Conducting Cybersecurity Regulatory Inspections at Nuclear Facilities

Samo Tomažič
Slovenian Nuclear Safety Administration
Litostrojska 54
1000 Ljubljana

Trent Nelson
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria

Tadej Šeruga
Slovenian Nuclear Safety Administration
Litostrojska 54
1000 Ljubljana

ABSTRACT
The research paper delves into the domain of conducting cybersecurity inspections at nuclear facilities, addressing the escalating need for high protection in an era of digitalization of safety, security and emergency preparedness systems at nuclear facilities, and increasing internal and external cyber threats. Nuclear facilities stand as prime targets due to their potential catastrophic consequences if their functions were compromised. Drawing on national legislations, industry standards, best practices, and test inspection, this paper outlines a structured inspection methodology tailored to nuclear facilities for cybersecurity. This methodology encompasses an inspection guide which includes three inspection techniques (document review, interviews, and direct observations), seven key cybersecurity regulation elements (cybersecurity program, identification of functions, systems and critical digital assets, risk management, protection of a system function, change management, supply chain, incident response) and their control objectives, and applicable international guides to be used to conduct the inspection. In conclusion, the paper underscores that effective cybersecurity inspections in nuclear facilities are paramount to national and global security.

Keywords
Nuclear sector, Nuclear facilities, Cybersecurity, Inspections, Regulations

1. INTRODUCTION
Conducting cybersecurity inspections at nuclear facilities is essential for many reasons. The first and most important one is prevention of disruptions of nation's critical functions and economy [1]. Any cyber-attack could lead to significant disruptions or have severe consequences, including public health risks and long-lasting hazardous effect on the environment [2], [3]. Additionally, nuclear facilities also face cyber threats such as insider threat, organized crime, terrorism and actions by foreign states, posing serious national security concerns [4]. Identifying these threats and vulnerabilities in advance is crucial to prevent cyber-attacks. Therefore, many nations have enacted legislation, and nuclear regulators have developed requirements to ensure all key cybersecurity regulation elements at nuclear facilities are considered [5], [6]. Inspections serve as an important regulator's tool to enforce compliance with the set requirements at nuclear facilities. Alongside inspections, there are also international advisory and peer review missions that check and assess compliance [7]. In essence, cybersecurity inspections, audits and assessments at nuclear facilities are proactive measures to evaluate and verify the implementation of key cybersecurity regulation elements defined in the corresponding legislation.

This paper provides an overview of the regulatory process and how regulatory cybersecurity inspections at nuclear facilities are conducted. Moreover, it presents not only the regulatory process, but also key inspection techniques and cybersecurity regulation elements that should be included as a minimum. Due to the sensitivity of the information, the names of countries, nuclear regulators and operators are anonymized.

2. CYBERSECURITY FOR NUCLEAR SECURITY
Nuclear security encompasses measures to prevent, detect, delay, and respond to theft of nuclear or other radioactive material, and sabotage of facility functions. They are essential to protect the public and the environment from the harmful consequences of exposure to ionizing radiation [8]. Nuclear security has many subdomains such as physical protection, transport security and the accounting and control of nuclear material, among others.

Cybersecurity represents a crucial subdomain of nuclear security, intersecting with all other nuclear security domains. It involves methods and strategies to protect facility functions, computer systems, networks, and other digital infrastructure from unauthorized access, attacks, modifications, or damage. In the realm of nuclear security, the integration of cybersecurity is essential. Its aim in nuclear facilities is to protect against digital threats while ensuring safe operations, which is particularly necessary due to rapid digitalization of nuclear systems [6], [9], [10].

Efforts for improved engineering system performance like reliability, efficiency, and remote management capabilities have led to the adoption of advanced and interconnected digital technologies in critical infrastructures, including smart grids, industrial systems, and modern nuclear plants. The integration of Information and Communication Technology (ICT) is necessary for near real-time network information assembly and automated control to maintain grid stability, accompanies the adoption of advanced digital technologies. Reflecting Industry 4.0 trends and the digitalization of industrial systems, digital instrumentation and control systems, devices like programmable logic controllers, and Ethernet/IP networks are increasingly used for improved communication and control, especially in non-safety nuclear industry applications. This significantly highlights cybersecurity as a major challenge in nuclear facilities. Improvements may expose infrastructures to increased cyber threats, potentially leading to severe safety risks [11], [12]. External threats, such as the accessibility of malicious tools, are just one aspect. Challenges are multifold and span over several domains and encompass both technical and cultural dimensions within the nuclear sector. Cultural challenges involve integration of IT and OT and their different

perspectives, limited interactions, and unclear procedures. Cooperation between both worlds is fundamental in adapting to new threats. Technical challenges include inherent insecurity by design, patching difficulties, and supply chain vulnerabilities [13].

To ensure cybersecurity at nuclear facilities, it is necessary to follow a structured approach established by standards and guidelines. Compliance to general industrial cybersecurity standards such as ISA99 and NIST SP800 (NIST Special Publication 800), along with nuclear industry-specific guidance from international bodies like the IAEA (International Atomic Energy Agency) and IEC (International Electrotechnical Commission), and national entities such as the NRC (Nuclear Regulatory Commission) and NEI (Nuclear Energy Institute) in the United States, is not just a recommendation but a necessity. These standards provide a framework that directs the nuclear sector in protecting its critical infrastructure against the spectrum of cybersecurity risks, ensuring that digital advancements do not compromise the security and safety of nuclear operations [14].

Bridging the gap between cybersecurity policies and their implementation in real-world practices at nuclear facilities are regulatory inspections. By thoroughly examining how adopted standards and guidance are applied in accordance with legislation, inspectors ensure that the guidelines are integrated into daily operations and are not merely documented procedures. Inspection is a specific aspect of broader regulatory frameworks, differing from 'audit' or 'regulation.' It involves superior organizations using different tools to regulate the performance and behavior of subordinate organizations. While inspections utilize information from documentation, they go beyond desk-based reviews of documents. A defining feature of inspections is the 'site visit,' where inspectors engage directly with service providers, assess organizational processes, and review records in person, emphasizing the hands-on, evaluative nature of the inspection process [15].

2.1 The Role of Nuclear Regulator and Regulatory Inspection

Nuclear regulators around the world are responsible for professional, administrative, supervisory and development tasks in the areas of radiation and nuclear safety and security, radiation practices and the use of radiation sources, environmental protection against ionizing radiation, nuclear cybersecurity, physical protection of nuclear material and facilities, non-proliferation of nuclear weapons, protection of nuclear goods, emergency preparedness, etc. [16].

To maintain the highest level of cybersecurity in the nuclear sector, the regulators should be first to develop, implement and maintain their own cybersecurity program and prove compliance with national legislation [17]. Only then, can they conduct inspections on their nuclear licensees.

The regulator, typically a government or authoritative body, holds the responsibility of enforcing safety and compliance standards in high-risk industries. It sets the criteria for compliance, devises the methodology for inspections, and determines their frequency and scope. Inspections should be systematic and comprehensive, extending beyond mere routine checks to profoundly evaluate the facility's operations. This includes assessing the compliance with technical standards and scrutinizing the organization's commitment to safety, as evidenced through policies, employee training, and the effectiveness of response strategies. The regulator is charged with integrating insights from past inspections, staying in touch with technological advancements, and promoting a proactive culture where safety and best practices are continuously evolved and shared. The integrity and transparency of the inspection process are also important. Regulators ensure that inspectors have unrestricted access to facilities, with the autonomy to conduct both scheduled and unannounced inspections. Inspectors, equipped with expertise in complex systems, are tasked not only with identifying current compliance issues but also with foreseeing potential future risks [18].

Similar to cybersecurity standards and guidelines, there are many interpretations regarding the scope and focus of inspections. NIST defines inspections as the process of examining an object for conformity assessment and deciding of its compliance with either detailed or general requirements, based on professional judgment. This definition emphasizes the importance of thorough examination and the expertise of the inspector in ensuring that the object meets the established standards [19].

The International Atomic Energy Agency describes inspections as a complex activity encompassing examination, observation, surveillance, measurement, and testing. These techniques are designed to assess structures, systems, and components, as well as materials and various operational endeavors. The IAEA categorizes inspections into two types. On one hand there are regulatory inspections, which are the focus of this paper. They are conducted or supervised by a regulatory body, to ensure compliance, safety, and the reliability of operational systems. On the other hand are in-service inspections, conducted throughout an asset's operational lifespan to detect age-related degradation and prevent system failures [20]. They are also more commonly known as self-assessments and audits. Numerous international resources, standards, and best practices exist for conducting these inspections. For instance, the IAEA has published a document on conducting computer security assessments which encompasses inspections, self-assessments and IPPAS (International Physical Protection Advisory Service) missions [7]. The NRC also developed a methodology in 2004 for conducting cybersecurity self-assessments at nuclear facilities. The methodology was confidential and wasn’t released only until few years ago. It is designed to enable decision-makers at nuclear facilities to comprehensively understand their security posture, manage associated risks, and implement appropriate cybersecurity measures [21], [22]. IPPAS missions are conducted at the request of an IAEA member state. They cover a broad spectrum of nuclear safety and security, are advisory in nature and not legally binding. They aim to promote safe nuclear energy use and provide comprehensive reviews in various areas, including technical assistance, compliance verification, and best practices sharing. Specifically, cybersecurity assessments are part of the IPPAS missions focusing on physical protection, with cybersecurity as an integral module. These assessments offer flexibility, allowing the host country to select specific areas for review, including national-level information and cybersecurity or assessments targeted at individual nuclear facilities [23].

2.2 Regulatory Process

There are many different regulatory processes in place in the nuclear sector. One example is presented below [5]. This process involves a series of steps which are chronologically listed below (Figure 1 represent the sequence of events of a regulatory process):

1. The state develops and adopts nuclear safety and security act.

2. The regulator develops and publishes regulations (requirements) and regulatory guides. If resources are

limited, the regulator may also choose to endorse other international standards or best practices.

3. Based on the regulations and regulatory guides, the operator develops a cybersecurity program, plan, policies, procedures, etc.

4. The operator submits the developed cybersecurity plan to the regulator for approval.

5. Once the cybersecurity plan is approved, the operator starts implementing the cybersecurity plan along with associated policies, procedures, etc.

6. After the implementation, the regulator conducts an inspection of the operator, using standardized and systematically developed inspection guides.

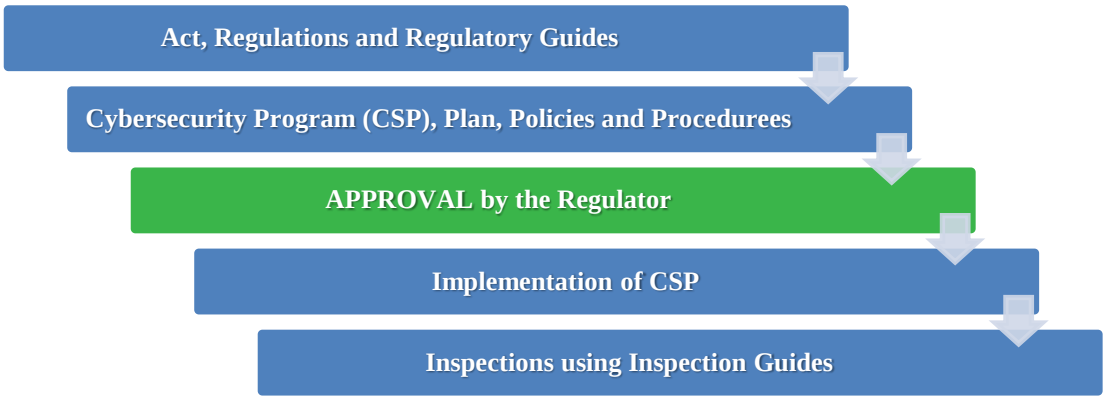

Fig 1: Regulatory Process Example

The complexity of nuclear power plants in combination with implementation of a cybersecurity program and thorough inspections of all key cybersecurity regulation elements, can take many years, sometimes even up to a decade. Additionally, inspections are not a one-time project, but an ongoing process which needs to be continuously evaluated and updated based on lessons learned and performed periodically.

It is important to acknowledge the resources and tools necessary for regulatory bodies to develop inspection guides. There can be significant disparities, especially among smaller or developing nations. Preparing for regulatory cybersecurity inspections in the nuclear sector is a complex task that requires extensive knowledge of ICT, INFOSEC, cybersecurity, and especially OT systems. It also demands significant financial resources and time commitment, straining both the inspection teams, which are often limited in personnel, and the facility operators who must balance their primary duties with compliance requirements.

The challenges are particularly daunting for developing countries, which might lack the necessary expertise, financial resources, or institutional capacity to develop comprehensive inspection guidelines independently. While they might conduct safety-related inspections, comprehensive cybersecurity inspections are often beyond their capabilities due to limited resources. This situation highlights the importance of international cooperation and knowledge sharing to assist smaller nations in enhancing their cybersecurity regulatory frameworks. During this research it became apparent, that many member states depend on the International Atomic Energy Agency for support and expertise to overcome these obstacles. In this context, this paper can be seen as a contribution to the broader goal of improving cybersecurity at nuclear facilities worldwide. By sharing insights and best practices, it aims to facilitate the development of robust inspection guides and the strengthening of cybersecurity measures, even in regions where resources may be limited.

3. METHODS

The methodology used in this research study was designed to ensure the development of a robust and adaptable inspection guide that is suitable, with minimal modifications, for global application. The methodology consisted of four phases.

In the initial phase of the development, a comprehensive review of existing literature, publicly available national legislations, industry standards, and best practices was performed. This included gathering information from relevant documents such as requirements, guides, standards, and papers on the topic of cybersecurity regulations and inspections from European states, the United States, and the IAEA.

Following the literature review, a descriptive research methodology was conducted to outline the key components of the inspection guide. This included a systematic analysis of the collected data to identify common themes, key elements, and trends in cybersecurity regulatory practices. By combining insights from different sources, the research aimed to establish a solid theoretical framework for development of the inspection methodology.

The findings were the basis for the development of the initial draft version of the inspection guide [24]. The initial draft version also included proceedings from a series of four consultancy meetings with nuclear cybersecurity experts and professionals, which were organized by the IAEA. During these meetings, approximately 30 experts from around the world provided feedback and refined the final outcomes, which are three inspection techniques and seven key cybersecurity regulation elements.

The study also involved hands-on validation in form of a pilot inspection at a nuclear facility. Albeit minor, the feedback from the inspection team was gathered, systematically analyzed, and the results were included into the development of the final version of inspection guide, which is already being used by at least two nuclear regulators.

In its final version, the inspection guide represents a comprehensive framework addressing various challenges of cybersecurity regulation in the nuclear sector. It is established in theoretical principles and international best practices, yet it remains flexible enough to accommodate country of facility specific modifications. Combined result of a literature review, descriptive research methodology, expert consultations, and a pilot inspection, are applicable across the entire nuclear sector.

3.1 Verification and validation of a draft guide

Upon completion, the draft guide underwent verification process, which included test inspection of a nuclear facility to evaluate its practical applicability. The process of verification through the pilot inspection is described in the next subsection, the results are presented in the "Results" section.

Based on the feedback gathered from the pilot inspection, the guide was revised and updated. Its efficacy and reliability were then confirmed through its continual application, currently by two regulatory bodies using this guide as the foundation for their inspections. There are strong indicators that guide will be adopted by more states, especially among the developing countries and those lacking knowledge or resources to develop such guide by themselves.

3.2 Conducting Test Inspection

In 2023 the nuclear regulator conducted the inspection on cybersecurity program of a nuclear facility, by using the developed draft inspection guide. The inspection team consisted of one senior inspector and two subject matter experts.

This inspection encompassed the first two cybersecurity regulation elements: cybersecurity program and identification of functions, systems, and critical digital assets. While conducting the inspection, techniques, described in the "Results" section were used with the intention of assessing their viability. The pilot inspection of the facility lasted for five days. The initial four days were dedicated for document review at a remote location in the regulatory offices. Documents that could be shared with the remote location (from the operator to the regulator) were shared and afterwards reviewed by the inspection team.

Based on the document review, the inspection team decided on what areas to focus on during the interviews, including deciding whom to interview, the interview methodology, timing, location, duration, etc. Additionally, they wanted to obtain additional information and support to confirm or refute findings from the document review.

On the final day, the inspection team visited the nuclear facility to conduct interviews with selected personnel and performed direct observations (walkdowns) of the facility. During this visit, the team identified several issues, which were subsequently documented in the final inspection report.

4. RESULTS

During the inspection, the senior inspector was simultaneously evaluating the process of using a draft inspection guide to determine its effectiveness. The results were deemed satisfactory, leading the regulator to decide on the adoption of this guide for the evaluation of all seven key cybersecurity regulation elements. Several minor issues were identified in the structure of the inspection guide and were corrected in the final version. The final version of the guide is applicable to both announced and unannounced inspections. It contains key cybersecurity regulation elements, their control objectives, relevant international guides and inspection techniques to be employed during the inspection. It also lists multiple verification elements that need to be validated for the cybersecurity program to be effective.

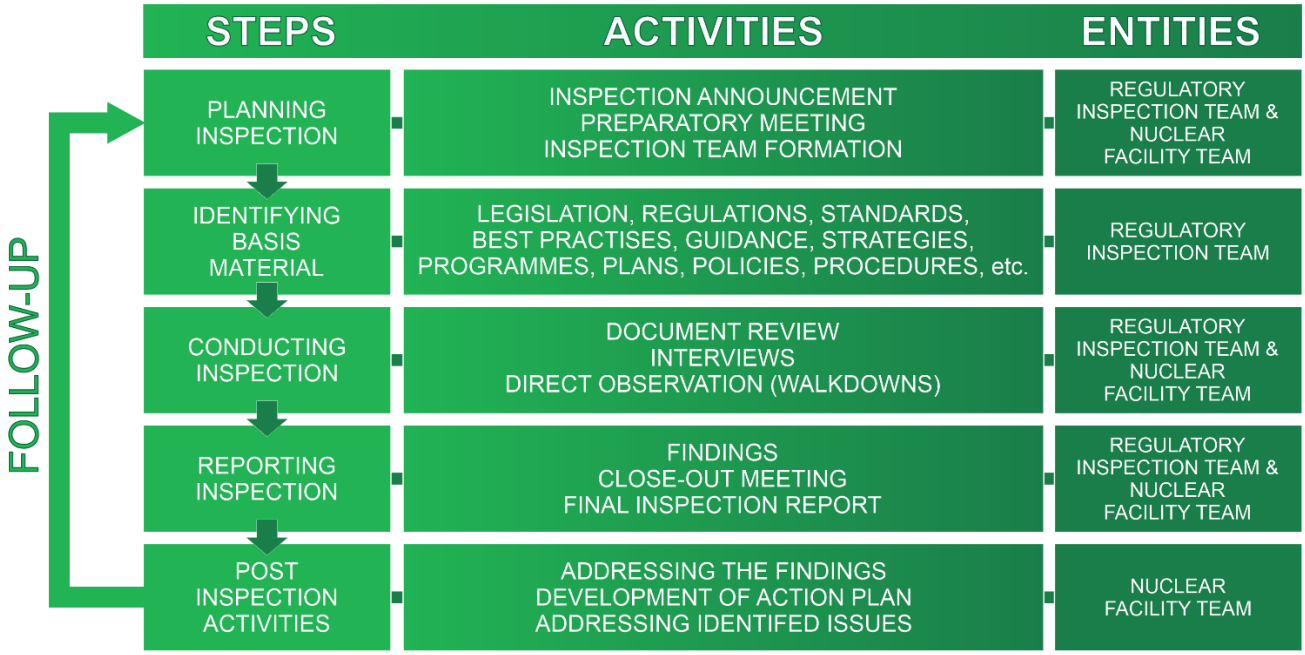

Fig 2: Inspection process

As summarized in Figure 2, the proposed methodology consists of five distinct steps, namely:

Planning Inspection: Preparation and organization of the inspection process, including the announcement of the inspection, holding a preparatory meeting, and formation of the inspection team. Inspections can also be unannounced. However, this isn't practiced for cybersecurity regulatory inspections.

Identifying Basis Material: Identification of national legislation, regulations, national or international standards, and other materials that are relevant for the inspection.

Conducting Inspection: Execution of the inspection which involves document review, conducting interviews, and direct observation (walkdowns).

Reporting Inspection: Documentation of findings, holding a close-out meeting, and preparation of the final inspection report., which serves as a foundation for an action plan.

Post Inspection Activities: Addressing the findings of the inspection, development of an action plan, and addressing identified issues.

In the following section inspection techniques are described in detail.

4.1 Inspection Techniques

The results from the descriptive research along with the proceedings of consultancy meetings with international nuclear cybersecurity experts indicate that inspectors commonly employ three techniques during inspections: document review, interviews and direct observations (walkdowns). These methods are not only prevalent in inspections but also widely used by auditors and assessors [7].

4.1.1 Document review

This process unfolds in two phases: before and during the inspection. Initially, a request for relevant documents is made to understand the program, plans, policies, procedures. This initial review aids in the development of the inspection plan. The range of documents that can be requested is wide, and it's up to the operator to decide what can be shared, considering the confidentiality level of the documents. The primary aim of reviewing documents is to assess compliance with relevant legislation and regulations.

4.1.2 Interviews

The document review process will aid in the development of the inspection plan with identified focus areas where interviews are needed to verify and clarify potential issues. The purpose of an interview is to collect and validate information through discussions with management, technical and administrative staff, and other relevant personnel. Ideally, interviews are conducted with staff employed at different levels and working areas within the facility. Interviewing is often more complex than other aspects of conducting an inspection, due to interpersonal dynamics involved. Effective interviewing requires the inspector (and the interviewee) to possess advanced social skills like empathy, listening, presentation, assertiveness, and conflict management. Additionally, determining "who" to interview is as crucial as knowing "what" to ask (question content and style), "when" to schedule the interview, "where" it should take place, and "how" it should be conducted (strategy).

4.1.3 Direct observations (Walkdowns)

Direct observations, or walkdowns, involve physically inspecting the facility, systems, or assets to identify any potential issues, hazards, or opportunities for improvement. This technique involves a trained inspector walking through the facility, observing the condition of various systems and/or assets, personnel, etc., while taking notes on any non-compliance with regulatory requirements. There are many places and processes to observe for each cybersecurity element. Walkdowns are also used by the operators for preventive maintenance purposes, identifying potential problems before they lead to costly breakdowns or operational downtime. The observations and findings from walkdowns are typically documented into a report, which can serve as a basis for prioritizing corrective actions or planning future maintenance and upgrades.

4.2 Key Cybersecurity Regulation Elements

Cybersecurity in the nuclear sector is of utmost importance, due to the potential consequences of cyber-attacks. Listed in Figure 2 are seven key cybersecurity regulation elements which aim to ensure that nuclear facilities are protected against broad spectrum of possible threats. In addition, every key cybersecurity regulation element encompasses multiple control objectives that should be covered during inspections.

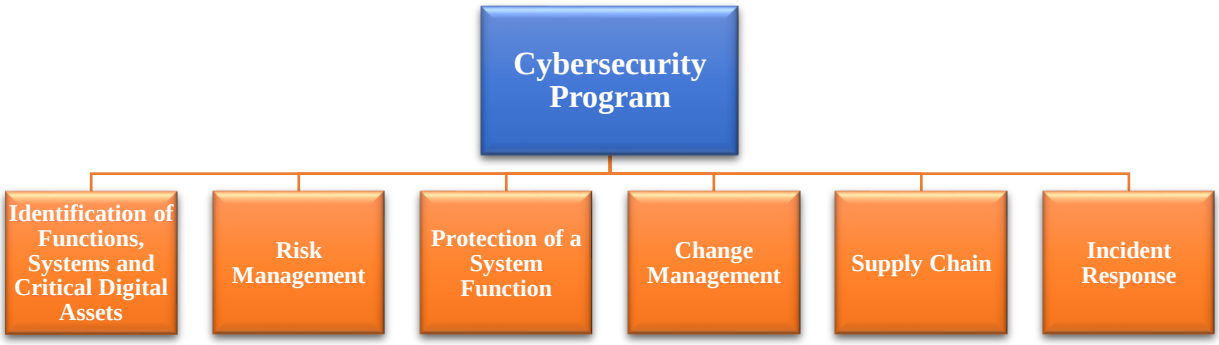

Fig 3: Seven Key Cybersecurity regulation elements

4.2.1 Cybersecurity Program

Operators should develop cybersecurity program, that forms the basis of all other cybersecurity elements listed below. During inspection, three control objectives for this element should be addressed:

- Development, implementation and maintenance of the cybersecurity program.
- Responsibility allocation and capability to perform cybersecurity activities.
- Consideration of all lifecycle stages of assets and systems.

4.2.2 Identification of Functions, Systems, and Critical Digital Assets

Cybersecurity relies on detailed list of all identified functions, systems, and critical digital assets. Lack of accurate identification or outdated information can undermine the entire cybersecurity infrastructure. This element encompasses two control objectives for inspection:

- Identification of functions, systems and digital assets, and maintenance of an active inventory of functions, systems, and digital assets.
- Protection of critical digital assets information.

4.2.3 Risk Management

A structured cybersecurity risk management process is essential, particularly in nuclear facilities. The operator should identify threats, vulnerabilities and risk associated with each digital asset and function to understand the impact on safety, security and emergency preparedness. Five control objectives for this element should be covered during inspection:

- Risk management.
- Facility cybersecurity risk management.
- Systems cybersecurity risk management.
- Threat management.
- Vulnerability management.

4.2.4 Protection of a System Function

Cybersecurity measures can be technical, physical, or administrative, or a combination of these. A combination of control measures should be selected based on a graded approach and the concept of defense in depth. Based on risk management, cybersecurity controls should be applied. In addition, implemented protective measures should provide detection, response, and recovery of safety, security functions and emergency preparedness functions. This element includes three control objectives for inspection:

- Defensive cybersecurity architecture.
- Cybersecurity by design.
- Access control management.

4.2.5 Change Management

Change management is the process of managing changes to critical digital assets, such as software, hardware, and documentation. Change control is an aspect of configuration management, which ensures that changes are controlled and systematic, preserving the security and integrity of these assets. Two control objectives for this element should be addressed during inspection:

- Change management.
- Configuration management.

4.2.6 Supply Chain

The complexity of the supply chain can create multiple attack vectors for cyber threats. To mitigate the risk, it is essential to implement contractual controls in the supply chain management process. This element has two control objectives that should be covered during inspection:

- Management of supply chain relationships.
- Evaluation and acceptance testing.

4.2.7 Incident Response

Should protective measures fail, operators must be prepared for a cyber-attack. To do so, they should develop, implement and maintain cybersecurity incident response plan, define roles and responsibilities, conduct exercises and drills, and establish reporting and notification criteria. This element has six control objectives that should be covered during inspection:

- Cybersecurity incident response plan.
- Definition of roles and responsibilities.
- Consideration of functional impacts.
- Execution of appropriate response.
- Conduct of exercises and drills.
- Implementation of reporting and notification systems.

Utilizing all seven key cybersecurity regulation elements along with associated control objectives, elevates the cybersecurity maturity level of a state, regulatory body, and a nuclear facility.

5. DISCUSSION

This paper aims to propose a structured inspection methodology tailored to nuclear facilities. The methodology encompasses an inspection guide which includes three inspection techniques:

1. Document review.
2. Interviews.
3. Direct observations or walkdowns.

Additionally, the guide emphasizes the importance of seven key cybersecurity regulation elements:

1. Cybersecurity program.
2. Identification of functions, systems and critical digital assets.
3. Risk management.
4. Protection of a system function.
5. Change management.
6. Supply chain.
7. Incident response.

The success of cybersecurity regulation elements is crucial for maintaining the safety and security of nuclear facilities. However, their effectiveness largely depends on having the right national laws in place. Therefore, nuclear regulators need to review and possibly update the current laws to ensure they fully support these important cybersecurity measures. Making these changes is key to building a strong and secure environment in nuclear facilities. We observe that systematic

inspection procedures are essential for identifying and addressing potential security risks, offering a comprehensive evaluation of cybersecurity postures of nuclear facilities. This study attempts to somewhat contribute to this. Noteworthy is also the benefit of this study for developing countries, which might lack the resources or expertise to independently develop and implement robust cybersecurity measures. Provided insights and the proposed inspection methodology can serve as valuable resources, helping these nations enhance their cybersecurity frameworks and align with international standards.

6. CONCLUSION

The paper navigates the domain of regulatory cybersecurity inspections at nuclear facilities, recognizing the urgent demand for enhanced protection amid the digitalization of safety, security and emergency preparedness systems. The paper presents an inspection methodology, anchored by a trio of techniques: document review, interviews, and direct observations or walk-downs. It emphasizes seven pivotal cybersecurity regulation elements, linked with multiple control objectives, ranging from cybersecurity programs to incident response strategies.

The dynamic nature of the cybersecurity landscape necessitates continuous improvements and adaptations of inspection methodologies. As cyber threats evolve and technology advances, inspection techniques must keep pace.

The developed methodology represents a foundational step in improving cybersecurity within nuclear facilities and requires further refinement to realize its full potential. There are numerous potential options for improvements.

Adoption of the methodology by more regulatory bodies and organizations would yield significant benefits. This would not only provide opportunities for further validation and refinement but also enable the accumulation of collective insights and experiences, ultimately contributing to the establishment of best practices in the field.

Additionally, exploring the scalability and applicability of the methodology across different national contexts is crucial. Collaborative efforts among international stakeholders, facilitated by organizations such as the IAEA, can play an important role in fostering knowledge sharing and capacity building initiatives. They are essential for supporting the adoption and adaptation of the methodology in diverse regulatory environments, thereby enhancing cybersecurity resilience on a global scale.

This study aims to be a supportive resource, offering guidance to help protect not only individual nations but also the global community in an era where digital systems are increasingly at risk. It provides an approach to enhancing cybersecurity in nuclear facilities, making it especially valuable for countries that might not have the resources to develop such strategies independently.

7. ACKNOWLEDGMENTS

We extend our gratitude to the IAEA and the experts who have contributed to this research.

8. REFERENCES

[1] Samo Tomažič and Igor Bernik, ‘Cyberattack Response Model for the Nuclear Regulator in Slovenia’, 2019, doi: 10.3217/JUCS-025-11-1437.

[2] J. A. Bullock, G. D. Haddow, and D. P. Coppola, ‘Cybersecurity and critical infrastructure protection’, in Introduction to Homeland Security, Elsevier, 2021, pp. 425–497. doi: 10.1016/B978-0-12-817137-0.00008-0.

[3] [International Atomic Energy Agency, Nuclear security recommendations on physical protection of nuclear material and nuclear facilities: INFCIRC/225/Revision 5. in IAEA nuclear security series Recommendations, no. 13. Vienna: International Atomic Energy Agency, 2011. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf

[4] SI-CERT, ‘SI-CERT (Slovenian Computer Emergency Response Team): Annual Report (2022)’, Slovenian Computer Emergency Response Team, Ljubljana, 2023. [Online]. Available: https://www.cert.si/wp-content/uploads/2023/06/Porocilo-o-kibernetski-varnosti_2022_web-1.pdf

[5] ‘Slovenian Nuclear Safety Administration: Rules on radiation and nuclear safety factors (2016)’. 2016. [Online]. Available: http://www.pisrs.si/Pis.web/pregledPredpisa?id=PRAV12796

[6] M. W. Sunseri, ‘PROPOSED DRAFT REGULATORY GUIDE 5.71, REVISION 1, “CYBER SECURITY PROGRAMS FOR NUCLEAR POWER REACTORS”’, Dec. 16, 2021. [Online]. Available: https://www.nrc.gov/docs/ML2134/ML21342A263.pdf

[7] IAEA, Conducting computer security assessments at nuclear facilities. Vienna: International Atomic Energy Agency, 2016. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf

[8] IAEA, Computer Security for Nuclear Security. Vienna: IAEA, 2021. [Online]. Available: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf

[9] A. Buzdugan and A. Buzdugan, ‘The Synergy Between Cyber and Nuclear Security. Case Study of Moldova’, in Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security, A. Sidorenko and H. Hahn, Eds., in NATO Science for Peace and Security Series C: Environmental Security. , Dordrecht: Springer Netherlands, 2020, pp. 223–231. doi: 10.1007/978-94-024-1909-2_16.

[10] Dr. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, Dr. N. Akhtar, and A. Kumar Jaiswal, ‘A Systematic Literature Review on the Cyber Security’, int.jour.sci.res.mana., vol. 9, no. 12, pp. 669–710, Dec. 2021, doi: 10.18535/ijsrm/v9i12.ec04.

[11] A. Ayodeji, M. Mohamed, L. Li, A. Di Buono, I. Pierce, and H. Ahmed, ‘Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors’, Progress in Nuclear Energy, vol. 161, p. 104738, Jul. 2023, doi: 10.1016/j.pnucene.2023.104738.

[12] I. Onyeji, M. Bazilian, and C. Bronk, ‘Cyber Security and Critical Energy Infrastructure’, The Electricity Journal, vol. 27, no. 2, pp. 52–60, Mar. 2014, doi: 10.1016/j.tej.2014.01.011.

[13] C. Baylon, R. Brunt, and D. Livingstone, Cyber security at civil nuclear facilities: understanding the risks. London: Chatham House, 2015.

[14] F. Zhang, ‘Nuclear power plant cybersecurity’, in Nuclear Power Plant Design and Analysis Codes, Elsevier, 2021, pp. 495–513. doi: 10.1016/B978-0-12-818190-4.00021-8.

[15] G. Boyne, P. Day, and R. Walker, 'The Evaluation of Public Service Inspection: A Theoretical Framework', Urban Studies, vol. 39, no. 7, pp. 1197–1212, Jun. 2002, doi: 10.1080/00420980220135563.

[16] I. Sirc and N. Ledinek, '2021 Annual Report on Radiation and Nuclear Safety in the Republic of Slovenia', Slovenian Nuclear Safety Administration, Ljubljana, Jan. 2023. [Online]. Available: https://www.gov.si/assets/organi-v-sestavi/URSJV/Dokumenti/Letna-porocila/2021/URSJV_LP_ang_2021.docx

[17] IAEA, Developing Regulations and Associated Administrative Measures for Nuclear Security: Implementing Guide. Vienna: IAEA, 2018.

[18] G. Caruso, 'Regulatory requirements and practices in nuclear power programmes', in Infrastructure and Methodologies for the Justification of Nuclear Power Programmes, Elsevier, 2012, pp. 94–125. doi: 10.1533/9780857093776.1.94.

[19] National Institute of Standards and Technology, 'Cybersecurity White Paper: EO Response', 2022. doi: 10.6028/NIST.CSWP.02042022-2.

[20] IAEA Nuclear Safety and Security Glossary. in Non-serial Publications. Vienna: INTERNATIONAL ATOMIC ENERGY AGENCY, 2022. [Online]. Available: https://www.iaea.org/publications/15236/iaea-nuclear-safety-and-security-glossary

[21] C. Glantz et al., Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants, NUREG/CR-6847, vol. 2004. 2004. [Online]. Available: https://adamswebsearch2.nrc.gov/webSearch2/main.jsp?AccessionNumber=ML15111A054

[22] G. P. Landine, C. S. Glantz, and G. A. Coles, 'A PROVEN APPROACH FOR EFFECTIVE COMPUTER SECURITY SELF-ASSESSMENTS AT NUCLEAR FACILITIES', Mar. 2020, [Online]. Available: https://www.osti.gov/biblio/1604145

[23] International Atomic Energy Agency, International Physical Protection Advisory Service (IPPAS) Guidelines. in IAEA services series. IAEA, 2014. [Online]. Available: https://books.google.si/books?id=s4feuQEACAAJ

[24] T. W. Edgar and D. O. Manz, Research Methods for Cyber Security. 2017, p. 404.