International Security Standards for Critical Oil, Gas, and Electricity Infrastructures in Smart Cities: A Survey Study

Cevat Ozarpa
Istanbul Technical University
106 PUBLICATIONS **474** CITATIONS

SEE PROFILE

M.Ali Aydin
Istanbul University
127 PUBLICATIONS **1,944** CITATIONS

SEE PROFILE

İsa Avci
Karabük University
102 PUBLICATIONS **294** CITATIONS

SEE PROFILE

International Security Standards for Critical Oil, Gas, and Electricity Infrastructures in Smart Cities: A Survey Study

Cevat Özarpa[1], Muhammed Ali Aydın[2],and İsa Avcı[2]

[1]Karabuk University, Engineering Faculty, Mechanical Engineering, 78050,
Karabuk, Turkey.
cevatozarpa@karabuk.edu.tr,
[2]Istanbul University-Cerrahpasa, Engineering Faculty, Department of
Computer Engineering, Avcılar, 34315, Istanbul, Turkey.
aydinali@istanbul.edu.tr, isaavci@ogr.iu.edu.tr

Abstract. International security standards used in smart grids, industrial control systems, and critical infrastructures have become important for institutions and organizations. Within the framework of these standards, it is aimed to increase the security and durability of smart networks, industrial control systems, and critical infrastructures. When determining the most useful best practice standards and guidance for implementing effective cybersecurity and information security, it is important to determine the role and scope of each, and how it will interact with other standards and guidance. Cybersecurity and information security standards are applied to all organizations in which they operate, regardless of sector and institution, regardless of their size. This study provides general information about international information and cybersecurity standards used and referenced in the detection and protection of security vulnerabilities in smart grids, industrial control systems, and critical infrastructure systems. In this study, we investigate 31 international security standards in smart grids, industrial control systems, and critical infrastructures concerning their origin country and publication date covering the years from 1971 to 2020. According to our research results, 22 security standards were developed in the USA.

Keywords: Smart Grids; Security Standards; Cyber Security; Energy Security

1 Introduction

Smart grids, industrial control systems, and critical infrastructures are important issues in many countries and throughout the world in the case of protection systems nowadays and the future. Many standards have been developed worldwide for the safe protection of critical systems by institutions. It should be made more reliable especially for vital systems. To protect such systems, the USA has been determined as a result of our research that European countries pay more attention to the development of these standards.

Protection of information assets, minimizing the risks faced by institutions, and ensuring business continuity is possible by implementing security standards with the support of senior management in institutions. When the available sources in the literature are researched and analyzed to ensure a high level of corporate information security, it is determined that there is no comprehensive and current study, the studies presented are not sufficient, mostly on commercial content or unreliable websites and brief information on how to protect them. Increasing system security in smart grids, industrial control systems, and critical infrastructures complies with international security standards. Besides, increasing safety on systems by complying with these standards plays an important role in reducing the environmental risk effects of energy that may occur in energy production.

Organizations, institutions, and industry firms are responsible for developing the level of risk they want to accept, which enables the information security officer to decide which risk reduction steps should be taken. Risk management is critical in industrial and smart grid systems environments. The established security standards define procedures to prevent and minimize the impact of certain events. Industrial systems such as ICS, critical infrastructures, smart grids, and SCADA will be discussed in the following sections, together with the security standards they need to reduce specific and uncertain risks [1].

Security standards are techniques that are usually introduced in published materials that try to protect the cyberspace of a user or organization. This environment includes users, networks, devices, all software, processes, information on storage or transfer, applications, services, and systems that can connect directly or indirectly to networks. The main purpose here is to reduce the risks, including removing vulnerabilities on these systems and preventing cyber attacks. These published materials consist of tools, policies, security concepts, security measures, guidelines, standards, risk management approaches, actions, training, best practices, assurance, and technologies [2].

In this study, 31 security standards are investigated around the world about smart grids, industrial control systems, and critical infrastructures. This review was made on security standards developed from 1971 to 2020. Also, in this study, the institution information belonging to the standards, the country, and the year of its extraction were investigated in detail. In this article, smart grids, Industrial Control Systems, and critical infrastructures are briefly described. With this study, the importance of such critical systems in terms of cyber and other security measures are emphasized. Also, the standards examined have been shown for which systems they are developed.

It is aimed to draw attention to critical infrastructures in researching smart grid, industrial control systems, and international security standards and to increase the security of the systems in these standards. Increasing the security level of these systems is directly proportional to the degree of compliance with the standards. In such critical systems, it is impossible to calculate environmental damage and the economic aspects of these damages when safety standards are not observed. Besides, life and property safety, global warming, environmental risks, and damages to living things are among the risks that may occur in these systems. It is impossible to estimate the extent of all these risks for the specified systems.

2 Smart Grids

Infrastructure services have an important position as an indispensable element for city life as given in Fig. 1. Control of these infrastructure services has gained vital importance due to the increase in the urban population. The growing population has made it impossible to use and control infrastructure without Information Technology (IT) applications [3].

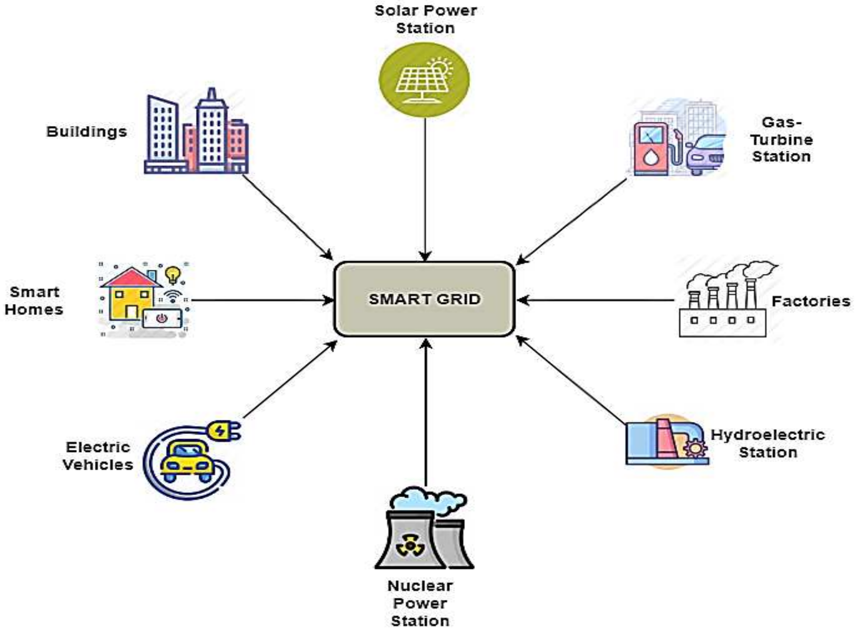

Fig. 1. Smart grid overview [4].

Infrastructure services have an important place as an integral part of urban life. Control over these infrastructural services has become vital with the growth of the urban population. A growing population has made it impossible to use and manage infrastructure without information technology (IT) applications. ISO (International Organization for Standardization), which deals with the optimal management of physical assets, states that infrastructure management should be holistic, systematic, risk-based, optimal, and sustainable. Organizational life plans are required through a foundation that manages structured and interconnected movements and systems of assets and institutions and monitors performance, risks, and costs throughout success [5]. This requires smart grids for systematic monitoring.

Intelligent Fieldbus communication is based on the IEC 61850 standard. The IEC 61850 substation protocol standard allows all protection, calculation, testing, and monitoring to be combined with a single standard protocol [6]. Otherwise, devices from different manufacturers will not be able to use a large number of protocols and interfaces that do not match or are not parallel to each other. In the technical field, equipment standardization and interoperability have been applied for a long time [7].

One of the most important contributions of smart grids is to protect the environment in terms of global warming and to prevent the energy used to be released into the environment. With this approach, the existence of smart grids is vital for the environment. All countries around the world determine their international strategies in terms of smart grids [8].

Smart grids are at the core of energy recovery, efficient use of energy, providing a livable world to future generations, and contributing to preventing global warming. Considering the overall environmental benefits of Smart Grids, energy efficiency, delaying new power plants and transmission lines, distributed generation, mass-scale renewables, clean power market, consumer incentive for conservation, support for more intelligent appliances at the demand-side, demand response for managing We can specify air pollution and advanced metering as a method of calculating environmental footprints [9].

3 Industrial Control Systems

Industrial Control Systems (ICS) are used globally in various industries to automate and control production plants. ICS industries include electricity, water, wastewater, food, and transportation [10]. It is a generic term that includes many control systems, including industrial control systems (ICS), control and data acquisition systems (SCADA), distributed control systems (DCS), and programmable logic controllers (PLC) [11].

Systems exist in many areas such as oil, chemical, electrical, and gas facilities that form the backbone of critical infrastructure. Site operators are constantly monitored and monitored by many different parts of the facility to ensure that their production systems are working properly.

In recent years, industrial control systems have become important due to the development of remote control systems, network technologies, and industrial equipment. ICS is control and monitoring networks and systems designed to support production processes. The largest subgroup of ICS is SCADA (Controller Control and Data Acquisition) systems.

ICS includes industry-standard technologies that are closely related to isolated systems, open architectures, and other corporate networks and the Internet. ICS products today are mainly based on standard embedded systems platforms applied to various devices such as routers or cable modems. Besides, these systems usually use the commercially available software. All of this has resulted in cost savings, ease of use, and remote control and monitoring from multiple locations. However, the main disadvantage of connecting to intranets and communication networks is the increased vulnerability to computer attacks.

ICS is critical to the operation of critical US infrastructures, which often have highly interconnected and interdependent systems, as shown in Fig. 2. It is important to note that approximately 85 percent of the country's critical infrastructures are privately owned and operated. Federal agencies also manage most of the manufacturing processes mentioned above and air traffic control. This section provides an overview of SCADA, DCS, and PLC systems, including typical topologies and components. To facilitate the understanding of these systems, various diagrams are presented showing the network topology, connections, components, and protocols available in each system. These examples only attempt to define conceptual concepts of topology. Real applications of ICS can be hybrids that blur the line between DCS and SCADA systems [12].

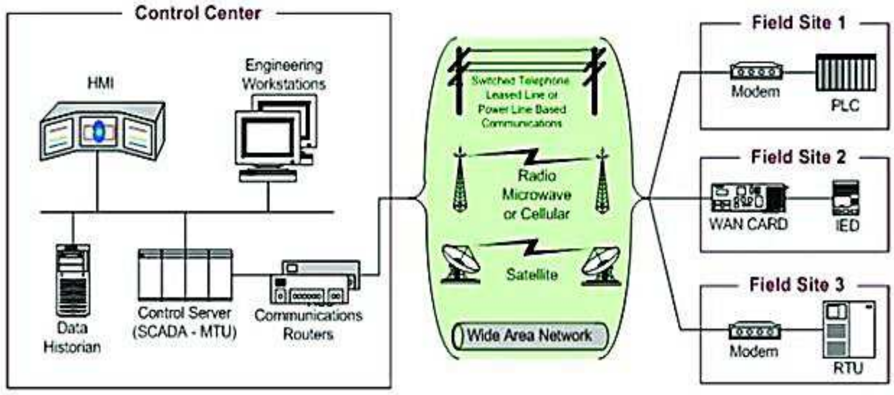

Fig. 2. Overview of industrial control systems [13].

The term "Industrial Control System" is broad; Specific examples of the ICS can be referred to as Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Energy Management Control System (EMCS), Emergency Medical Service (EMS) terms or other, but they can all perform the same basic function. Hardware components that make up an ICS are classified as operational technology (OT) According to information technology (IT), which usually refers to computer equipment on almost every table. While ICS elements are mostly composed of electro-mechanical devices, some are other field devices and control computers that communicate with other computers in the system with minimal human interaction [12].

4 Critical Infrastructures

The critical infrastructure includes all energy-related generation and storage facilities, transmission lines and routes, and consumption facilities and systems as illustrated in Fig. 3. Platforms and natural gas wells used in the production of energy sources such as oil and natural gas, all pipelines and LNG terminals from the main transmission lines that play a role in the transportation of these resources to the secondary transmission lines reaching the homes, tankers, refineries, pump stations, renewable energy facilities, dams and conversion power generation control, and protection systems, nuclear power plants, and all kinds of power generation systems, including power plants [14].

The critical infrastructure consists of three main parts: natural gas, oil, and electricity [4]. These are the basic vital elements of world society and the needs for these elements for the future should be taken into consideration. It is essential to implement a sustainable, environmentally compatible safety rule and policy based on uninterrupted flow and supply security and non-leakage in oil and gas pipeline facilities [15].

The economic welfare and development of the modern state, the use of advanced technology, and the development of the level of production and development to ensure the effective use of energy resources and infrastructure security is an indispensable element of national security policies [16]. In addition to coal, oil, and natural gas, the widespread use of nuclear energy, the information technologies that ensure the use of energy and the critical infrastructures that make up the distribution systems, ensure the safety and security of the critical infrastructures, making the continuous flow of fuel, gas, and electricity used in daily life. The International Energy Agency (IEA) redefines the three vital elements of balanced energy policies as energy security, economic development, and environmental protection [17].

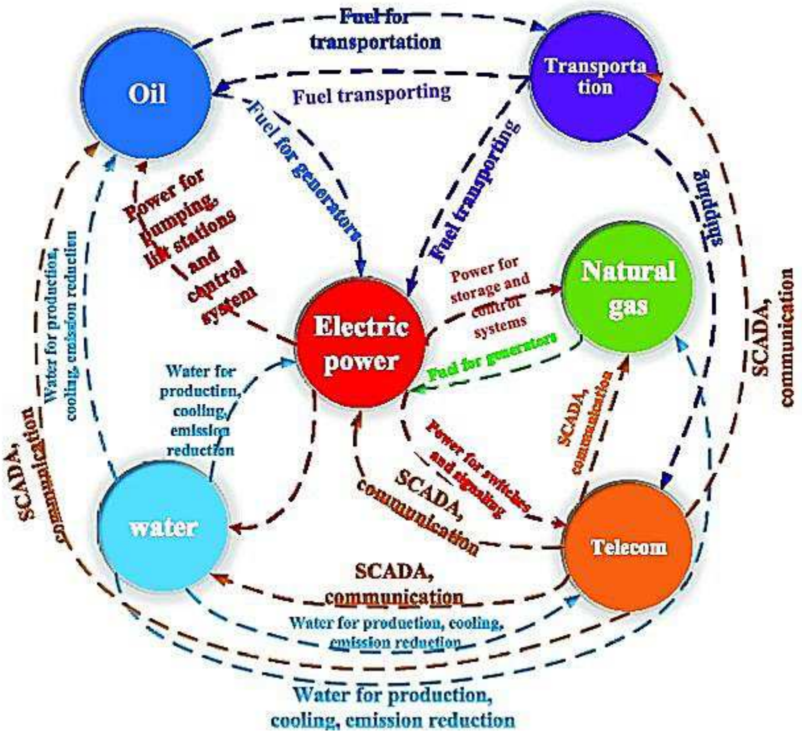
Fuel for transportation
Transporta tion
Oil
Fuel transporting
Fuel for generators
Fuel transporting
shipping
Power for pumping, lift stations and control system
Natural gas
Power for storage and control systems
Fuel for generators
Electric power
Water for production, cooling, emission reduction
Water for production, cooling, emission reduction
SCADA, communication
SCADA, communication
Power for switches and signaling
SCADA, communication
SCADA, communication
water
SCADA, communication
Telecom
SCADA, communication
Water for production, cooling, emission reduction
Water for production, cooling, emission reduction

Fig. 3. Overview of critical infrastructures [18].

Critical infrastructure security covers the sectors listed below. Also, it is important for the safety and security of these sectors and environmental compliance and controls.

- The sector of chemical
- The sector of commercial facilities
- The sector of communications
- The sector of critical manufacturing
- The sector of dams
- The sector of defense industrial base
- The sector of emergency services
- The sector of energy
- The sector of financial services
- The sector of food and agriculture
- The sector of government facilities
- The sector of healthcare and public health

- The sector of information technology
- The sector of nuclear reactors, materials, and waste
- The sector of transportation systems
- The sector of water and wastewater systems

5 Investigation of International Security Standards

International safety standards are the techniques described in the critical systems of a user or organization and the materials published in general to protect the environment. This environment includes users themselves, networks, devices, all software, processes, and information in systems that can be connected directly or indirectly to storage or transportation, applications, services, and networks. The main goal is to reduce the risks that organizations have, including preventing or reducing their environmental impact from malicious attacks. These include published materials tools, policies, security concepts, security measures, rules, risk management approaches, actions, training, best practices, assurance, and collections of technologies.

Our study explores the international security standards developed worldwide, from 1971 to 2020, and details are provided in Table 1 below. Also in this table, the publication date, year, institution information, and explanation of the standards are given in historical order. This study covers cybersecurity, information security, business continuity, and security developed especially for smart grids, critical infrastructures, and ICS.

Table 1. International Security Standards

	Standards	**Description**	**Year**	**Institution**	**Country**
1	ILTA	The LegalSEC of the International Legal Technology Association provides the legal community with guidance for risk-based information security programs [19].	1971	ILTA	USA
2	NIST SP 800	Publications in NIST's Special Publications (SP) 800 series provide information that concerns the computer security community. This series includes the guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities [11].	1990	NIST	USA

3	ISO/IEC 27031	This Standard closes the gap between the event itself and overall business continuity and creates a key link in the cyberspace flexibility chain [20].	2000	ISA	USA
4	DHS	Department of Homeland Security- It is a security standard that provides advice to developers to increase security in ICS systems of various industrial organizations [21].	2002	DHS	USA
5	BSIMM	Building Security in the Maturity Model is geared towards software security and provides a framework for organizing a range of activities to help manage and measure enterprise security initiatives [22].	2006	BSIMM	USA
6	IEC 62351	IEC 62351 is an industry-standard aimed at improving safety in automation systems in the field of power systems [23].	2007	IEC	Switzerland
7	CIS 20	The Internet Security Center has a standard 20 control that is originally developed by SANS [24].	2008	CIS	USA
8	ISO/IEC 15408:2009	ISO / IEC 15408 defines the software and hardware security evaluation criteria of these standard information security devices consisting of 3 standards: information technologies, security techniques, and evaluation criteria for information security [21].	2009	ISO	Switzerland
9	NRC RG 5.71	Cybersecurity of nuclear infrastructures [25].	2010	NRC	USA
10	RFC 6272	This is the identification of internet protocols for the smart grid [26].	2011	RFC	USA
11	ISO/IEC 22301	ISO / IEC 22301 is an international standard for business continuity management systems (BCMS) and forms the final part of cyber flexibility [20].	2012	ISO	Switzerland
12	ISO/IEC 27001	It is a meticulous and comprehensive guide to protect your information within the principles of privacy, integrity, and usability [20].	2013	ISA	USA

13	ISO/IEC 27002	It provides helpful, practical guidance on the implementation of ISO / IEC 27001 [20].	2013	ISA	USA
14	PAS 555	PAS 555 adopts an approach to explain the appearance of effective cybersecurity and can be used to verify that solutions are comprehensive [20].	2013	BSI	England
15	IEEE 1686-2013	IEEE standard for intelligent electronic devices' cybersecurity capabilities [27].	2013	IEEE	USA
16	NERC CIP	NERC has approved version 5 of critical infrastructure protection cybersecurity standards (CIP Version 5), which represents significant progress in reducing cyber risks to the collective power system [28].	2013	NERC	USA
17	NIST SP 800-53	This publication provides a catalog of security and privacy controls for federal information systems and organizations and various threats such as organizational operations, organizational assets, individuals, other organizations and hostile cyber-attacks, natural disasters, structural failures, and human errors [11].	2013	NIST	USA
18	NISTIR 7628	NISTIR 7628 is a comprehensive document for security designers/practitioners in smart grid research and implementation. NISTIR 7628 covers top-down and bottom-up approaches in risk assessments and security analysis [11].	2014	NIST	USA
19	IEEE C37.240	This standard is the cybersecurity of communication systems [27].	2014	IEEE	USA
20	VGB R175	This is cybersecurity requirements for power plants [29].	2014	VGB	Germany
21	IEEE 2030-2011	This is energy storage systems' interoperability [27].	2015	IEEE	USA

22	NIST SP 800-82 Rev. 2	This document Audit SCADA systems, DCS and PLC such other control system configurations, including the unique performance, reliability, and security requirements in terms of Industrial Control Systems (ICS) on how to protect provides guidance [11].	2015	NIST	USA
23	ISO/IEC 27035	ISO / IEC 27035 is an international standard for incident management. This standard also includes guidance to update policies and processes and to minimize the risk of repetition to strengthen existing controls following analysis of the event [30].	2016	ISA	USA
24	ISA/IEC 62443 (ISA99)	The ISA99 committee will set up standards, proposed practices, technical reports, and related information to define procedures for the implementation of electronically safe production and control systems and safety practices and the evaluation of electronic safety performance [31].	2017	ISA	USA
25	ISO/IEC 27019:20 17	It guides the control of processes applied to process control systems used in the energy company industry for the production, transmission, storage, and distribution of electrical energy, gas, oil, and heat [30].	2017	ISA	USA
26	CSA V4.0	The Cloud Security Alliance provides Security Guidelines for Critical Focus Areas in Cloud Computing v4.0 to increase security and reduce risk in the adoption of cloud computing technologies [32].	2017	CSA	USA
27	BS 7799-3 2017	Information security management systems and Guidelines for information security risk management [33].	2017	BSI	England

28	NIST 800-53/CSF	Special Publication 800-53 of the National Institute of Standards and Technology (NIST) provides controls for federal information systems but can be used by commercial organizations [11].	2018	NIST	USA
29	ISO 15118-1:2019	This is vehicle-grid communication [30].	2019	ISO	Switzerland
30	GB/T22239:2019	GB/T22239 is the "Information Security Technology-Basic Rule for Classified Protection of Information System Security" [21].	2019	GB	China
31	IEC 61850:2020	The IEC 61850 standard has been developed to standardize communication in the high-voltage substation [23].	2020	IEC	Switzerland

It gives detailed information about international security standards in our practice. The security standards of these critical systems, especially mentioned in our study, appear to have been established by the ISA institution in the USA. For this reason, the importance and benefit of the USA on security arise. When their studies are investigated, it is observed that the threats of cyber attackers continue to increase, as they depend on technology in terms of greater confidence in the global world. Emerging cyber threats lead to large-scale cyberattacks, which can harm the critical infrastructures of countries. It is possible to argue that the wider adoption and implementation of cybersecurity and information security standards will contribute to the critical infrastructure of countries and provide better flexibility. This could lead to a country's security strategy to have higher success against threats that no longer pursue national borders. This may link global society to a common defense and better cooperation and the ability to respond to globally developed cyber resilience.

To achieve an international security standard, the followings shall be taken into account [34]:

- Determine the right standards for the organization or information systems.
- Become familiar with this security standard.
- Interact with organizations that know this security standard, and/or use an external consultant within the company.
- Identify the gaps in your organization that are not currently in compliance with the standard and develop a plan to address these gaps.
- Contact a certification body.

International security standards offer us a common set of reference points that enable us to assess whether an organization with information technology systems has processes, procedures, and other controls that meet an agreed minimum requirement. If an organization is compliant / meets a certain standard, it gives confidence to third parties, such as customers, suppliers, and business partners, about that organization's ability to deliver it to that standard. It can also provide an organization with a competitive advantage over other organizations. For example, systems of an organization that comply with a security standard may have an advantage over competitors who do not evaluate customers' products or services.

Conclusions

International security standards aim to increase the security and durability of equipment and software used in smart grids, critical infrastructures, and industrial control systems, while also minimizing the effects of security risk. We see that the application of security standards established at both domestic and international level is high. Our aim in this study is to indicate how important countries are to protect the security of critical systems and by which countries more studies are carried out for these security standards.

In this academic research study, international standards on cybersecurity and information security issues developed from past to present are researched and given according to historical order. This study covers 26 international cybersecurity and information security standards used in smart networks, critical infrastructures, and industrial control systems. Besides, this study shows in which year and countries the standards created were developed. In particular, this research paper shows that 22 of the studies were developed in the USA, while others were developed in Switzerland, the UK, and China. In the evaluation, we have made as a result of this study, we suggest that countries that have not done any work in the international security standards studies should support the countries that work.

In this study, it is also envisaged that system security is not a product or service, it is a live process that follows the safety standards in the human factor, technology, and education triangle and high-security level cannot be mentioned unless these three elements are complementary. Finally, to ensure that researchers guide their academic work by applying standards that are specially prepared in the related fields on cybersecurity and other security issues. Also, our work contributes to taking security measures in critical systems used by institutions and reducing their environmental impact.

Acknowledgments

We would like to thank Istanbul-Cerrahpaşa University and Karabuk University

computer engineering departments and institutions for their support in conducting this study.

References

1. Clayborn, A.,"Security Standards for ICS & SCADA: Types & Overview.", study.com/academy/lesson/security-standards-for-ics-scada-types-overview.html, (AT 03.07.2020).
2. Leszczyna, R., Standards on Cyber Security Assessment of Smart Grid. International Journal of Critical Infrastructure Protection, 10.1016/j.ijcip.2018.05.006, 2018.
3. Nam, T., & Pardo, T. A., Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times (pp. 282–291), ACM, 2011.
4. Feroze, F., Javaid, N., Towards Enhancing Demand Side Management using Evolutionary Techniques in Smart Grid. 10.13140/RG.2.2.34456.49920, 2017.
5. Minnaar, J. R., Basson, W., and Vlok, P. J., Quantitative methods required for implementing pas 55 or the ISO 55000 series for asset management. South African Journal of Industrial Engineering, 24(3):98-111, 2013.
6. Baigent, D., Adamiak, M. and Mackiewicz, R., IEC 61850 communication networks and systems in substations: an overview for users, 2004.
7. Dönmez, M., Smart grids, and integration, BTC Business Technology, 2013.
8. Elder,http://www.elder.org.tr/Content/yayinlar/TAS%20TR.pdf, (AT 01.07.2020).
9. Smart-energy, https://www.smart-energy.com/opinion-pieces/smart-grid-environmental-benefits/#:~:text=It%20takes%20a%20Smart%20Grid,reduced%20pollution%20%E2%80%94%20stating%20the%20benefits.&text=Energy%20efficiency%20%E2%80%93%20Increased%20asset%20utilization,operation%20and%20fewer%20peaking%20units, (AT 28.06.2020).
10. Stouffer, K., Falco, J., and Scarfone, K., Guide to industrial control systems (ICS) security. NIST Special Publication, 800. 82, 2013.
11. NIST, https://nvd.nist.gov/, (AT 23.06.2020).
12. ENISA, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada, (AT 02.02.2020).
13. Holm, H., et al., A survey of industrial control systemtestbeds. In: Buchegger, S., Dam, M. (eds.) Secure IT Systems. Lecture Notes in ComputerScience, pp. 11–26. Springer, Heidelberg, 2015.
14. Özertem,H.S.,https://www.academia.edu/2449511/Critical_Energy_Insrastructure_Project_Final_Report_Kritik_Enerji_Altyap%C4%B1_G%C3%BCvenli%C4%9Fi_No_3, 2012.
15. The White House, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences’, pp. 5-6, 2003.
16. Caşın, M.H., Critical Energy Infrastructure Security and Institutional Framework, Hazar Strateji Enstitüsü, İstanbul, pp. 5-6, 2014.
17. CRS Report for Congress, ‘Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences’, pp. 5, 2005.
18. Bie, Z. , Li, Y. et al., Battling the Extreme: A Study on the Power System

Resilience, Proceedings of the IEEE, pp. (99):1-14., 2017.

19. Iltanet, https://www.iltanet.org/resources/legalsec, (AT 08.01.2020).
20. Itgovernance, https://www.itgovernance.co.uk/cybersecurity-standards (AT 10.01.2020).
21. Timpson D., Moradian E., A Methodology to Enhance Industrial Control System Security, 22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Procedia Computer Science 126 (2018) 2117–2126, 2018.
22. BSIMM, https://www.bsimm.com/framework.html, (AT 05.01.2020).
23. Ipcomm, https://www.ipcomm.de/protocol/IEC62351/en/sheet.html, (AT 11.01.2020).
24. Cisecurity, https://www.cisecurity.org/controls/, (AT 18.01.2020).
25. NRC, https://www.nrc.gov/docs/ML0903/ML090340159.pdf, (AT 15.07.2020).
26. RCF, https://www.rfc-editor.org/info/rfc6272, (AT 16.07.2020).
27. IEEE, https://standards.ieee.org/standard/C37_240-2014.html, (AT: 20.07.2020).
28. NERC, https://www.nerc.com/pa/CI/Pages/Transition-Program.aspx, (AT 09.01.2020)
29. VGB, https://www.vgb.org/shop/s-175e-ebook.html, (AT 23.07.2020).
30. ISO, https://www.iso.org/standard/68091.html, (AT 08.01.2020).
31. ISA, https://www.isa.org/isa99/, (AT 08.01.2020).
32. NIST,https://csrc.nist.gov/publications/detail/nistir/7628/archive/2010-08-31, (AT 08.01.2020).
33. Eia, https://www.eia.gov/outlooks/ieo/, (AT 03.07.2020).
34. Mutasim, M. et al., Novel Approach of Quantifying Energy Security in terms of Economic, Environmental and Supply Risk Factors, Journal of Advanced Research in Fluid Mechanics and Thermal Sciences 57, Issue 1 (2019) 100-109, 2019.