11th International Conference on Electrical, Electronics and Computer Engineering (IcETRAN), Nis, 3-6 June 2024

Possibility of Insider Threat to Nuclear Power Plants

Milica Ćurčić
Department of Phisical Chemistry
Vinca Institute of Nuclear Science – National Institute for the Republic of Serbia
Belgrade, Serbia
email: milica.curcic@vin.bg.ac.rs
ORCID: 0000-0002-4326-4036

Marija Janković
Department of Radiation and Environmental Protection
Vinca Institute of Nuclear Science – National Institute for the Republic of Serbia
Belgrade, Serbia
email: marijam@vin.bg.ac.rs
ORCID: 0000-0002-2255-7163

Slavko Dimović
Deprtment of Radiation and Environmental Protection
Vinca Institute of Nuclear Science – National Institute for the Republic of Serbia
Belgrade, Serbia
email: sdimovic@vin.bg.ac.
ORCID: 0000-0003-2666-5417

***Abstract*—Nuclear power plants represent critical infrastructure assets essential for global energy production, embodying both immense potential for state and significant risks. This paper examines the possibility of insider threats within nuclear power plants, clarifying the complex interplay among human factors, security measures, and technical vulnerabilities. By synthesizing existing literature, this study explains the multifaceted nature of insider threats, encompassing malicious actions by employees, contractors, or other trusted entities operating within the facility.**

The analysis delves into various dimensions of insider threats, primarily focusing on the motivation, capabilities, and intentions of insiders to attempt unauthorized removal or sabotage of nuclear or other radioactive material. This study also examines the main attributes of insider threats, i.e., access, authority, and knowledge. Drawing upon insights from security and radiation protection disciplines, this paper explores the behavioral and organizational factors that contribute to insider risk, emphasizing the importance of understanding human dynamics in safeguarding nuclear facilities.

Furthermore, this study assesses the efficacy of existing security measures in mitigating insider threats and identifies areas for improvement. In this paper, we examine strategies ranging from access controls and background checks to personnel screening and psychological profiling, evaluating their strengths, limitations, and ethical considerations. This also includes analyses of pathways through which insiders may exploit vulnerabilities to compromise plant security.

Through a comprehensive examination of insider threat scenarios and countermeasures, this paper underscores the imperative for a multidisciplinary approach to nuclear plant security, integrating technical, procedural, and human-centered elements. It advocates for enhanced training and awareness programs to cultivate a culture of vigilance among plant personnel and stakeholders, emphasizing the shared responsibility of safeguarding nuclear facilities against insider threats. Central to this approach is the promotion of a robust nuclear security culture, fostering a mindset of continuous improvement and adherence to best practices in security protocols and risk mitigation strategies.

Keywords—nuclear security, insider threats, nuclear power plants, nuclear security culture

I. INTRODUCTION

Nuclear power plants represent critical infrastructure assets, supplying significant portions of the world's electricity needs. However, their strategic importance also renders them prime targets for potential attacks. The critical role they play in the energy system, connected with the catastrophic consequences of a successful breach, underscores the urgency of ensuring their safety and security. Recent geopolitical events, such as the conflict in Ukraine, have heightened awareness of the vulnerabilities faced by nuclear facilities, prompting renewed focus on enhancing their protection measures. Therefore, great attention is paid to identifying and analyzing potential security threats to nuclear power plants. Nuclear security threats encompass individuals or groups driven by motivation, intent, and capability to engage in criminal or unauthorized activities involving nuclear or radioactive materials, facilities, or related actions, as deemed detrimental to nuclear security by the state [1].

Due to this, there is a dedicated focus on analyzing potential perpetrators of attacks on nuclear power plants. The IAEA defines potential attackers as "adversaries," referring to individuals engaged in or attempting to execute malicious acts. These adversaries may be either insiders or outsiders. Insiders pose a significant security risk to any critical infrastructure. While various definitions of insiders exist, Bulling et al. provide a comprehensive definition: “an insider refers to an individual within an organization or with access to critical components of the organization. This could include employees, contractors, consultants, or anyone with a trusted relationship or position within the organization. Insiders may act alone or in collusion with others” [2].

The unique nature of the insider threat in nuclear power plants is evident in several aspects. Firstly, it involves the specific knowledge required by employees in nuclear power plants, encompassing specific safety and security measures. Additionally, it involves the type of threat insiders may attempt and the potential severity of consequences that could result.

Insiders may also work with external accomplices, ranging from state-sponsored actors and terrorist organizations to organized crime groups and cybercriminals. This collaboration introduces an additional layer of complexity to the security landscape. In this way, with their combined capacities, these

actors constantly probe for vulnerabilities in an attempt to exploit weaknesses in security protocols and infrastructure.

Understanding these nuances is crucial for mitigating insider threats effectively. By recognizing the inherent vulnerabilities and evolving threat environment, stakeholders can develop proactive measures to safeguard against potential attacks and enhance the resilience of nuclear facilities in an increasingly volatile world.

II. Adversaries as a Security Threat to Nuclear Facilities

In discussions regarding nuclear power plant security, the primary concern is based on the potential for accidents. This apprehension is grounded in the spectrum of possible outcomes, whether they be technical accidents like Chernobyl or natural disasters leading to such accidents, such as Fukushima. Additionally, ongoing warfare in Ukraine introduces a new understanding that a severe nuclear plant accident may occur amidst conflict. Nonetheless, the high level of technical sophistication in nuclear facilities, coupled with continual enhancements in security and safety protocols, indicates a minimal likelihood of such occurrences. Hence, significant emphasis is placed on human factors as potential catalysts for security issues. Indeed, as technical protection measures become more sophisticated, potential attackers targeting critical infrastructures are turning their focus towards exploiting human vulnerabilities. Consequently, the human factor continues to remain a prominent concern on the threat agenda in all security analyses.

In the present day, addressing the diverse risks associated with nuclear security involves a significant emphasis on the human aspect. This includes devising security protocols specifically aimed at preventing unauthorized removal or sabotage by employees targeting an organization's operations. Human factors play a pivotal role in both the design and execution of security measures. While technical measures are essential, they alone cannot ensure the system's efficacy, necessitating the integration of the human element into the equation. Individual involvement is crucial for the effective implementation of security measures. More specifically, the evolution of people's attitudes and perceptions regarding nuclear security over time can significantly impact their responses to security-related tasks and activities.

Hence, significant attention is paid on identifying and analyzing potential perpetrators of attacks on nuclear power plants. The IAEA defines potential attackers as “adversary” to denote any individual engaged in or attempting to carry out a malicious act. This adversary could be either an insider or an outsider. The term ‘insider’ is used to describe “an individual with authorized access to (nuclear material) associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security” [3]. The discrepancy in attention towards the issue of insiders becomes evident when comparing the depth of the 2020 definition with that of 2008. The previous defines a threat as “an adversary with authorized access to a nuclear facility, a transport operation or sensitive information” [4], while the newest offers a far more comprehensive understanding. In both Guides, the term ‘outsider’ is used to describe an adversary other than an insider [3,4]. In simpler terms, insiders include both employed personnel within nuclear power plants and contractors. Conversely, external threats comprise various malicious actors such as terrorists, organized criminal groups, and cyber attackers, extending to threats from other state-sponsored groups. Special consideration should be given to former employees who have been dismissed but retain knowledge about the nuclear power plant activities and processes, connections with current staff, and harbor negative sentiments towards the facility, despite lacking access.

In this paper, we focus exclusively on insiders as a security threat, with the conclusion that external threats also represent a significant security threat to nuclear power plants. The seriousness of the security threat posed by insiders is underscored by the fact that the International atomic energy agency (IAEA) offers explicit recommendations on how countries where the nuclear power plant is located should respond and delineates their obligations in this regard. The initial step in assessing insiders as a security threat to nuclear power plants begins with a comprehensive national nuclear security threat assessment conducted by the state and its competent authorities. This assessment evaluates the range of existing threats related to nuclear security; encompassing both physical and cyber security risks, discerning the attributes and characteristics of potential adversaries [5]. The outcome of a national threat assessment is a document delineating the comprehensive threat environment and detailing all identified credible threats.

State authorities should define threats and associated capabilities through credible information sources, formulating a design basis threat (DBT). The DBT stems from the state's evaluation of unauthorized removal and sabotage threats, and it describes the “attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated” [5]. Another option available to the state is to formulate representative threat statements (RTS) that include the attributes and characteristics of potential insider and/or external adversaries, aimed at unauthorized removal or sabotage, intended to be used to develop prescriptive requirements for the protection of defined materials and/or facilities [5].

Also, the state must distinctly delineate and delegate nuclear security responsibilities to competent authorities, which may encompass regulatory bodies, law enforcement agencies, customs and border control, intelligence and security agencies, health organizations, and others [6]. Broadly speaking, all these bodies are responsible for combating nuclear threats, including those arising from insiders within nuclear power plants.

The state and the regulatory body establish the legislative and regulatory framework, which imposes various obligations on operators. Among these, a critical responsibility is for operators to design, implement, and uphold security systems for radioactive material in accordance with regulatory mandates [6]. Therefore, the operator is obliged to implement all prescribed measures and provide assurances that demonstrate quality and effectiveness of its security program. In this case, nuclear power plant has the responsibility to advance all

measures and activities aimed at preventing the actions of insiders. To effectively organize protection against insiders, responsible personnel at nuclear power plants must begin by understanding their characteristics. This understanding forms the cornerstone for implementing robust security measures.

III. CHARACTERISTICS OF INSIDER THREAT

While technical security measures and physical protection systems are devised to counter all potential adversaries, insiders present a distinct security challenge due to certain inherent characteristics. The opportunity for insiders to engage in illicit activities stems from their specific attributes. The IAEA specifies that insiders possess at least one of the following attributes, granting them advantages over external adversaries when carrying out malicious activities: access, authority and knowledge.

Access: insiders possess authorized access to the areas, equipment, and information required to fulfill their responsibilities. This encompasses physical entry to nuclear facilities, nuclear materials, associated systems, components, and equipment, as well as computer systems. Moreover, access also covers remote computer systems overseeing processes, safety assurance, sensitive data storage, or bolstering nuclear security. However, operators must avoid allowing remote access to critical systems, especially those crucial for safety [3].

The attribute of access among insiders manifests in various forms, each posing unique challenges to security measures. For instance, authorized access to work areas provides insiders with opportunities to exploit vulnerabilities, such as accessing containment areas during crane operations, which may lead to unauthorized access to restricted targets. Moreover, special temporary access arrangements or emergency access for fire, medical, or police purposes can also be exploited by insiders to gain unauthorized entry to sensitive areas or systems. This includes both escorted and unescorted access scenarios, where individuals may abuse their privileges for malicious intent.

Furthermore, when we talk about the access to targets, the duration and circumstances of access during normal operations or special circumstances play a crucial role in determining the risk posed by insiders. Whether through network or remote access, insiders can exploit their privileges to infiltrate critical systems, such as design information, accounting systems, physical protection systems (PPS), or nuclear material accounting and control (NMAC) systems. Additionally, insiders with access to safety systems, process systems, tools, or knowledge of standard and emergency exfiltration routes pose significant threats to nuclear security. By leveraging their access, insiders can sabotage safety protocols, manipulate processes, or facilitate the unauthorized removal of sensitive materials or information.

Authority: Insiders possess the authorization to carry out operations within the scope of their assigned responsibilities and may also hold the power to oversee other employees. This authority may be used to support malicious acts, including either physical or computer based acts such as digital file or process manipulation [3].

Authority can manifest in various forms among insiders, each presenting distinct challenges to security protocols: authority over oneself encompasses instances where insiders may exempt themselves from established procedures or choose not to adhere to prescribed protocols, exploiting their autonomy for unauthorized actions. In terms of authority over people, formal authority denotes designated oversight over others, while semi-formal authority involves organizational cultural norms that restrict individual behavior. Informal authority relies on personal influence, which insiders may exploit to manipulate colleagues or subordinates. Temporary authority arises from temporary work authorizations or when insiders fill in for supervisors, providing opportunities for unauthorized access or actions during these periods of elevated responsibility. Authority over tasks and equipment grants insiders the ability to assess alarms, prepare sensitive forms, or authorize processes and procedures, which can be exploited to compromise security measures or manipulate systems. Falsified authority poses a significant risk when insiders fabricate credentials or accesses, enabling them to bypass security measures and carry out malicious activities under false pretenses.

Knowledge: Insiders may possess varying degrees of familiarity with the facility, its activities, and systems, ranging from basic to expert levels. This may include knowledge that could enable an insider to bypass or defeat dedicated physical protection systems and other facility systems that contribute to nuclear security, such as safety and nuclear material accounting and control (NMAC) systems, operating procedures and response capabilities [3].

Insiders may possess detailed information regarding the locations, characteristics, and specific details of potential targets within the facility. Additionally, they may have insights into the optimal times to access these targets, allowing them to exploit vulnerabilities more effectively. Also, insiders may be familiar with intricate details of the facility layout, including access points and restricted areas. They may also have knowledge of available tools and equipment that could be utilized for illicit or malicious activities. Moreover, insiders may possess expertise in concealing their actions and avoiding detection within the facility environment. Furthermore, insiders may have comprehensive knowledge of various security systems deployed within the facility, including equipment, processes, procedures, and operations. They may also be aware of vulnerabilities in physical protection systems (PPS), nuclear material accounting and control (NMAC) systems, safety and radiation protection measures, as well as information and cyber systems, enabling them to exploit weaknesses for malicious purposes.

In light of these examples, it becomes evident that the attribute of insiders presents considerable challenges to nuclear security. With authorized access to critical areas and systems, coupled with varying levels of authority over tasks and personnel, insiders possess the means to exploit vulnerabilities for malicious ends. Furthermore, their knowledge of facility layouts, security systems, and operational procedures affords them the capability to circumvent safeguards and evade detection. It is important to point out that an insider might not possess all three attributes but might still have sufficient capability to conduct a malicious act.

In order to increase the likelihood of success, insider adversaries may prolong their nefarious activities over an extended period. This strategy might involve: (a) tampering with physical protection equipment or safety equipment to prepare for an act of sabotage, (b) falsifying records so that the

insider adversary is able to repeatedly remove without authorization small amounts of lower category nuclear material that has less robust protection than higher category nuclear material without being detected or (c) removing nuclear material without authorization in amounts below measurement system detection thresholds [3]. Insiders could exploit normal or abnormal facility conditions, such as during maintenance or material movement, selecting opportune moments to carry out their malicious deeds. Therefore, addressing the nexus of access, authority, and knowledge is imperative for implementing robust security measures to safeguard against insider threats in nuclear facilities.

Indeed, beyond access, authority, and knowledge which afford insiders opportunities, analyzing another critical factor—insider motivation—is essential when considering potential attacks. Insiders may harbor diverse motivations for instigating malicious acts, spanning from financial gain and ideological, political convictions to seeking revenge, personal recognition, or greed to religion. Some people might even be blackmailed into assisting to external adversary. These motivations can operate independently or in combination, potentially exacerbated by mental health issues or external recruitment by adversaries aiming to exploit their access, authority, or knowledge [7].

Furthermore, insiders can occupy any position within an organization, regardless of hierarchy, and individuals at all levels may find sufficient incentive to engage in malicious behavior. Moreover, it's crucial to recognize that personnel not directly employed by the operator, such as vendors, first responders, contractors, or regulatory inspectors with periodic authorized access to the facility, also pose potential insider threats and should be considered accordingly.

In essence, the motivations driving insider threats are multifaceted and interconnected, reflecting a range of personal, psychological, and external influences. Understanding these motivations is critical for implementing effective security measures to mitigate the risks posed by insider threats across all levels of an organization and among individuals with authorized access to sensitive facilities.

Different types of insiders can be identified based on their characteristics, motivations, and intentions. By understanding what drives them and what they aim to achieve, security measures can be tailored to address specific vulnerabilities and mitigate risks. This approach enables the differentiation of various types of insiders, facilitating a more targeted and proactive response to potential threats. One such categorization provided by the IAEA guide (Fig. 1.) divides insiders according to their awareness of participating in an attack and their characteristics [3].

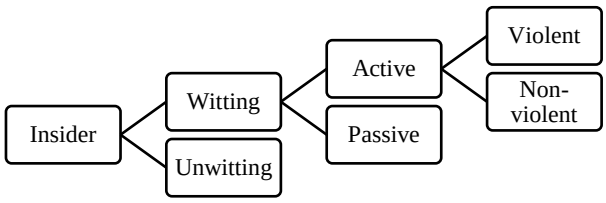

Fig. 1. Different types of insider

An unwitting insider is characterized by a lack of intent and motivation to commit a malicious act. They are typically exploited by adversaries without their awareness. For example, in a computer-based attack, an unwitting insider may unknowingly click on a malicious link in an email, falsely believing it to be from a trusted source. This action inadvertently provides information or authenticated access to an adversary, without the insider's understanding of the consequences.

An insider adversary is an individual within an organization who engages in malicious activities with full awareness, intent, and motivation. Insider adversaries can be further categorized as either passive or active, with active insider adversaries being subdivided into violent or non-violent categories. This classification is invaluable for assessment purposes, such as developing adversary profiles in threat assessments or design basis threat (DBT), as well as creating scenarios to test nuclear security measures as part of the evaluation process for the nuclear security system.

Indeed, a passive insider adversary may assist another adversary by providing information to be used in performing a malicious act. However, unlike an active insider, a passive insider adversary refrains from direct participation in the malicious act itself. Their involvement is limited to sharing information or intelligence that aids the perpetrator. Additionally, a passive insider adversary is more likely to disengage from the activity if there's a high probability of being identified or if the risks become too great. This distinction underscores the varying degrees of involvement and risk tolerance among insider adversaries.

An active, non-violent insider adversary employs stealth or deceit to facilitate or directly carry out a malicious act. This type of insider may engage in activities such as attempting theft of nuclear material through abrupt or protracted means. Additionally, they may assist external adversaries by disabling alarms, ignoring security protocols, or opening doors to unauthorized areas within the facility. However, it's important to note that while they may risk detection, they are less likely to risk being positively identified. This distinction highlights their preference for avoiding direct attribution of their actions, prioritizing evasion over confrontation. Moreover, an active, non-violent insider adversary is likely to terminate the malicious act if there's a high likelihood of being positively identified, indicating a level of self-preservation and caution in their approach.

An active, violent insider adversary shares similarities with an active, non-violent counterpart but distinguishes themselves by their willingness to employ physical force against personnel to achieve their malicious objectives. Like their non-violent counterpart, they may engage in actions such as theft of nuclear material or facilitating malicious acts through deceit or subterfuge. However, the use of physical force sets them apart, indicating a greater propensity for aggression and direct confrontation in pursuit of their goals. Furthermore, depending on the circumstances, an insider adversary may transition from a non-violent to a violent approach, adapting their tactics as needed to overcome obstacles or achieve their aims [3]. This means that all types of insiders must be given significant attention in the analysis.

IV. Nuclear Security Culture

Addressing insider threats in nuclear power plants presents a multifaceted challenge due to various factors. Firstly, the unique nature of each facility demands a tailored approach to assessing and mitigating insider risks. What works for one power plant may not be effective for another due to differences in infrastructure, personnel, and operational protocols. Moreover, mitigating insider actions requires a comprehensive strategy blending both technical and nontechnical methods. Implementing such a program systematically is crucial to ensuring its efficacy across all levels of the plant's operations. This entails not only adopting proven practices but also customizing them to suit the specific needs and vulnerabilities of the facility. Ultimately, achieving robust detection and deterrence of insider acts necessitates rigorous testing and adaptation. By continually refining strategies based on real-world insights, nuclear power plants can enhance their resilience against insider threats, safeguarding both their operations and the surrounding communities from potential harm.

While challenging, addressing insider threats is indeed achievable. One effective strategy involves cultivating and enhancing a robust nuclear security culture. Nuclear security culture represent the assembly of characteristics, attitudes and behaviors of individuals, organizations and institutions which serve as a means to support, enhance, and sustain nuclear security [8]. In other words, nuclear security culture refers to the beliefs, understandings and practices that the people engaged in a nuclear organization bring to its security. If they believe that it is every individual’s responsibility to contribute to the security of all organization, and take security responsibilities seriously as a part of their daily practices, they are part of an organization in which a security culture has taken the root [7]. Improving the nuclear security culture within a facility is indeed a crucial aspect of addressing insider threats. A strong security culture fosters a mindset where all personnel are vigilant, aware, and committed to upholding security protocols and reporting any suspicious activities. All organizations involved in implementing physical protection should give due priority to the security culture, to its development and maintenance necessary to ensure its effective implementation in the entire organization [8].

Active involvement from the Executive and Board levels is crucial for establishing and maintaining effective and enduring nuclear security culture programs. Organizations should contemplate appointing a dedicated executive position focused on security and integrating security objectives into corporate milestones. Effectively communicating and conveying the importance of security initiatives at these levels is best accomplished by framing them within the context of business needs and overarching risk management strategies [9].

By cultivating a culture that values security, nuclear power plants can enhance awareness among employees regarding the potential risks posed by insiders. This includes promoting a sense of responsibility among staff members to actively participate in security measures and report any concerning behaviors or incidents promptly. Moreover, a robust security culture facilitates the implementation of effective training programs to educate personnel about insider threat detection and mitigation strategies. It also encourages open communication channels, enabling employees to voice their concerns without fear of reprisal. Ultimately, investing in improving the nuclear security culture can significantly contribute in strengthening defenses against insider threats, complementing other technical and procedural measures within the facility's security framework.

The absence of a robust security culture significantly contributes to the emergence of unwitting insiders. When individuals within an organization are not adequately educated or trained on security protocols, policies, and best practices, they may inadvertently engage in actions that compromise security. Without a strong emphasis on security awareness and a culture of vigilance, employees may fall prey to social engineering tactics, such as phishing emails or pretexting, thereby unwittingly aiding adversaries in their malicious activities. Therefore, fostering a culture of security consciousness and providing ongoing training and education are essential in mitigating the risk posed by all but especially unwitting insiders.

In order to determine the level of nuclear security culture, it is necessary to perform a periodic self-assessment. The purpose of self-assessment in nuclear security culture is to estimate how deeply ingrained nuclear security is within an organization's ethos. This entails assessing key aspects of security culture against benchmarks for optimal performance. Such assessments are vital for understanding the strengths and weaknesses of an organization's security culture, fostering awareness at all levels. Unlike technical audits, they focus on human dynamics, shedding light on behaviors and interactions within the organization. While results may not directly dictate technical actions, they offer insights into underlying reasons, guiding the development of more effective security measures. This comprehensive approach considers internal dynamics and external influences, enhancing overall security resilience [10]. The IAEA offers guidance detailing a methodology for self-assessing nuclear security culture.

V. Conclusion

People are undoubtedly an organization's greatest asset, yet they can also present insider risks. While organizations deploy sophisticated physical and cyber security measures against external threats, the recruitment of insiders becomes an appealing avenue for those seeking access. This dual nature underscores the complexity of security challenges, as individuals entrusted with access and knowledge can exploit vulnerabilities from within. Therefore, nuclear power plants must balance trust with vigilance, implementing robust monitoring and screening processes to detect and mitigate insider threats. By recognizing the potential risks posed by insiders, nuclear power plants can enhance their security posture and safeguard against both internal and external adversaries.

Due to their access, authority, and knowledge, insiders possess several advantages that make them as a serious security challenge: they can bypass certain technical and administrative security measures to carry out theft or sabotage, leveraging their insider status to exploit vulnerabilities. Insiders have the capability to execute their objectives through a sequence of discrete actions over an extended period. This approach reduces the likelihood of detection and enhances the probability of achieving success. Insiders also have the

opportunity to identify the most vulnerable targets within the organization and determine the optimal timing to carry out malicious acts. This strategic advantage allows them to maximize the impact of their actions while minimizing the risk of interception.

Insider adversaries encompass a spectrum of threats within nuclear facilities. Unwitting insiders, lacking intent, inadvertently aid adversaries. Passive insiders share information but refrain from direct involvement, prioritizing anonymity. Active, non-violent insiders employ stealth or deceit, avoiding direct confrontation and termination if identification risks increase. Active, violent insiders escalate to physical force, posing a direct threat to personnel and security. Understanding these distinctions is crucial for effective threat assessment and security measures. By recognizing the motivations and behaviors of various insider types, nuclear facilities can implement tailored strategies to mitigate risks and safeguard against insider threats.

Regularly benchmarking the nuclear security culture within a nuclear power plant is vital for ensuring that existing security systems are capable of safeguarding against a wide range of threats including insiders. It also plays a key role in guiding the development of future initiatives related to security culture. Methodologies for self-assessing nuclear security culture have been devised by organizations like the IAEA, which can be customized to suit various contexts. Furthermore, nuclear power plants can enhance their security posture by conducting frequent short-term security checks, such as ad hoc challenges and cyber penetration testing exercises. These proactive measures contribute significantly to maintaining a robust and adaptive nuclear security culture.

VI. Acknowledgment

This work was supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, as part of the funding of the scientific research work of the University of Belgrade, “Vinča” Institute of Nuclear Sciences (Grant number. 451-03-66/2024-03/ 200017, 05.02.2024.)

References

[1] Objective and Essential Elements of a State’s Nuclear Security Regime. IAEA Nuclear Security Series No. 20, Vienna, 2013.

[2] D. Bulling, , M. Scalora, R. Borum, J. Panuzio & A. Donica, Behavioral science guidelines for assessing insider threats. University of Nebraska Lincoln Public Policy Center, 2008.

[3] Preventive and Protective Measures against Insider Threats. IAEA Nuclear Security Series No. 8-G (Rev. 1). Vienna, 2020.

[4] Preventive and Protective Measures against Insider Threat. IAEA Nuclear Security Series No.8, Vienna, 2008.

[5] National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements. IAEA Nuclear Security Series No.10-G. Implementing Guide. Vienna, 2021.

[6] Security of Radioactive Material in Use and Storage and of Associated Facilities. Nuclear Security Series No.11-G (Rev. 1.) Vienna, 2019.

[7] Nuclear Security Governance: Nuclear Security Management Certification Programme. Textbook. World Institute for Nuclear Security, Vienna, 2018.

[8] Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series No.13, Vienna, 2011.

[9] K. Dewey, G. Foster, C. Hobbs & D. Salisbury. Nuclear Security Culture in Practice. A Handbook of UK Case Studies. Centre for Science & Security Studies. King’s College London, 2021.

[10] Self-assessment of Nuclear Security Culture in Facilities and Activities. IAEA Nuclear Security Series No. 28-T. Technical Guidance, Vienna, 2017.