework for assessing standards for safety critical computer-based systems. In: :33–44IEEE Comput. Soc; 1999.

45. IEEE Power & Energy Society. Power System Relaying Committee. , IEEE Power & Energy Society. Substations Committee. , Institute of Electrical and Electronics Engineers. , IEEE-SA Standards Board. . *C37.240-2014 – IEEE standard cybersecurity requirements for substation automation, protection, and control systems.* : ; 2014.

46. Kreutzmann Helge, Vollmer Stefan. *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP).* 2014.

47. Netbeheer Nederland . *Privacy and Security of the Advanced Metering Infrastructure.* : ; 2010.

48. NRC . *NRC RG 5.71 Cyber Security Programs for Nuclear Facilities.* : ; 2010.

49. IEEE . *IEEE 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.* 2013.

50. Advanced Security Acceleration Project . *Security Profile for Advanced Metering Infrastructure.* : ; 2010.

51. DOE , NIST , NERC . *Electricity Subsector Cybersecurity Risk Management Process.* May: ; 2012.

52. The Smart Grid Interoperability Panel Cyber Security Working Group . *NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity.* : NIST; 2014.

53. IEC . *IEC/TS 62351-1: Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues.* 2007.

54. Cleveland Frances. *IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure.* : International Electrotechnical Commission; 2016.

55. IEEE Standards Coordinating Committee 21 . *IEEE guide for the interoperability of energy storage systems integrated with the electric power infrastructure.* : ; 2015.

56. IEC . *IEC TR 62541-2:2016 OPC unified architecture - Part 2: Security Model.* 2016.

57. IEEE-SA Standards Board . *IEEE 1402 (R2008) – IEEE Guide for Electric Power Substation Physical and Electronic Security.* : ; 2008.

58. IEC . *IEC 62056-5-3:2016 Electricity metering data exchange - The DLMS/COSEM suite - Part 5-3: DLMS/COSEM application layer.* : ; 2016.

59. ISA . *ISA99, Industrial Automation and Control Systems Security.* 2017.

60. Stouffer Keith, Pillitteri Victoria, Lightman Suzanne, Abrams Marshall, Hahn Adam. *NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2.* : NIST; 2015.

61. IEC . *IEC 62443-2-1: Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.* 2010.

62. ISA . *The 62443 series of standards Industrial Automation and Control Systems Security.* : ; 2016.

63. ISA . *ISA 62443-2-2 Security for industrial automation and control systems – Implementation Guidance for and IACS Security Management System.* 2013.

64. IEC . *IEC TR 62443-2-3: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment.* 2015.

65. IEC . *IEC/TR 62443-3-1: Industrial communication networks âĂŞ Network and system security âĂŞ Part 3-1: Security technologies for industrial automation and control systems.* 2009.

66. ISO/IEC . *ISO/IEC TR 27019:2013: Information technology âĂŤ Security techniques âĂŤ Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.* 2013.

67. DHS . *Catalog of Control Systems Security: Recommendations for Standards Developers.* : ; 2009.

68. ISO/IEC . *ISO/IEC 27001:2013: Information technology âĂŞ Security techniques âĂŞ Information security management systems âĂŞ Requirements.* 2013.

69. ISO/IEC . *ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls.* 2013.

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

71. Kissel Richard, Stine Kevin M, Scholl Matthew A, Rossman Hart, Fahlsing James, Gulick Jessica. *NIST SP 800-64 Rev. 2 Security Considerations in the System Development Life Cycle.* : ; 2008.

72. Souppaya Murugiah, Scarfone Karen. NIST Special Publication 800-124 Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST special publication.* 2013;:30.

73. IEC . *Smart Grid.* 2018.

74. Ontario Smart Grid Forum . *Ontario Smart Grid Forum.* 2017.

75. OpenSG . *Security Working Group.* : ; 2017.

76. IEEE Standards Association . *IEEE Smart Grid Interoperability Series of Standards.* 2015.

77. National Institute of Standards and Technology . *NIST SP 1108r3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0.* : Na; 2014.

78. CEN-CENELEC-ETSI Smart Grid Coordination Group . *Smart Grid Set of Standards Version 3.1.* : ; 2014.

79. CEN-CENELEC-ETSI Smart Grid Coordination Group . *SG-CG/M490/H_Smart Grid Information Security.* : ; 2014.

80. European Commission . *M/490 Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment.* : ; 2011.

81. State Grid Corporation of China . *SGCC Framework and Roadmap to Strong & Smart Grid Standards.* : State Grid Corporation of China; 2010.