A Hybrid Security Approach to Nuclear Power Plants

Received: 24 January 2024; Accepted: 8 March 2023 *Research Article*

Ebutalha CAMADAN
National Defence University
Ankara, Türkiye
ecamadan@kho.msu.edu.tr
ORCID: 0000-0001-7669-5601

Beste DESTİCİOĞLU TAŞDEMİR
National Defence University
Ankara, Türkiye
bdesticioglu@kho.msu.edu.tr
ORCID: 0000-0001-8321-4554

Fikret BAYKALI
National Defence University
Ankara, Türkiye
fbaykali@kho.msu.edu.tr
ORCID: 0000-0001-7518-8851

***Abstract*— It has recently been observed that the energy crisis in the countries has become more severe as a result of the experienced global crises. Similarly, in response to the rising demand for energy, countries have started to use alternative energy sources. Nuclear power plants are regarded as one of the best alternatives for producing energy, in part due to their high energy output and low carbon emissions. However, there are significant adverse effects on both human and environmental health from a potential radioactive leak. Hence, in order to produce nuclear energy safely, the necessary safety precautions should be taken. Providing cyber security has grown in importance as a result of the advancement of technology, both in nuclear power plants and other areas. The 2010 STUXNET attack is an illustration of how challenging and crucial it is to implement the necessary security measures against cyberattacks in nuclear power plants. It has been determined from studies in the literature that there are studies that look at environmental, occupational health and safety, and cyber security concerns separately in nuclear power plants, but that there isn't a study that appears at these issues simultaneously and comprehensively. In order to follow the studies on environmental safety, occupational health and safety, and cyber security in nuclear power plants in an integrated manner, a hybrid safety and security unit approach has been proposed in this study. Additionally, this research will examine the precautions that should be taken in a nuclear power plant for environmental safety, occupational health and safety, and especially cyber security.**

Keywords—cyber security, occupational health safety, nuclear security, nuclear power plants

I. INTRODUCTION

Traditional fossil fuel use is still widespread throughout the world [1]. One of the most important energy-political issues in almost all countries is the lack of environmentally friendly and green energy sources. These concerns are a crucial component of interstate competition and can also be addressed within the context of energy security. Another issue with shifting to alternative energy sources is energy efficiency. Reducing carbon emissions is one of the green movement's global effects. In this context, nuclear energy is being used as an alternative energy source by both developed and developing countries. Reducing carbon emissions is one of the green movement's global effects. In this context, nuclear energy is being utilized as an alternative energy source by both developed and developing countries. In fact, studies carried out in these countries have discovered a strong correlation between the use of nuclear power and the intention to reduce carbon emissions [2]. Traditional fossil fuels now make up a larger portion of the energy supply, which has ensured the establishment of certain standards for both cost and safety precautions. On the other hand, it is challenging to compile accurate statistics on this topic because nuclear accidents and nuclear attacks are extremely rare occurrences. Nuclear safety is a complex issue, even though investments in nuclear energy have emerged as sustainable investments in terms of lowering carbon emission rates and environmental costs. In order to assess the problem in an integrated framework, a hybrid security model can be applied to the safety of nuclear power plants to test the long-term viability of investments and security. The top 10 countries account for 84.6% of the world's nuclear energy use [3] and use generated electricity by nuclear power plants. There are significant flaws in the global supply of nuclear energy in terms of energy diversity. Competition between nations with nuclear energy and countries seeking access to it is triggered by this circumstance. Europe is a crucial region for competition. After the conflict between Russia and Ukraine in February 2022, there were serious issues with Europe's energy supply [4]. It has been noted that after this war, efforts to diversify the energy supply, particularly in Europe, have increased [5]. Nuclear investments in the Middle East are another source of international tension, in addition to Europe. Particularly, Israel and the United States view Iran's nuclear energy projects as a danger. As an example of a cyberattack on critical infrastructures, the STUXNET attack has also been cited in the literature [6]. The study will discuss the requirements of a common security architecture after discussing the issues of cyber security, environmental and occupational safety in nuclear power plants.

II. CYBER SECURITY

A. Cyberattack Types and Their Effects

The integrity of our information systems and communication infrastructures has historically and now being endangered by a variety of cyberattacks. Human life may not be affected by the exposure of institutions and organizations working in different areas to these cyberattacks. When this issue is considered in the context of nuclear power plants, it is found that it will have a significant negative impact on both human life and international security. We discuss cyber dangers and possible defenses against nuclear power facilities throughout our study. Within this data, if we want to bring together the basic components as a result of our literature research;

- Malware: This malicious software can be used to steal, change, corrupt, or delete data in information systems or communication infrastructures [7]. Typically, it is transferred between systems using USB or external memory. Viruses and Trojans are the most harmful varieties of malware. The addition of viruses to applications or files allows them to replicate within the system, slowing it down and erasing data when activated by intended users. Trojans are frequently disseminated among systems by social engineering. It seeks to steal sensitive information while corrupting and destroying the systems it has infected.
- Ransomware: This kind of hack demands a ransom in exchange for decrypting the passwords and encrypting the data of the relevant systems [8].
- Social Engineering: Hackers aim to obtain confidential data by manipulating the emotions of company employees or target persons through emotional contact or persuasion [9].
- Phishing: Although it is an e-mail-based attack, it aims to capture the sensitive data of the target people with the links it publishes on e-mail attachments with the social engineering technique [10].
- DdoS: It prevents the relevant server or system from serving by subjecting a server or system serving on the network to data transmission over the capacity limits [11].
- Man-in-Middle Attack (MITM): It is a type of attack that allows obtaining or changing various data by listening to communications on the network [12].
- Password Attacks: It is the type of attack intended to enter the relevant system by guessing the passwords of users with full or limited authority on the system [13].
- Inside Threats: This type of threat refers to the data, system integrity or confidentiality of institutions or organizations; It includes the types of actions that can be done intentionally or unintentionally by the person authorized in the relevant system.

B. SCADA Systems in Nuclear Power Plants

These systems are used for data monitoring and control of industrial processes such as electricity networks, water networks, space stations and nuclear systems [14]. SCADA systems have used open access networks rather than closed access networks at some points to facilitate efficiency and business process monitoring. These types of networks have been exposed to a series of cyber-attacks over time. Intentional cyber-attacks by malicious personnel working in Nuclear Power Plants or unintentional cyber-attacks by an authorized personnel in the system working in these plants may cause a nuclear reactor to malfunction. In addition, this situation should not be considered as “inside threats” on the basis of personnel only. When we look at the world history, some cyber-attacks have been made on SCADA systems. These attacks are mentioned in the following articles.

- In 2010, SCADA systems of global oil, energy and petrochemical companies were targeted with a series of cyber attacks.
- In 2012, malware attacks were carried out on SCADA systems of Saudi Aramco, one of the largest energy systems [15].
- In 2013, a cyber-attack was carried out by Iranian hackers on a dam in New York [15].
- In the security report published by the German government in 2014, the SCADA systems of the German Steel Factory were the target of cyber-attacks [16].
- Due to the cyber-attack on electricity grids in Ukraine in 2015, approximately 250,000 people were left without electricity for a long time [17].
- According to FBI and Homeland Security reports, cyber-attacks were carried out on Nuclear Power Plants across the USA [14-18].

The most prominent cyber-attack against Nuclear Energy Stations worldwide and the most important cyber-attack against critical infrastructures has taken its place in the literature as STUXNET [6]. It was assumed that this attack damaged up to one-fifth of Iran's Nuclear Power Centrifuges. This attack can be considered as a cybersecurity wake-up call for SCADA systems.

STUXNET is a malicious computer worm created for the purpose of cyber-attack on Iranian nuclear facilities [19]. The main target of this worm is devices connected to centrifuges managed by PCLs via a USB stick connected to the SCADA system. STUXNET targets to listen to all nodes in the network by infecting Siemens SIMATIC Spen7 programs and tries to communicate with control servers by sending data in encrypted form [20]. As a result of communicating with the control servers, it disrupts the operation of the centrifuges.

C. Grouping of Cyber Attacks Against Nuclear Power Plants

The types of cyber threats mentioned in the Cyber Attack Types and Effects section of our study are based on two different points. These are internal and external sources. We think that threats from outside the institution are less likely to occur due to the fact that the SCADA systems used in the nuclear power station operate in closed networks and that the main factor is the unintentional intermediation of the personnel working in the institution. Moreover, it is difficult to state that personnel security and data security are separate structures. When we look at it from both perspectives, it will provide an important indicator in terms of reliability and testability that the unit inspecting these two units should look from a third perspective. Specifically, the variety of attacks on nuclear power plants in the face of a cyber incident can be examined under 5 different headings. The classification of cyber events and attack types that may occur in nuclear power plants is shown in Figure 1.

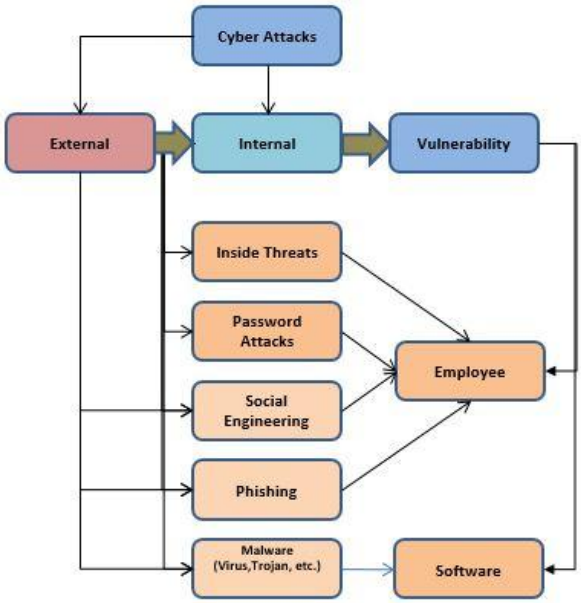

Fig. 1. Cyber Attack Types Reasons

III. Environmental and Occupational Safety in Nuclear Power Plants

The International Atomic Energy Agency emphasizes that nuclear energy obtained from nuclear reactors has an indispensable place among the energy sources used today [21]. On the other hand, nuclear energy production is still a controversial issue since the production of nuclear energy involves great risk [22]. There is a risk that a leak or an accident that may occur in nuclear power plants will affect large masses, primarily those working at the plant, including those living in the vicinity of the plant. An accident that may occur at a nuclear power plant can affect not only that country but also the surrounding countries . For example, the radiation emerged as a result of the Chernobyl Nuclear Power Plant accident that occurred in 1986 affected Ukraine, Belarus, Russia and Turkey as well [23].

When the accidents in nuclear power plants are examined, it is seen that most of them occur due to lack of safety precautions and human errors [24]. Therefore, in order to ensure both employee safety and environmental safety, it is necessary to take measures to prevent accidents in nuclear power plants. Proactive measures taken before an accident occurs are both more humane and cheaper [24]. Therefore, employers operating nuclear power plants should also take the necessary safety measures to prevent accidents. When it comes to measures to ensure environmental safety, the measures taken to prevent pollution of the air and water and the measures taken to prevent the destruction of the environment come to mind. However, an accident that may occur in nuclear power plants or any nuclear leakage that may occur in the power plant affects not only the personnel working at the power plant, but also the people living in the region where the nuclear power plant is located. Therefore, in addition to occupational health and safety measures in nuclear power plants, environmental safety measures should be taken to protect the personnel living in the region where the power plant is located. Some of the measures taken to ensure the occupational safety of employees in nuclear power plants are also effective in ensuring environmental safety.

IV. Security Unit Proposal of Nuclear Power Plants: Main Security Unit

The "Security Units" phases we recommend for the control and management of cyber-attacks against Nuclear Power Plants or physical and digital threats at the power plants are shown in Table I.

TABLE I. SCOPE OF UNITS

Phase	Units	Scope
1	Cyber Security	All digital devices at facility/ on network or not
2	Human Security	Ensuring the occupational health and safety of the employee and accident prevention
3	Environmental Security	Preventing the negative effects of nuclear materials on humans and the environment

A. Cyber Security Unit

This proposed security unit is responsible for the cyber security and policies of all digital devices in the Nuclear Power Plant, with or without access to the network at the power plant, operating in the power generation process at the plant. This unit performs the duties listed in the following items, respectively:

- Creating and managing the policy, strategy and training plans regarding the cyber security of the facility,
- To determine the cyber criticality level of the devices connected to the SCADA system in the facility and to follow up the authorization of the user personnel.
- To follow the records of the devices and storage units in the facility, to do the security tests and to follow the process,
- To provide training to the personnel working at the facility on the measures that can be taken against phishing and social engineering attacks,
- Creating password awareness by informing the personnel working at the facility about dictionary attacks and brute force attacks within the scope of password attacks,
- Within the scope of today's technology, viruses, Trojans, worms, etc. to follow the latest versions of malware types, to perform security tests on the devices on the independent closed network to be created of these versions, and to make a demo application by explaining the process to the personnel working in the facility,
- Identifying potential damage to occupational health and safety/environmental safety in case of a security weakness that may occur in the cyber security dimension and coordinating with these units.

B. Human Security Unit

Human Security Unit is responsible for protecting the health and safety of those working at the nuclear power plant. Therefore, employees should take the necessary precautions to work in a safe environment. In addition, it should determine the necessary preventive actions to prevent leaks or accidents that may occur.

In this section, firstly, the occupational health and safety measures to be taken by Human Security Unit in order to create a safe working place in nuclear power plants are discussed, then the issues that need to be taken into account in establishing environmental safety are specified and the measures that are effective in establishing both occupational health and safety and environmental safety are determined. The activities to be carried out by the Human Security Unit in terms of occupational health and safety are as follows.

In nuclear power plants, it is necessary to prevent the danger from the source. If the hazard cannot be avoided at its source, workers should be provided with appropriate personal protective equipment [25]. Protective armor should be made of suitable materials and of sufficient thickness between the source that emits radiation and the working environment. Materials such as concrete and soil can be used to make this armor. Preventing radiation from its source in this way is important in terms of ensuring the safety of both the employees at the power plant and those working in the region where the power plant is located. If the amount of radiation cannot be reduced sufficiently with this measure, appropriate personal protective equipment should be provided to the employees and employees should be provided to work using these personal protective equipment. In addition, employees should be informed about radiation exposure and limit values and the use of personal protective equipment [25]. Personal protective equipment to be used by employees should be available against any risk of radioactive leakage. In nuclear power plants, it is necessary to reduce the risk of radiation emission by installing the necessary ventilation systems in the irradiated areas.

Only personnel trained in these areas should be allowed to work in areas with radiation. In addition, there should be a sufficient number of expert personnel in the power plant. Employees should be given training on issues such as hazards in the workplace, occupational health and safety within the periods specified in the legislation. Periodic health examination of the personnel to be employed in the nuclear power plant should be carried out before and after the work starts, every year. In addition, exposure measurements should be made with dosimeters in order to determine the radiation exposure of employees [24].

A "Radiation Protection Program" should be established for each nuclear power plant in order to ensure the safety of employees in case of any leakage. This document should include information such as radiation exposure and limit values, protective measures, and personal protective equipment used.

C. Environmental Security Unit

Identifying potential damage to occupational health and safety/environmental safety in case of a security weakness that may occur in the cyber security dimension and coordinating with these units.

The Environmental Security Unit should carry out the necessary studies in order to prevent the damage that the nuclear power plant may cause to the environment. Since some of the measures taken on occupational health and safety are also effective in ensuring environmental safety, this unit should work together with the Human Security Unit. In this section, both the studies that should be carried out by the Environmental Security Unit and the studies that should be carried out jointly by the Environmental Security Unit and the Human Security Unit are included.

It should be ensured that the water used in nuclear power plants to reduce the temperature is given to the environment after the necessary treatments are made. This unit should carry out the necessary studies in this regard [20].

When nuclear power plants, nuclear waste storage facilities, nuclear fuel storage facilities, waste processing facilities do not take the necessary precautions, radioactive materials that will threaten the environment and human health pollute the environment. The main purpose of nuclear safety measures is to ensure that any radioactive leakage occurs inside the building (shelter/protection building), or to ensure that the radioactive release takes place under the allowable limits and in a controlled manner in case of an accident [27].

Therefore, in the event of a leak in nuclear power plants, necessary precautions should be taken to prevent the release of radioactive material to the environment. Starting from the establishment phase of nuclear power plants, risk analyzes should be carried out by taking into account the events and accidents that may occur, the causes and probabilities of these accidents. Necessary protective measures should be taken for activities with high risks. Risk analyzes should be updated considering the risks that may arise in any change in the materials used in the plant or in the production process [28]. In the prepared risk analysis, both risks related to environmental safety and occupational health and safety of the employee and the safety of the plant should be evaluated. The STUXNET attack that took place in Iran showed how important it is to ensure cyber security at nuclear power plants. Therefore, in the risk assessment, suggestions should be included in the evaluation of the risks for cyber attacks and the studies to be done to prevent these attacks. As a result, in the risk assessment of the nuclear power plant, risks related to cyber security should be included in addition to the risks related to the health and safety of the employee and environmental safety. In addition, an emergency plan should be prepared for nuclear power plants and an exercise should be carried out at least once a year [26].

D. Main Security Unit

This proposed security unit represents the main security unit responsible for cyber, human and environmental security sub-units. In scope, it plays a role in the main authority of security and policies for which sub-security units are

responsible. The main security unit fulfills the responsibilities described in the following items:

TABLE II. RESPONSIBILITIES OF MAIN SECURITY UNIT

Security Units	Responsibilities
Main Security Unit	-To create and implement the policy, strategy and training plans of the cyber, human and environmental security units -Following the resolution process of the relevant units in case of security breaches that may occur in the facility and ensuring its implementation -To identify current security problems worldwide and to take precautions by informing the relevant units -To monitor the network and communication infrastructure and to audit the Cyber Security unit by performing cyber vulnerability tests -To identify the threats that may occur within the scope of occupational health and safety and to audit the Human Security unit by making risk analysis. -Identifying threats within the scope of environmental conditions and security and auditing the Environmental security unit by making risk analysis - Identifying common openings for Cyber, Human and Environmental units and analyzing the behavior of these units as feedback.

TABLE III. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT CYBER+HUMAN SECURITY

Main Security Sub-Unit	Responsibilities
Cyber+ Human Security	-Detecting and controlling the common threats to cyber infrastructure and human health in case of possible cyber security attacks -Identifying situations that may threaten the health of the personnel working in the facility and ensuring the sustainability of the cyber infrastructure that may be affected in this context, with personnel redundancy.

TABLE IV. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT CYBER+ENVIRONMENTAL SECURITY

Main Security Sub-Unit	Responsibilities
Cyber+ Environmental Security	-Detecting and controlling the common threats to cyber infrastructure and environmental health in case of possible cyber security attacks -To determine the harmful situations that may occur for the environmental health of the facility and to ensure the continuity of the cyber infrastructure that may be affected as a result of this situation.

TABLE V. RESPONSIBILITIES OF MAIN SECURITY SUB-UNIT HUMAN+ENVIRONMENTAL SECURITY

Main Security Sub-Unit	Responsibilities
Human+ Environmental Security	-Reducing radiation emission by covering the surrounding of the reactor with an absorbing material -Reducing the amount of radioactive material released to the environment by establishing appropriate ventilation installations -In the risk assessment prepared for the nuclear power plant, the assessment of the risks related to the environmental effects of an accident or nuclear release

V. CONCLUSION

In this study, the "Main Security" unit was proposed within the scope of possible violations and attacks in response to cyber, human and environmental threats faced by nuclear facilities, and the type of joint solutions to overcome these situations with coordination between units was investigated. We consider that in case of possible cyber, human and environmental attacks, only cyber infrastructure and communication deterioration, human health deterioration and environmental health deterioration will not be possible. Therefore, it will be possible to overcome the threats that may occur in the facility and the attacks against the facility by ensuring that these recommended units work together. Cyber security, environmental security and occupational health and safety at nuclear power plants are carried out by different departments. However, in nuclear power plants, cyber security, occupational health and safety and environmental safety are in interaction with each other, and it is seen that risks are prevented by taking common precautions. In this study, common measures taken to ensure cyber security, occupational health and safety and environmental security were examined. For this reason, it is thought that effective security measures will be taken by establishing a common security unit that deals with cyber security, occupational health and safety and environmental safety in nuclear power plants, and thus nuclear power plants will operate more safely. In the final analysis, the intricate nature of the security of nuclear power plants necessitates the security architecture to be provided with control units that monitor and balance each other. The control unit, which constitutes the basic proposition of the study, also describes a theoretical approach produced against this problematic.

The necessity for the security of nuclear power plants to be in a multidimensional and complex architecture is a natural consequence of nuclear competition. On the other hand, the fact that physical/virtual attacks such as nuclear terrorism have not yet been experienced shows that new studies will be needed on this subject.

REFERENCES

[1] M. Naimoğlu, “The impact of nuclear energy use, energy prices and energy imports on CO2 emissions: Evidence from energy importer emerging economies which use nuclear energy,” Journal of Cleaner Production, vol. 373, p. 133937, 2022.

[2] A. Azam, M. Rafiq, M. Shafique & J. Yuan, “Towards achieving environmental sustainability: the role of nuclear energy, renewable

energy, and ICT in the top-five carbon emitting countries," Frontiers in Energy Research, vol. 9, pp.1-11, 2022.

[3] M. Sadiq, R. Shinwari, F. Wen, M. Usman, S.T. Hassan & F. Taghizadeh-Hesary, "Do globalization and nuclear energy intensify the environmental costs in top nuclear energy-consuming countries?" Progress in Nuclear Energy, vol. 156, p.104533, 2023.

[4] M. Umar, Y. Riaz, & I. Yousaf, "Impact of Russian-Ukraine war on clean energy, conventional energy, and metal markets: Evidence from event study approach," Resources Policy, vol. 79, p.102966, 2022.

[5] B. Steffen & A. Patt, "A historical turning point? Early evidence on how the Russia-Ukraine war changes public support for clean energy policies." Energy Research & Social Science, vol. 91, p.102758, 2022.

[6] S.R. Ameli, H. Hosseini, & F. Noori, "Militarization of Cyberspace, Changing Aspects of War in the 21st Century: The Case of Stuxnet" Against Iran," Iranian Review of Foreign Affairs, vol. 10(29), pp.99-136, 2019.

[7] Alanazi, M., Mahmood, A., & Chowdhury, M. J. M. (2022). SCADA vulnerabilities and attacks: A review of the state - of - the - art and open issues. Computers & Security, 125, 103028.

[8] Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express, 4(1), 14–18.

[9] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[10] Nazir, S., Patel, S., & Patel, D. R. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, 70, 436–454.

[11] Polat, H., Turkoglu, M., Polat, O., & Sengur, A. (2022). A novel approach for accurate detection of the DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. Expert Systems With Applications, 197, 116748.

[12] Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. International Journal of Critical Infrastructure Protection, 25, 14–35.

[13] Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666.

[14] S. Ghosh, & S. Sampalli, "A Survey of Security in SCADA Networks: Current Issues and Future Challenges," IEEE Access, vol. 7, pp.135812–135831, 2019.

[15] Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. In Survival (Vol. 55, Issue 2, pp. 81–96). Taylor & Francis.

[16] Lee, R. M., Assante, M. J., & Conway, T. (2014). German steel mill cyber attack. Industrial Control Systems, 30(62), 1-15.

[17] Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29

[18] Department of Homeland Security and The Federal Bureau of Investigation, Russian government cyber activity targeting energy and other critical infrastructure sectors, Tech. Rep. TA18-074A, Mar. 2018, pp. 1–18.

[19] Homay, A., Chrysoulas, C., Boudani, B. E., Da Cunha Sargedas De Sousa, M. J., & Wollschlaeger, M. (2020). A security and authentication layer for SCADA/DCS applications. Microprocessors and Microsystems, 103479.

[20] Z. Masood, R. Samar, & M.A.Z. Raja, "Design of a mathematical model for the Stuxnet virus in a network of critical control infrastructure," Computers &Amp; Security, vol.87, p.101565, 2019.

[21] World Nuclear Association, https://world-nuclear.org/ (10.01.2023)

[22] S. Gandhi & J. Kang, "Nuclear Safety and Nuclear Security Synergy," Annals of Nuclear Energy, vol.60, pp.357-361, 2013.

[23] W. Hallenbeck, Radiation Protection. Reported thus far are 237 cases of acute radiation sickness and 31 deaths. CRC Press. s. 15. 1994.

[24] Kahraman, Z. & Yürüten Özdemir, K. "Nükleer Enerjinin Riskleri ve Nükleer Santrallerde İş Sağlığı ve Güvenliği," Karaelmas Journal of Occupational Health and Safety, vol. 6(1), pp.53-65, 2022.

[25] B. Desticioğlu & B. Özyörük, "Türkiye'de Sektörel Bazda Gelecek Yıllar için İş Kazası Sayısı Tahmini," in Bilimsel Araştırmalar Kitabı 2022: İktisadi ve İdari Bilimler, Ed. A. Yalçın, Ankara: Akademisyen Yayınevi, 2018, pp.143-156.

[26] Resmi Gazete, "6331 Sayılı İş Sağlığı ve Güvenliği Kanunu," https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6331.pdf (10.01.2023).

[27] Türkiye Enerji Nükleer ve Maden Araştırma Kurumu TENMAK, https://www.tenmak.gov.tr/2016-06-09-00-43-55/135-gunumuzde-nukleer-enerji-rapor/835-bolum-05-nukleer-guvenlik.html (10.01.2023).

[28] H. George-Williams, M. Lee and E. Patelli, "Probabilistic Risk Assessment of Station Blackouts in Nuclear Power Plants," in IEEE Transactions on Reliability, vol. 67, no. 2, pp. 494-512, June 2018.