Turkish Journal of Computer and Mathematics Education Vol.14 No.3(2023),1193-1200
Research Article

MODERN-DAY ASSET SECURITY AND MANAGEMENT METHODOLOGY

Md Fahim Ahammed
MSc-Information Assurance and Cybersecurity, Gannon University, USA
ahammed001@gannon.edu

ABSTRACT
Asset security and risk management are crucial for overall economic growth, and a country's stability and populace safety depend on them running reliably and safely. For such a system, the assets' proper operation is crucial, and any threats that could adversely affect the assets could cause serious disruption. Risk management is a crucial component of the safeguarding important infrastructure There are numerous approaches and frameworks for locating assets, calculating vulnerabilities, and analyzing vulnerabilities. The interdependencies between the assets, however, and the cascade effects of the assets' innate weaknesses are not given enough attention. By introducing a fresh asset focus risk management method for the critical infrastructure, this research aims to close that gap. It offers a methodical approach for locating and analyzing vital assets, as well as any potential hazards or dangers to vital infrastructure. In our work, weconsider how cascading vulnerability impacts on assets can pose risks and threaten users. To illustrate the applicability of the method, we utilize a running example from a smart grid system. Our findings demonstrate that certain assets are prioritized and more susceptible than others for the power grid system, which can have a significant negative influence on overall business continuity.
Keywords - risk management, risk assessment, risk-generating factor, risk matrix, industry, critical infrastructure.

1. INTRODUCTION
Organizations that provide critical infrastructure (CI) are made up of vital resources including IT gear, software, facilities, networks, services, people, and complicated procedures that work together to support the entire operation of the business. Such systems face various security threats, including cyber-security threats, physical attack, etc., which could result in any potential risks, due to the inherent complexity of technology and its interaction with people andsystems consisting of multiple, distributed, and independently operating systems [1]. Since there is a chance of loss [2] or an uncertain event that might happen and affect the organization's fulfillment of strategic, operational, and financial goals [3], risks areconnected to every component of essential infrastructure. One of the most serious problems in the critical infrastructure organization, its networks, and related assets and vulnerabilities is the cybersecurity threat [4]. In order to establish effective protection to secure the assets, it is required to identify the assets and prioritize them basedon how they support the entire business. For this, a strong risk management strategy is required. In order to accomplish the success of the firm, there are already established risk management techniques and standards, such as ISO 31000:2018, which embodies the identification, analysis, planning, tracking, controlling, and communication of risk [5]. The identification and analysis of cascade consequences from susceptibility to threat and risks, however, is not given enough attention. An asset focus risk managementmethodology that identifies assets and their vulnerabilities and analyzes potential vulnerabilities by demonstrating their cascade effects on the assets and contributing to the threat and risks is the novel contribution of this article. We employ a methodical process to identify and rank the assets and vulnerabilities, and we adhere to notions such as asset, threat, and risk. Through the cascade effect of vulnerabilities to the asset and causes of risks, the assets and risks are analyzed. This undoubtedly aids the CI organization in reducing the risks and vulnerabilities by implementing appropriate controls in a proactive manner. To show how the work is applicable, we operate a power grid system as an example. The findings demonstrate that the suggested method successfully discovers asset vulnerabilities and analyzes risks through the cascading effects of vulnerabilities on assets.

Problem statement and its relationship to significant scientific and practical tasks. Today's industrial enterprises can only operate successfully if they efficiently manage their risks. Despite the fact that there has been a general accumulation of knowledge in risk assessment and risk management for specific types of economic activity (financial, investment), the risks inherent in industrial companies as complex industrial systems have not been thoroughly studied. Therefore, it is crucial to create a thorough system for industrial firms to manage their risks as production systems today.

The evaluation of recent research on the issue. The foundational writings of Smit, A. [1], Nayt, F. H. [2], and Balabanov, I. T. [3] take into consideration the key theoretical components of risk assessment and risk management. It is possible to locate Simon Marvell and Partner [4], K. Arrow [5], S. Ramadhani [6], I.T. Balabanov [3], and Bialas, A. [8] among modern international economists who are researching therisk problem in entrepreneurship. The works of Ukrainian economists I.U. Fekete, A. [9], P. Szor [10], Abouzakhar,

N.[11], Dalziell, E.P. [12] and others also addressed the definition of risk and the features of risk management techniques. However, it should be highlighted that the majority of studies use individualshort- or long-term risk projections. These hazards have different identification, forecasting, and management techniques, and contemporary risk management is rarely considered. Therefore, it is crucial for today's industrial firms to create and apply a methodology for risk assessment and risk management of production systems in the short and long term, with further coordination of the results.

Defining the research's goals. The purpose of the work is to provide an overview of methods for industrial enterprise risk assessment and management, supporting the need for a thorough investigation of industrial enterprise risks as production systems, which entails a separate evaluation of short-term and long-term risks with further harmonization of the obtained results.

Describing the key findings and the support for them. In the contextof current risk management, a risk related to a production system is understood as an occurrence of an event, an action, or a collection ofrelated events, an action, or a collection of related actions, related tothe operation and development of a production system, and the occurrence of which results in deviations from the developed strategy's implementation and from the financial performance of the production system as compared to what is predicted, expected, or scheduled. Negative deviations from the developed strategy's implementation can be seen as achieving poor financial outcomes over the long haul. The foregoing risks are implemented, and as a result, both in the short- and long-term, they have a negative financial impact. There are important distinctions between how industrial enterprises estimate their short-term and long-term risks, which are disregarded in both the theory and the practice of contemporary risk management [13]. The majority of research only use long-term or short-term risk assessments. Such a strategy violates the management process's guiding principle of continuity and may have grave unfavorable effects.

The following **(figure 1)** highlights the primary distinctions between the short-term and long-term risk assessment procedures.

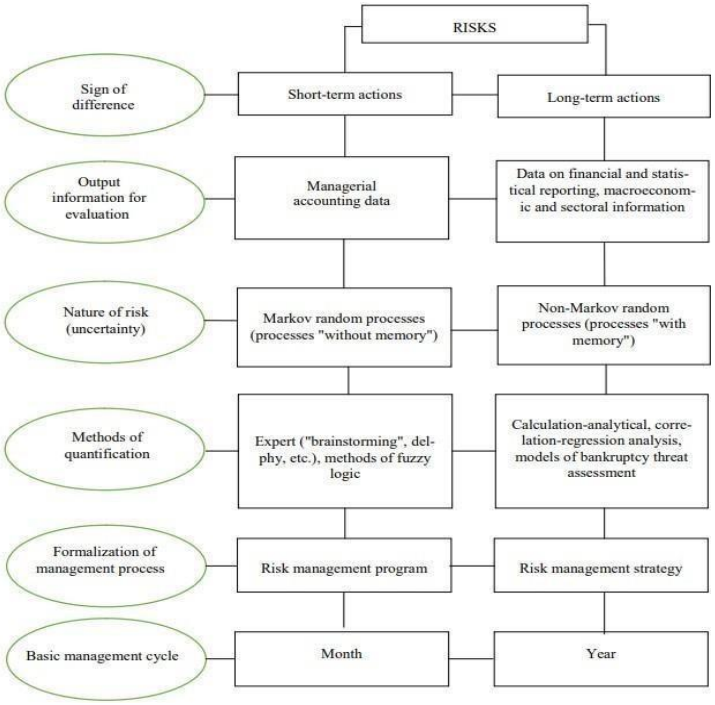

Fig. 1: Characteristics of short- and long-term risk assessment and management

2. RELATED WORK

Although not systematically addressed, there are studies in the literature that have been proposed on asset identification, potential vulnerabilities, threat outcomes, risk, and risk assessment. In order to overcome the difficulties of identifying important assets, S. Ramadhani [6] suggested a novel method based on multicriteria decision theory. Themethodology didn't offer a methodical procedure for making a criticality conclusion. On how to deal with the internal and external effects of a hazardous incident that happened in the specified critical infrastructure, Izuakor, C. and R. White. [7] offered a revolutionary structured risk management strategy. It adhered to the ISO31000 standard for communicating and monitoring risks. Interdependencies are also taken into account in this essay. There was no formula in the study for calculating risk magnitudes and control mitigations. Bialas, A. [8] explained how people determine what is important to them based on how much influence society has over them. demonstrates how to determine what is crucial in light of the fact that threats and cascade consequences cannot be fully protected. The repercussions of threats are discussed in the paper rather than threat prevention. The important characteristics of recognizing the above include strategic proactive planning, the goal of civil protection, and risk managementactions. Fekete, A. [9] Built the TVRA model for the telecommunication system by analyzing a telecommunication system using UML. This model also made a systematic examination of the security objectives, assets,weaknesses, unwanted incidents, and threats. P. Szor [10] suggested a multi-level graph strategy for decision making that gathers and analyzes sensor data from a city utilizing context dimension trees, ontologies, and baysian belief networks, the data gathering, context, and interface engines that make up the system architecture. However, knowledge exchange and sharing are crucial to enhancing its performance. Abouzakhar, N. [11] expanded the concept of a new attribute called "location" and put forth a thorough model for IP Multimedia Subsystem (IMS) network vulnerability research. They were able to in order to detect cases when security-relatedattributes are broken, automated verification approaches are used to further examine the behaviors. Hasan [13] provided a model that uses the Infrastructure Vulnerability Assessment Model to quantify vulnerability and applied it to a medium-sized clean water system.

Instead than identifying assets, this paper quantified system weaknesses. McQueen, M., et al. [14] evaluated the most recent research on the SCADA systems' cybersecurity risk. Numerous risk assessment techniquescreated or used in the context of a SCADA system were explored in the work. The objectives, application domains, risk management stages, concepts, impact measurement, sources of probabilistic data, evaluation, and tool support of these distinct methodologies were all examined. Based on the findings, a simple classification framework for SCADA system cybersecurity risk assessment techniques was proposed. A model for calculating how long it will take to compromise a system component that is visible to an attacker was put out by NERC, C. [15]. Based on known and obvious vulnerabilities, attacker skill level, and predicted value of the time-to-compromise, the model estimates these variables. The model was employed to quantify the risk reduction between a SCADA system and the reference system. A mechanism for achieving a quantitative risk reduction estimation was created in the work of Esser, M. [16], which involved risk reduction on a partial SCADA system. A graph theoretical technique with ten steps was used in the process. NERC, C. [15] covered the precise techniques used to calculate the time-to-compromise in step 6of the process. In order to provide a security framework for the identification and protection of critical cyber assets that support the reliable operation of the electric power grid, organizations like the North American Electric Reliability Corporation (NERC) establishedthe cybersecurity standards for critical infrastructure protection (CIP002 through CIP 009) Moteff, J. and P. Parfomak. [17]. The cyber-security framework was created by the National Institute of Standards and Technology (NIST) to improve the security and resilience of a country's critical infrastructure Yan, Y., et al. [18]. To enhance information security, develop risk management procedures, and promote adoption among organizations, NIST offers a framework for risk management. These studies all support the need for the significance of identifying critical infrastructure assets' vulnerabilities. However, we have noted a number of things. A systematic strategy that supports the organization of critical infrastructure by identifying key assets, their vulnerabilities, and the cascading effects of those weaknesses on the assets is particularly lacking. Additionally, the majority of the risk management process places greater emphasis on identifying critical assets before assessing vulnerability than it does on vulnerability assessment for critical infrastructure. A systematic asset identification and vulnerability assessment approach for critical infrastructure risk management that takes into account the cascade effect of vulnerability on the threat and risk is the novel contribution of our work.

SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS.

To safeguard organizational operations and assets, people, other organizations, and the country from a variety of threats and risks, such as hostile attacks, human error, natural disasters, structural failures, foreign intelligence entities, and privacy risks, this publication offers a catalog of security and privacy controls for information systems and organizations. The controls are flexible, adaptable, and part of an organization-wide risk management approach. The controls cover a wide range of needs that are a result of the purpose and business needs, as well as laws, executive orders, directives, rules, policies, standards, and guidelines. Finally, the unified control catalog covers security and privacy from an assurance viewpoint as well as from a functionality standpoint (i.e., the effectiveness of functions and processes supplied by the controls) (i.e., the measure of confidence in the security or privacy capability provided by the controls). To make sure that information technology products and the systems that rely on them are adequately reliable, functionality and assurance are addressed.

SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS.
This document offers a list of security and privacy controls for federal information systems and organizations as well as instructions on how to choose controls to safeguard the nation from a variety of threats such as hostile cyberattacks, natural disasters, structural failures, and human errors, as well as organizational operations (including mission, functions, image, and reputation), organizational assets, people, other organizations, and individuals (both intentional and unintentional). The information security and privacy risk management approach is adopted throughout the organization, and it includes customized security and privacy controls. The controls cover a broad range of security and privacy needs across the federal government and critical infrastructure, resulting from laws, executive orders, policies, directives, regulations, standards, and/or mission/business requirements. The guide also explains how to create customized sets of controls, or overlays, that are designed for certain missions or business functions, technologies, or operational situations. Finally, the list of security controls discusses security from the perspectives of assurance and functionality (the potency of the security functions and processes offered) (the measures of confidence in the implemented security capability). In order to ensure that information technology component products and the information systems developed from those products utilizing sound system and security engineering principles are adequately trustworthy, it is important to address both security functionality and assurance.

3. USING AN INSTANCE

The operating example power grid SCADA system that is used in our work is described in this part in general terms. Three key parts make up the system: a power plant, a transmission substation, and a distribution grid. The network of power lines and related machinery that is used to transfer and distribute electricity over a region is known as the power grid. Transportation, communication networks, water, power, and public institutions like schools, hospitals, post offices, and even jails are examples of these facilities Amin, S.M. [19]. Industrialcontrol systems (ICS), which enable digital control of the physical operations of equipment, are a part of the cyber-physical systems used in the electric industry. Whereas generation equipment, such turbines, was once purely mechanically operated, today's equipment is primarily protected and controlled by ICS synchronously, through automation, and occasionally remotely. The majority of power grids have become more susceptible to cyberspace incursions as a result ofthese technical advancements. An increasing number of Internet protocol (IP) capable access points have been added to the grid network as a result of initiatives to modernize older grid system components in order to incorporate new digital automation, or smartgrid technology AIRMIC, A. and A. Irm. [20]. As a result of the increased system connectivity, the integration of operational technology (OT) and information technology (IT) in ICS broadens the scope of the cyber threat environment. Networks can lose security over time because they are frequently modified to provide one-time access for a specificnecessity or convenience and are never properly restored. Equipmentthat can be accessed remotely is more open to public discovery on unsecured networks or the Internet. Cybersecurity, C.I. [21] contends that the generating, transmission, and distribution systems of the U.S. power grid each provide unique and similar risks to the steady flow of electricity through cyber-physical assets.

4. FRAMEWORK FOR RISK MANAGEMENT

The conceptual view of risk management areas and the supporting processes are included in the suggested framework. A description of the strategy is given in this section.

4.1 CONCEPTUAL VIEWPOINT

A set of modeling principles that are necessary to comprehend, control, and communicate cybersecurity risks are included in the suggested framework. For the creation of the framework for cybersecurity risk management that will take cascading impact into account, we have identified a few principles that are essential. On the basis of such ideas, a thorough examination of the many approaches,instruments, and strategies that can be used to a risk management framework in critical infrastructure organizations has been carried out. The following provides an overview of the ideas incorporated within the suggested framework:

Assets: Assets are the physical or intangible things that an organization needs and values. An essential step in risk management is the identification of key assets and the valuation of each critical asset.

Threat actor: A threat actor is a team, company, or person acting with ulterior motives. They can be identified by their location, capabilities, and resources used to launch a cyberattack against the company, as depicted in **figure 1**. For risk identification and mitigation, all accessible information on the threat actor must be made available.

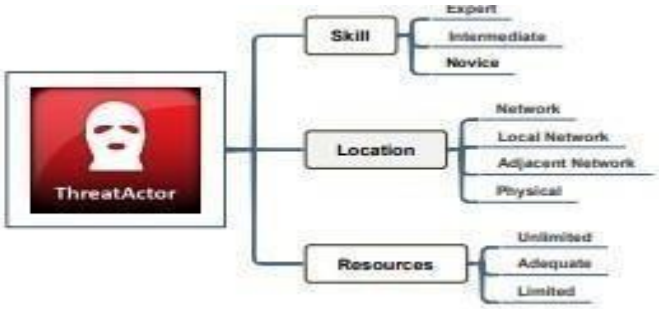

Fig 2. Threat actor description

Vulnerabilities and threat: A threat actor can weak spot an asset and exploit it as a vulnerability. The risk is the possibility of unauthorized access to an asset as a result of a threat actor exploiting a weakness in the asset.

Risks: Risk in the context of a critical infrastructure organization is the likelihood that an organization won't achieve its objectives, such as confidentiality, integrity, or availability, since there's a chance that a threat actor will get in the way.

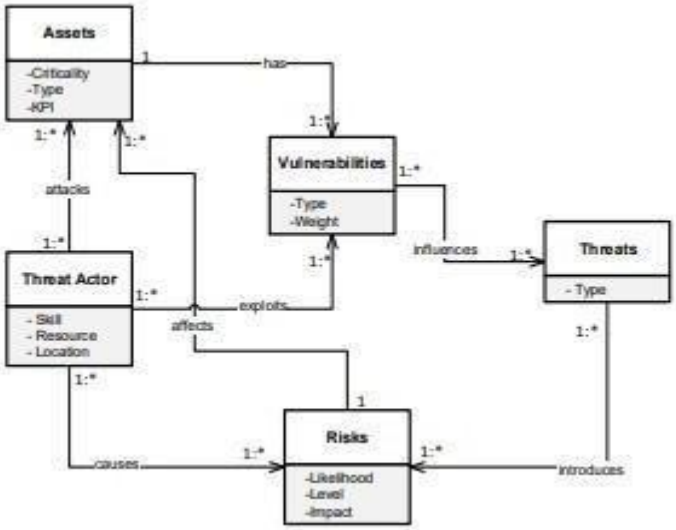

Fig 3. Metamodel

As shown in **figure 3**, the ideas are connected through actions that enable asset identification, vulnerability assessment, threat assessment, risk assessment, and cascade effect management. Assets are required for the operation of critical infrastructure companies and must be kept secure for the continuation of the business, yet theseassets are susceptible to vulnerabilities in their systems. Threat actors use these vulnerabilities to attack the asset, and if they are notfixed in a timely manner, they may affect a threat that creates risk, which is likely to result in the exploitation of the asset. Risk assessment is done to mitigate the risks once they have been recognized.

4.2 PROCESS

The procedure consists of a methodical group of actions that are connected to one another to support particular risk management tasks. To establish the procedure, we adhere to the principles outlined in the current risk management standards ISO 310000 [22], NIST SP800-30 framework [23], and NERC CIP standards [15]. Understanding the assets, vulnerabilities, and threats that might put critical infrastructure organizations at risk is of great importance.

4.2.1 IDENTIFICATION AND CLASSIFICATION OF ASSETS:

Asset identification is essential for effective risk management and must begin before any risks are discovered. Identification and prioritization of assets based on organizational criticality levels is the goal of asset identification. A vulnerability assessment is then performed using the obtained asset list and categorization as input. To defend against cyberattacks and the ensuing destruction, vital assets must be identified. Critical Infrastructure is made up of vital resources that are absolutely important for the organization's steady and reliable operation, and cyberattacks could have disastrous effects like power outages or water supply shortages. Examples of this Taylor, J.M. and H.R. Sharif [24] is a computer virus that infected up to 30,000 Windows-based systems connected to the network of a Saudi Arabianoil firm. The company's commercial operations were hampered as a result, and workstations and data were lost.

Stuxnet [24] was a nasty computer worm that affected and harmed the Iranian nuclear program by focusing on SCADA systems. The electrical grid was the target of a cyberattack that resulted in a complete blackout in Ukraine. Attackers who were successful in installing malicious software into the SCADA network field gateway devices compromised its information systems and momentarily cutoff the delivery of electricity to end users [25].

Through a methodical process and the use of the asset focus, this activity determines the most important CI assets. The importance of these resources to the organization determines their order of priority. Consequently, it is possible to comprehend what a crucial asset is and how to protect it from a cyber-attack. Since they have knowledge of the system and are able to identify asset types, asset impact types, and the necessary level of protection for each asset, including the sensitivity and value of a specific asset, it is essential toinvolve and engage the relevant stakeholders within the organizationfor this activity to be effective. Acquiring crucial assets is the last step in this action, and it is completed using the results of the other tasks.

Task 1A: Determine assets: The initial stage in any risk management procedure is asset identification. An essential step in risk management is identifying and valuing each major asset of a critical infrastructure company. As depicted in **figure 3,** these crucial resources may include data, software, hardware, SCADA systems, communications, and networks. It is vital to identify critical assets as well as assess their critical failure modes or loss impact because critical assets are defined as assets with a high consequence and high chance of failure. The following three steps are examined to identify important assets:

First Step: Asset Focus. Because the assets that make up our critical infrastructures are not all equally critical, asset focus refers to the specific assets to be taken into account for vulnerability and threat assessment as well as risk analysis. The software assets, programs, or applications that critical infrastructure businesses employ for their business operations should be taken into account while focusing on assets. If such assets are not effectively managed, they may expose the company to compliance concerns, reputational problems, and even threats to its very existence. Data assets are bits of information that a computer system stores and uses. The physical parts of a computer system, communication device, and networkcomprise hardware assets.

Second Step: Choosing objectives and key performance indicators (KPI) in: In terms of security and organizational context, this step defines the organizational goals for the critical infrastructure. The primary objectives are generally availability, integrity, and confidentiality. The key performance indicators for the organizational context are taken into consideration based on these aims. In order to support cybersecurity initiatives, it is also required to determine the critical operational duties of the critical infrastructure. A key performance indicator is crucial to risk management. These are the advantages and objectives that my organizations have set, and they must be accomplished. KPI is assigned a range of 1-0. Critical infrastructure that is secure should be able to deliver the following KPI:

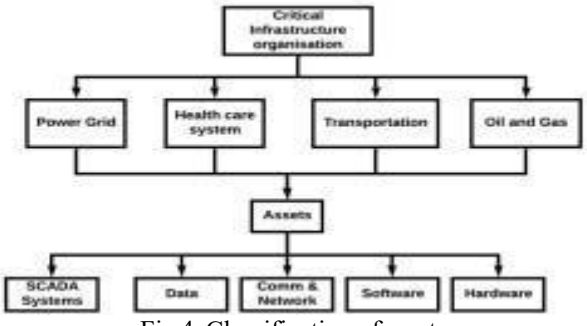

Fig 4. Classification of assets

Confidentiality: This KPI addresses the disclosure of private information to unauthorized users, internal users of key infrastructure, outside users, and malicious attackers. To avoid data leakage, it entails the deletion and transfer of data between authorized users in a safe setting. Installing encryption/decryption components at both ends of an insecure connection is one of the simplest ways to provide confidentiality [25].

Integrity: refers to the ability to guard against any unauthorized alterations or deletions.
Availability: The phrase "availability" refers to the guarantee that the systems in charge of providing, storing, and processing information are reachable by those who need them and when they need them.
Reliability (R): With the help of this KPI, the vital infrastructure may continue to operate reliably and efficiently despite any internal or external problems.
Authorization (ATH): With the aid of this KPI, an organization can define an actor's access privileges and rights to informational resources.

Authenticity (AUT): With the aim of enhancing security, usability, and administration, this KPI advances authorized user identification and verification technologies. It has the ability to link an authorized user to the precise information and service type that they need.
Privacy: With the help of this KPI, a company can keep confidential information about themselves and their users out of the hands of others. Both the protection of information and its proper use are involved.

Maintainability (M): Maintainability is related to the average amount of time required to fix a damaged asset and get it back in working order within a predetermined time frame. Less than a day, several days, a week, several weeks, a month, or even a year, could be considered the length of the period.
Conformance (CON): This KPI verifies that assets, including services, adhere to the required standards.
Accountability (ACC): This KPI guarantees that an actor's performance or behavior in relation to anything for which they are responsible will be assessed.

REFERENCES:

[1]. Smit, A. (2016). Ssledovanie o prirode i prichinah bogatstva narodov (1-3). M.: Eksmo
[2]. Nayt, F. H. (2003). Risk, neopredelennost i pribyil. M.: Delo.
[3]. Balabanov, I. T. (1996). Risk-menedzhment. M.: Finansyii statistika.
[4]. Simon Marvell and Partner, The Real And Present Threat Of A Cyber Breach Demands Real-Time Risk Management. 2015: p. 18
[5]. "Post-Genesis Digital Forensics Investigation," Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 164–166, 2017. S. Ramadhani, Y. M. Saragih, R. Rahim, and A. P. U. Siahaan.
[6]. Purdy, G., ISO 31000: 2009—setting a new standard for risk management. Risk analysis, 2010. 30(6): p. 881-886.
[7]. Izuakor, C. and R. White. Critical Infrastructure Asset Identification: Policy, Methodology and Gap Analysis. in Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14-16, 2016, Revised Selected Papers 10. 2016. Springer.
[8]. Bialas, A., Risk management in criticalinfrastructureFoundation for its sustainablework. Sustainability (Switzerland), 2016. 8(3): p. 240.
[9]. Fekete, A., Common criteria for the assessment of critical infrastructures. International Journal of Disaster Risk Science, 2011. 2(1): p. 15-24.
[10]. The Art of Computer Virus Research and Defense by P. Szor 2005, Addison-Wesley Professional
[11]. Abouzakhar, N. Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations. in European Conference on Information Warfare and Security. 2013. Academic Conferences International Limited..
[12]. Dalziell, E.P. and S.T. McManus, Resilience, vulnerability, and adaptive capacity: implications for system performance. 2004.
[13]. Hasan, M. R. (2022), Cybercrime Techniques in Online Banking. Int. J. of Aquatic Science, 13(1), 524-541. Retrieved from: https://www.journal-aquaticscience.com/article_158883.html (January 2022)
[14]. McQueen, M.A., et al., Time-to-compromise model for cyber risk reduction estimation, in Quality of Protection. 2006,Springer. p. 49-64
[15]. McQueen, M., et al., Quantitative Cyber Risk Reduction Estimation for a SCADA Control System. 2005, INL/EXT- 05-00319, Idaho National Laboratory, CSSC Report, prepared forUS Department of Homeland Security
[16]. NERC, C., Standards as Approved by the NERC Board of Trustees May 2006. [17]. Esser, M., A Framework for Protecting Our Critical Infrastructure. 2017

[18]. Moteff, J. and P. Parfomak. Critical infrastructure and key assets: definition and identification. 2004. DTIC Document

[19]. Yan, Y., et al., A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE communications surveys & tutorials, 2013. 15(1): p. 5- 20.

[20]. Amin, S.M., Smart grid: Overview, issues and opportunities. advances and challenges in sensing, modeling, simulation, optimization and control. European Journal of Control, 2011. 17(5-6): p. 547- 567.

[21]. AIRMIC, A. and A. Irm, structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. The Public Risk Management Association,London, UK, 2010.

[22]. Cybersecurity, C.I., Framework for Improving Critical Infrastructure Cybersecurity. 2014.

[23]. Baldoni, R., Critical infrastructure protection: threats, attacks, and counter-measures. 2014, Technical report.

[24]. Liang, G., et al., The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 2017. 32(4): p. 3317- 3318.

[25]. Taylor, J.M. and H.R. Sharif. Security challenges andmethods for protecting critical infrastructure cyberphysical systems. in Selected Topics in Mobile and Wireless Networking (MoWNeT), 2017 International Conference on. 2017. IEEE

[26]. Ani, U.P.D., H. He, and A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 2017. 1(1): p.32-74.