

CYBER SECURITY RISK ANALYSIS AND TECHNICAL DEFENSE ARCHITECTURE RESEARCH OF ICS IN NUCLEAR POWER PLANT CONSTRUCTION STAGE

YUN GUO

Huaneng Shandong Shidao Bay Nuclear Power Company
Rongcheng, ShanDong Province, China
Email: guoyun_2018@163.com

XINXIN LOU

Bielefeld University
Bielefeld, Germany

EDITA BAJRAMOVIC

Friedrich Alexander University Erlangen-Nuremberg, Department of Computer Science
Erlangen, Germany

KARL WAEDT

Framatome GmbH
Erlangen, Germany

Abstract

The stable operation of ICSs (Industrial Control System) directly affects the safe production of NPPs (Nuclear Power Plants). With the frequent cyber attacks aiming at ICSs, cyber security is becoming an important factor affecting nuclear safety. With the continuous development of the digitalization and networking of devices in current industry, the cyber security of ICSs in NPPs is facing unprecedented challenges. Therefore, it is necessary to take cyber security into consideration since the NPPs planning and construction stage. In the paper, we analyze the cyber security risks from elements of threats and vulnerability that are faced by ICS during the construction phase from the perspective of the business owner of NPPs. In addition, we propose technical defense architectures respectively for newly built NPPs and NPPs being built, by combining the related standards and guidelines. At last, the paper proposes building ICS cyber security test platforms based on digital twin to verify the feasibility of the defense architecture.

1. INTRODUCTION

In the past, the ICSs of NPPs were considered as relatively safe because they were isolated from the outside world and used specialized hardware and software to run proprietary protocols. However, with the higher degree of industrial digitalization and networking, the Windows OS and industrial Ethernet based on IEEE802.3 have been widely used in ICSs. This causes ICSs are becoming open and facing unprecedented security threats. From the "Stuxnet" incident [1] in Iran to the recent power blackout in Venezuela [2][3], the cyber security of ICSs in power plants is facing more and more challenges. Cyber security has become an essential part of production safety, the violation of security in critical ICSs of NPPs can directly cause reactor shutdown events, which will lead to nuclear safety issues. Therefore, it's essential to take cyber security into consideration when an NPP is in construction stage. There are two types with regarding to NPPs under construction, which are newly built ones and ones being built. For NPPs belonging to the first type, cyber security can be considered from the design phase, which means that all the critical ICSs of an NPP can be planned and designed from a perspective of integration and systematization, thus a reasonable technical defense architecture may be adopted. For NPPs belonging to the second type, due to the lack or deficiency of cyber security factor in the early stage, along with the high capital and time costs of redesigning ICSs, so it is necessary to study the defense architecture under the premise of the availability of ICSs according to the existing situation. In addition, being different from the priorities of three elements referred as CIA (Confidentiality, Integrity and Availability) of information security in the management network, ICSs have higher requirements on the availability, real-time, controllability, which means priority should be given to availability when carrying out the defense architecture against the cyber attacks. Therefore, it is

essential to develop a test platform for ICSs of NPPs so that all the changes related to ICSs especially those in relation to cyber security can be fully tested before they can be applied into the real environment with no damage and degrading to the availability of ICSs.

2. STANDARDS RELATED TO ICS CYBER SECURITY OF NPP

As the importance of increasing cyber attacks, to regulate the cybersecurity issues in nuclear and other industrial domains, international or national committees developed some guidances and standards, such as RG 5.71[4], IEC 62645[10]. Some of them are selected and classified as showed in Table 1.

TABLE 1. SELECTED STANDARDS RELEVANT WITH CYBER SECURITY

Series number	Content and applicable domain	Safety/security
IEC 62645	Requirements for security program of I&C (Instrumentation & Control) systems in NPPs	Cyber security relevant
IEC 62443	Secure development life-cycle requirements of IACS	Cyber security relevant
NIST SP800-82	A guidance on creating secure ICS	Cyber security relevant
NRC RG5.71	Special guidance of protection of digital assets related to nuclear facilities	Cyber security relevant
IAEA NSS 17	technical guidance on implementing a computer security programs	Cyber security relevant
IAEA NSS 20	Basis for Nuclear Security Recommendations	Cyber security relevant
SAC GB/T 22239-2019	Baseline for Classified Protection of Cybersecurity applicable to cyber security of all industries	Cyber security relevant
IEC 62859	Requirements of integrating safety and cybersecurity for I&C systems and architectures	Safety and cyber security integrated
IEC 63069 (still updating)	Applicable in process industry, as a framework for functional safety (IEC61508) and security (IEC62443)	Safety and cyber security integrated

2.1. RG 5.71

US NRC RG 5.71 is a computer security guide developed by the U.S. Nuclear Regulatory Commission (NRC) for the protection of digital computers, communication systems and networks in accordance with federal regulations, and is intended to ensure digital facilities and communications related to nuclear facilities. The guidelines develop a cyber security plan based on the identification of CDAs (Critical Digital Assets) to establish, implement and maintain cyber security procedures. The core idea of RG 5.71 is to establish a defense-in-depth architecture to ensure the ability to detect, prevent, respond, mitigate and recover for CDAs. It recommends a possible architecture which divides security levels of ICS into five security levels and describes the security requirements and principles between different levels, yet it doesn't define the concrete security controls of each level.

2.2. IEC series of standards

In 2014, IEC issued IEC 62645 which focuses on the issue of requirements for computer security programs and system development processes to prevent and/or minimize the impact of cyber attacks against computer-based I&C systems. The primary objective of this standard is to define adequate programmatic measures for the prevention of, detection of and reaction to malicious acts by digital means (cyber attacks) on I&C (Instrumentation and control) possibly integrating HPD (Hardware Description Language - Programmed Devices) systems. IEC 62645 Ed2, issued end of 2019, divides the security level of ICS into BR (Baseline Requirements), S3, S2 and S1,

yet it doesn't define security measures for each system individually. At the level of IEC 62645, as top-level Nuclear IEC cybersecurity standard, this would lead to a great amount of studies along with the cost and to many problems to connect communicating systems, which would be too detailed at the top-level. It puts an emphasis on requirements related to the communication between systems and system-related security requirements.

IEC 62443 aims at providing guidelines about manufacturing and control systems security, dealing with various categories of systems, facilities, and plants in different industries. The concept of SL (Security Levels) was introduced on the basis IEC 62443-3-3 and IEC 62443-4-2 and the related ML (Maturity Levels) on the basis of IEC 62443-2-4 and IEC 62443-4-1. A qualitative approach can be taken to deal with ICS network security issues based using the SL and ML grading.

The above multipart IEC 62443-x-x standards apply to ICS in multiple industries, while the IEC 63096 under development is a customized standard for ICSs in NPPs. It addresses the lack of detailed, graded and lifecycle-specific security guidance for NPPs. IEC 63096 provides 14 security controls clauses that, together, contain 35 main security categories and 114 controls to guide how to deploy security measures in NPPs. IEC 63096 is specified as a third level IEC SC45A document. It is intended for an audience of designers and operators of NPPs, vendors and subcontractors, licensors, and system evaluators.

2.3. NSS series

NSS (Nuclear Security Series) is a publication issued by IAEA (International Atomic Energy Agency) to provide international consensus guidance on all aspects of nuclear security to support States as they work to fulfil their responsibility for nuclear security. Among those, NSS 17, 20,23 are close related to cyber security of NPPs.

NSS 20 specifies the nuclear security fundamentals which set requirements for the essential elements of a state's nuclear security regime including the legislative and regulatory responsibilities. It provides for the establishment of regulations and requirements for protecting the confidentiality of sensitive information and for protecting sensitive information assets.

NSS 17 is a technical guidance which provides guidance specific to nuclear facilities on implementing a computer security programs and evaluating existing programs.

NSS 23 is an implementation guide which provides guidance on implementing the principle of confidentiality and on the broader aspects of information security such as integrity and availability. It assists States in bridging the gap between existing government and industry standards on information security, the particular concepts and considerations that apply to nuclear security and the special provisions and conditions that exist when dealing with nuclear material and other radioactive material.

2.4. Classified protection of cyber security in China

Beginning in 1994 with the State Council's Decree "Regulations on the Security Protection of Computer Information Systems of the People's Republic of China", China's classified protection of cyber security was gradually promoted in an orderly manner and was fully applied in various industries. The security level is determined by two dimensions. One dimension is the importance of the object in national security, economic and social life. The other dimension is the degree of damage to the national security, social order, interests of citizens, legal persons and other organizations when the object is destroyed. Each level corresponds to different control measures in terms of management requirements and technical requirements.

In May 2019, China issued a series of standards for classified protection 2.0. The main differences between the new series and the previous series include:

- (a) The new standards expand the scope incorporating cloud computing, mobile internet, Internet of Things, ICS etc. into the scope of standards.
- (b) It is now recommended to use the triple protection architecture supported by secure communication network, secure boundary and secure computing environment along with the management center.
- (c) The requirements of TC (Trusted Computing) technology are strengthened in this version.

3. CYBER SECURITY RISK ANALYSIS OF ICS IN THE CONSTRUCTION STAGE

3.1. Critical digital assets identification

The main difference between NPPs and general thermal power plants in ICS is that some ICSs of NPPs perform SSEP functions which refers to safety, security, and emergency preparedness. According to RG 5.71, these systems are called critical digital assets (CDAs). In the construction phase, the business owner (future NPP operator) should advise the general contractor to identify all the CDAs and determine the security level of each system so that different security zones can be divided. Furthermore, risk analysis can be done based on the security level ranging from level 4 to level 0 of which level 4 requires the highest protection.

The Classified Protection Regulation of China also provides a method to define the protection level of each digital asset. Different security levels correspond to different protective measures which are detailed in the pertinent standard. Using this method, there are also five levels for the protected objects ranging from level 1 to level 5 of which level 5 requires the highest protection. In RG 5.71, the security level is determined by the importance related to SSEP whereas in China's Classified Protection Regulation, the security level is determined by two dimensions mentioned in 2.4. This paper suggests that we could establish the correspondence or a mapping between these two security levels to assist the identification of the CDAs.

3.2. Threats of critical ICS

This paper suggests that two dimensions are used for threats identification according the sources, which are external/internal factor and human/non-human factor. The threats of critical ICSs can be divided into four types including external human, external non-human, internal human and internal non-human factors. From the aspects of motivation, intention and ability, of all the four kinds of threats, the biggest threats are respectively the Advanced Persistent Threat (APT) due to political factors (external human factors), various natural disasters such as earthquakes and tsunamis (external non-human factors), deliberate destruction from internal employees or contractor personnel (internal human factors) and equipment or system failure (internal non-human factors).

3.3. Vulnerabilities of critical ICS

There are commonly six main approaches used in vulnerability analysis, which are respectively cause-based, threat-based, impact-based, attack-based, repair-based, and location-based approaches[16]. The paper uses a threat-based approach to analyze and identify the vulnerability of critical ICS.

The main vulnerability for ICS of NPPs is detailed in TBALE 2.

TABLE 2. VULNERABILITY IDENTIFICATION USING THREAT-BASED APPROACH

Threats	Vulnerabilities
external human threat	no access control or very weak
	staff have no cybersecurity awareness or very little
	no physical protection measures or very weak
	no valid identity authentication mechanism
	lack of information protection
	system or software has vulnerability
	lack of border protection
	susceptible to virus infection
	unable to guarantee the security of the computing environment from start to end
	internal human threat
	unable to guarantee the security of the computing environment from start to end

external threat	non-human	located in areas vulnerable to natural disasters with poor resistance mechanism poor physical environment conditions, such as improper temperature and humidity and assets are susceptible to these conditions
internal threat	non-human	lack of redundant design lack of operational status monitoring and early warning

4. TECHNICAL DEFENSE ARCHITECTURE RESEARCH

Because of the long construction cycle of an NPP, it will take huge cost to change the defense architecture after it was confirmed in the design phase. Therefore, it is necessary to study the cyber security defense architecture of ICS in newly built NPPs and NPPs being built respectively.

4.1. Technical defense architecture for critical ICSs in newly built NPPs

Traditional defense architecture for ICSs is commonly based on passive defense mode which consists of firewall, host-based antivirus software and IDS (Intrusion Detection System). This architecture has the following problems:

- (a) It fails to prevent attacks in advance because passive detection only acts when an attack occurs. For example, when an IDS alarmed, it means that an attack is moving on.
- (b) Host-based antivirus software and terminal control software need to be installed on the ICS and may be incompatible with the ICS host, which may result in failure to deploy.
- (c) Unlike the centralized deployment of the flow analysis software in the management network, the ICSs are usually networked independently, so multiple security devices need to be deployed when using this architecture, resulting in a dramatic increase in maintenance workload.
- (d) Early industrial control protocols were designed on the basis of physical isolation, the cyber security issues were not fully considered. Most industrial control protocols are lacking security mechanisms such as integrity, encryption and identity authentication, which could not effectively deal with issues of monitoring and identity forgery[17].

For newly built NPPs, in response to the above problems, we propose to adopt TC (Trusted Computing) [18][19]technology when ICSs are designed. What is a TC? Starting from the initial "trust root", TC technology can pass "the trust" using "chain of trust" when the platform environment performs each conversion, which thus ensures that the computing environment of the platform is always trustworthy. TC technology has the following advantages[19][20]:

- (a) TC ensures that the entire system is always in a trusted environment and achieves active defense against attack events.
- (b) ICSs designed with TC technology no longer needs to deploy host-based antivirus software, which can avoid compatibility issues and greatly reduce the maintenance workload of security equipment.
- (c) TC technology ensures that the system is always in a trusted environment, preventing vulnerable industrial protocols from being intercepted or tampered with.

In summary, for newly built NPPs, this paper suggests a possible technical defense architecture that can be designed as described in Fig. 1.

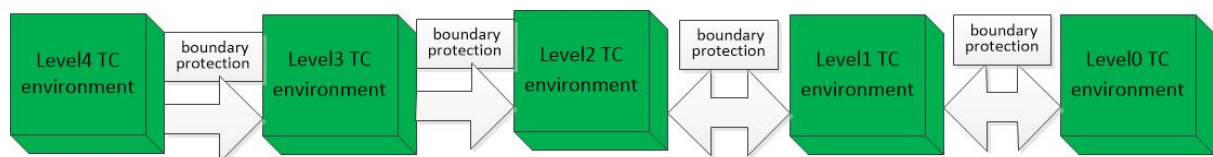


FIG. 1. Defense architecture for newly built NPP

The architecture in Fig. 1. uses the defense-in-depth motif recommended by RG 5.71 and IEC 62443. It is based on the simplified cyber security defensive architecture given by RG 5.71 and makes improvement by using the combination of inherent security and boundary security ensures the security:

- (a) It uses boundary protection technology to ensure boundary security. For example, A firewall can be deployed to achieve logical isolation between security zones that allow two-way data interaction; diodes (physically unidirectional security gateways) or air gaps can be deployed to achieve strong isolation between security zones that only allow one-way data flow.
- (b) Designing and implementing an ICS using TC technology can ensure its inherent security. By encapsulating CPU, memory, a root of trust for measurement, a root of trust for storage, and a root of trust for verification in ICS hardware, malicious code execution can be prevented. For example, PLCs of NPPs often need to be controlled and diagnosed by the lower computer, and the attacker can use the vulnerability of the lower computer to attack the PLC. If the PLCs are designed and implemented by the TC technology, such attacks can be prevented because of the malicious code can't be executed in the trusted environment.
- (c) When an attacker exploits a vulnerability of a system located in a low-security level zone to infiltrate an ICS located in a high-security level zone, it will be first prevented by the boundary protection control. If this control fails, the malicious code still cannot be executed within the system as stated in above (b), thus forming a defense-in-depth architecture. Such design can effectively address risks mentioned in section 3.3 except risks caused by the exploiting of vulnerability by external non-human threats.

4.2. Technical defense architecture for critical ICS in nuclear power plants being built

For plants being built, replacing the existing ICS with a new system designed and developed with TC technology will increase the cost and the compatibility risk, and may affect the overall construction progress and timescale of a NPP. Referencing the requirements especially the extension requirements for ICS of classified protection of cyber security (version 2.0) in China[24], the paper proposes a semi-active defense architecture based on secure communication networks, boundary protection and secure computing environments which can detect and block threats in time. The architecture is detailed in Fig. 2.

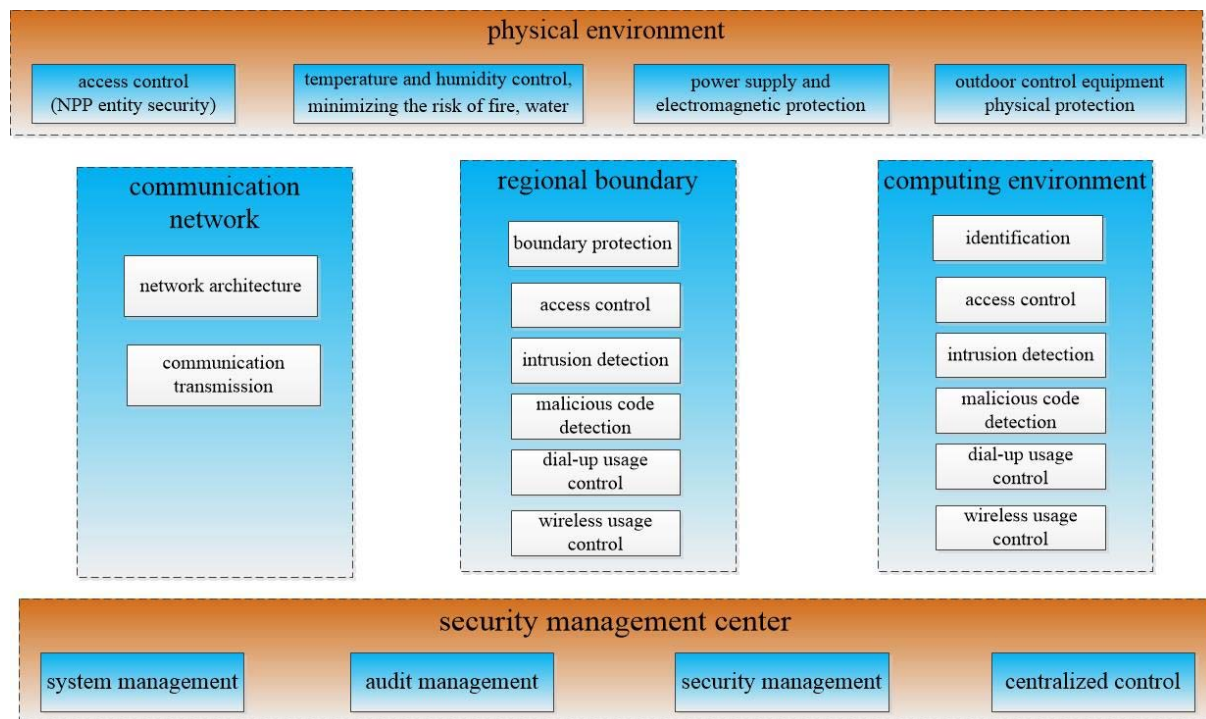


FIG. 2. Defense architecture for NPPs being built.

This architecture uses the "triple protection and one center" approach to ensure cyber security and builds a semi-active defense-in-depth system.

- (a) The communication network provides a secure network link for ICS. It requires reasonable network division and design of network equipment redundancy. Integrity enforcement, authentication, encryption and other measures are needed to ensure the security of communication transmission.
- (b) The secure regional boundary is used to ensure the control of the data flow between different security zones. The firewall can be used to achieve the border access control. IDS exclusive for ICS can detect the attack behavior in time, and the auditing system can be deployed at the border to audit the access behavior of all users. For ICS, special control over wireless networks and dial-up networks is required. For example, an ICS that uses wireless communication technology needs to identify unauthorized wireless devices that are launched in its physical environment and report unauthorized attempts to access or interfere with the ICS.
- (c) The secure computing environment is used to ensure the security of the running environment of ICSs. For an NPP being built, the replacement of ICS systems based on TC technology requires high cost, but other measures can be used to improve the security of the computing environment. For example, a strong authentication method can be adopted to identify users, mandatory access control or role-based access control (RBAC) optionally combined with Attribute Based Access Control (ABAC) mechanisms can be used to prevent unauthorized access.
- (d) The security management center provides unified identity authentication and authorization management for system administrators, auditors, and security personnel of ICS. At the same time, the security management center can also implement unified monitoring and comprehensive analysis of security devices and network devices in the area to detect attack events, issue early warnings and trace back when an attack event occurs.

4.3. Cyber security test platform for ICS in NPPs

ICS have stringent requirements for high availability and some ICS with real-time control functions, such as the protection system, will directly cause reactor shutdown events. Therefore, the cyber security technical defense architecture of critical ICS must be fully tested and verified. This means that a cyber security test platform for ICS is necessary. The traditional way to build a test platform is to use real equipment, which also means high investment cost and inflexibility of changes. The authors of this paper also put forward an idea of using DT (Digital Twinning) technology to build a platform to do a functionality and cybersecurity analysis[22]. DT is a technology to model assets with all their geometrical data, kinematic functionality and logical behavior using digital tools, not only to replicate, but to digitize physical objects in virtual space and simulate the behavior characteristics of physical objects in real environment. The three biggest advantages to use DT to construct a platform for testing and verifying the defense architecture consist in:

- (a) In the design phase of the ICS, DT can improve the accuracy of the design and verify the performance of the ICS in analogy to the security defense design in a real environment especially for many kinds of ATA (Attack Tree Analysis)
- (b) After the ICS is delivered to the business owner and while it is running, it is more convenient and less expensive to deploy various security measures on a DT-based test platform.
- (c) Because the DT-based test platform is highly consistent and synchronized with the real physical environment, the security measures proven effective and compatible on the platform can be deployed in the real production environment to ensure the business continuity of the ICS.

5. CONCLUSION

With the continuous development of intelligence and digitalization in NPPs, especially the integration of IT (Information Technology) and OT (Operational Technology), ICS will face more cyber security challenges. For newly built plants, they are recommended to take the cyber security factor into consideration from the planning and design phase according to the principle of “synchronous design, synchronous construction, synchronous operation”, and establish an active defense system based on TC technology and boundary protection technology to make the ICSs in NPP more secure. For plants being currently built, it is recommended to establish a semi-active defense system against the cyber security issues, which is based on the combination of boundary protection, network communication, computing environment control and centralized management. Meanwhile, this paper

proposes to explore an ICS test platform based on DT technology, which allows us to monitor the running state of ICS and to verify any security measures before it is deployed in the real environment.

However, this paper also notes that although TC technology has been applied in the power industry, there is no ICS based on TC technology in existing NPPs. It still requires enterprises in the supply chain to dedicate more researches. Besides, DT technology is still in its early stages and matured yet, and although its feasibility has been demonstrated, more efforts are needed to achieve mature applications.

ACKNOWLEDGEMENTS

We thank all the reviewers.

REFERENCES

- [1] KUSHNER, K., The Real Story of Stuxnet,
<https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- [2] TELESUR, Venezuela Denounces US Participation in Electric Sabotage (2019),
<https://www.telesurenglish.net/news/Venezuela-Denounces-US-Participation-in-Electric-Sabotage-20190308-0021.html>
- [3] FORBES, Could Venezuela's Power Outage Really Be A Cyber Attack,
<https://www.forbes.com/sites/kalevleertaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/>
- [4] OFFICE OF NUCLEAR REGULATORY RESEARCH, Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities, U.S. Nuclear Regulatory Commission, 2010.
- [5] IEC COMMITTEE 65, IEC 62443-1-1: Industrial Communication Network and System Security part 1-1: Terminology, Concepts and Models, IEC, 2009.
- [6] IEC COMMITTEE 65, IEC 62443-3-3: Industrial Communication Network and System Security Part3-3: System Security Requirements and Security Assurance Levels, IEC, 2014.
- [7] IEC COMMITTEE 65, IEC 62443-3-1: Industrial Communication Network and System Security Part3-1: Security Technologies for Industrial Automation and Control Systems, IEC, 2009.
- [8] IEC COMMITTEE 65, IEC 62443-4-2: Industrial Communication Network and System Security Part 4-2: Technical Security Requirements for IACS Components, IEC, 2019.
- [9] IEC COMMITTEE 65, IEC 62443-2-1: Industrial Communication Networks Network and System Security Part 2-1: Establishing an Industrial Automation and Control System Security Program, IEC, 2010
- [10] IEC COMMITTEE 45, IEC 62645 Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programs for Computer-based Systems, IEC, 2014.
- [11] IEC COMMITTEE 45, IEC, IEC 63096 Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Security Controls.
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, Nuclear Security Series No. 17, IAEA, Vienna (2011).
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, Nuclear Security Fundamentals, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015).
- [15] MICHELLE MICHAEL, Whitepaper Industrial Security based on IEC 62443,
https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf
- [16] HUANG, M., ZENG, QK., Research on classification attributes of software vulnerability, Computer Engineering (2010) 184–186.
- [17] FENG, T., LU, Y., Research on vulnerability and security technology of industrial Ethernet protocol, Journal on Communications (2017) 1–12.
- [18] Trusted Computing Group. TCG,
<http://www.trustedcomputinggroup.org/>
- [19] SHEN, CX., ZHANG, HG. et.al., Research and development on trusted computing technology, Science China: Information Science (2010) 139-166.

- [20] ZHANG T., Research on Theory and Key Technologies of Trusted Network in Electric Power Industry Control System. North China Electric Power University (2013).
- [21] SADEGHI, A.-R. et.al., “Security and privacy challenges in industrial internet of things”, DAC '15 Proceedings of the 52nd Annual Design Automation Conference, ACM New York, USA (2015).
- [22] LOU, X. et.al., “An idea of using Digital Twin to perform the functional safety and cybersecurity analysis” , Accepted by the 49th GI Annual Conference INFORMATIK 2019 (2019).
- [23] BAJRAMOVIC, E. et.al., “Security Challenges and Best Practices for IIoT”, Accepted by the 49th GI Annual Conference INFORMATIK 2019 (2019).
- [24] SAC/TC260, GB/T 22239-2019: Information Security Technology-Baseline for Classified Protection of Cybersecurity, Standardization Administration of The People's Republic Of China, 2019.