DOI 10.15199/74.2024.12.1

Mitigating Risks from Counterfeit and Substandard Components in Nuclear Power Plants through Nuclear Quality Management Measures

Ograniczanie ryzyka związanego z komponentami podrobionymi i niespełniającymi norm w elektrowniach jądrowych przez środki zarządzania jakością

Marek Tengler

Słowa kluczowe: komponenty podrobione, komponenty sfałszowane, komponenty niespełniające norm, elektrownie jądrowe, bezpieczeństwo jądrowe, zarządzanie jakością jądrową (NQM), ASME NQA-1, ISO 19443

Przemysł jądrowy stoi w obliczu poważnych wyzwań związanych z komponentami podrobionymi, sfałszowanymi i niespełniającymi norm (CFSI), które zagrażają: bezpieczeństwu, niezawodności i zgodności z przepisami. W artykule zbadano ryzyka stwarzane przez CFSI, w tym awarie systemów, naruszenia przepisów i brak zaufania społecznego, jednocześnie podkreślając problemy związane z bezpieczeństwem, takie jak potencjalny sabotaż. Podkreślono rolę zarządzania jakością jądrową (NQM) w łagodzeniu ryzyka obejmującego środki zapobiegawcze, protokoły wykrywania i strategie ciągłego doskonalenia. Przedstawiono porównawcze spostrzeżenia dotyczące norm: ASME NQA-1 i ISO 19443, szczegółowo opisując zamówienia, zarządzanie niezgodnościami i audyty dostawców. W artykule zbadano również wnioski wyciągnięte z poprzednich incydentów i przedstawiono zalecenia dotyczące wzmocnienia nadzoru nad łańcuchem dostaw, egzekwowania przepisów i stosowania zaawansowanych technologii w celu zabezpieczenia obiektów jądrowych.

Keywords: counterfeit items, fraudulent items, substandard components, nuclear power plants, nuclear safety, Nuclear Quality Management (NQM), ASME NQA-1, ISO 19443

The nuclear industry faces significant challenges from counterfeit, fraudulent, and substandard items (CFSIs), which jeopardize safety, reliability, and regulatory compliance. This article examines the risks posed by CFSIs, including system failures, regulatory breaches, and public distrust, while highlighting security concerns such as potential sabotage. To mitigate these risks, the article emphasizes the role of Nuclear Quality Management (NQM), which includes preventive measures, detection protocols, and continuous improvement strategies. Comparative insights into ASME NQA-1 and ISO 19443 standards are provided, detailing procurement, non-conformance management, and supplier audits. The article also explores lessons learned from past incidents and offers recommendations for enhancing supply chain oversight, regulatory enforcement, and the use of advanced technologies to secure nuclear facilities.

The presence of counterfeit, fraudulent, and substandard[1] items (CFSIs) in the nuclear industry poses serious risks that can compromise both safety and operational reliability. Nuclear power plants rely on high-quality, rigorously tested components to ensure safe and efficient operations. CFSIs, however, may not meet the required standards, leading to potential system failures in critical areas such as reactor pressure vessels, control systems, and cooling mechanisms. These failures could reduce safety margins and, in severe cases, result in accidents that involve radioactive releases, threatening both the environment and public health.

Beyond safety concerns, CFSIs also introduce significant reliability issues. Substandard components often fail prematurely, increasing the frequency of repairs and maintenance, causing unplanned plant outages, and raising operational costs. Identifying and replacing these

[1] There is commonly encounter the acronym CFSI that indicates S as "Suspect" item instead rather appropriate the term "Substandard", that here is used for the description purpose of much intensive falsification and misusing of standards and their criteria.

MSc. Marek Tengler (marek.tengler@rizzoassoc.cz) – Rizzo Associates Czech

faulty components can be time-consuming and costly, potentially disrupting plant operations and diminishing overall reliability. Moreover, the presence of CFSIs may result in non-compliance with nuclear safety regulations, as regulatory bodies such as the IAEA or NRC impose strict standards on component quality. Non-compliance can lead to penalties, legal challenges, and the suspension of plant licenses, further exacerbating operational risks, and in the end, costs caused by overall looses of not generate energy and consequences by the search for and elimination of non-conformities.

The supply chain in the nuclear industry is highly complex, and CFSIs can infiltrate at various stages (see six stages of supplier's tiers), including procurement, manufacturing, and maintenance. This poses a challenge for operators to maintain control over the quality of all components, particularly when dealing with international suppliers. Once CFSIs enter the supply chain, they are often difficult to trace, making it harder to ensure the safety and integrity of all affected systems. Furthermore, the discovery of CFSIs can erode public trust in nuclear safety, as any failures or incidents attributed to substandard parts could undermine confidence in the industry's ability to uphold stringent safety standards.

Security concerns (see also NIS2[2])) are also paramount when considering the potential for CFSIs to be introduced maliciously as part of sabotage efforts. Vulnerabilities in key systems could be exploited, threatening national security. Additionally, CFSIs in electronic components could expose nuclear plants to cybersecurity risks, where compromised hardware or software might allow for unauthorized access or operational disruptions.

UNDERSTANDING CFSI IN IAEA TERMINOLOGY

The term CFSI is significant because it touches on the integrity and quality assurance of components used in nuclear facilities, which directly affects nuclear safety and security.

Counterfeit Items: These are items deliberately misrepresented to be something they are not, often mimicking genuine products but produced without the proper manufacturing oversight or materials.

Fraudulent Items: Items that are intentionally misrepresented or altered for financial gain or to deceive the purchaser, such as changing documentation to indicate compliance with technical standards when in fact the item does not meet those standards.

Substandard or Suspect Items: Components or materials whose compliance with standards or authenticity cannot be confirmed. This includes items with unusual characteristics, such as lack of certifications, deviances in standards application, improper markings, or suspect sources.

DESCRIPTION OF KEY RISKS POSED BY CFSIS

The presence of counterfeit, fraudulent, and substandard items (CFSIs) in the nuclear industry are presenting critical risks due to the stringent safety and operational requirements of nuclear facilities. These risks affect not only the reliability and safety of operations but also regulatory compliance, public trust, and national security. A detailed examination of distinguished risks, supplemented with references to relevant International Atomic Energy Agency (IAEA) documents and industry standards are discussed further as following.

Safety Risks

System Failures: Nuclear power plants depend on high-quality, rigorously tested components to ensure the safety of operations. CFSIs, which do not meet the required standards, may lead to equipment malfunctions or system failures. This risk is particularly acute in reactor operations, cooling systems, and containment structures. According to the IAEA's TECDOC-1169, respectively IAEA Nuclear Energy Series NP-T-3.26, ensuring the traceability and quality of components is crucial in nuclear safety. If counterfeit or substandard items fail, the consequences can include reactor shutdowns, compromised cooling systems, or breaches in containment, threatening plant safety.

Accidents and Radioactive Releases: The most severe risk involves the potential for accidents that lead to radioactive material release. The failure of CFSIs in critical systems such as reactor pressure vessels, control rods, or emergency cooling systems could result in a loss of control over the reactor. This could escalate to core damage or the release of radioactive materials, as outlined in IAEA Safety Standards SSR-2/1, which addresses the prevention of accidents in nuclear power plants. A failure in any safety-critical component could lead to scenarios similar to past nuclear incidents, raising concerns about environmental and public health impacts.

Reduced Reliability and Increased Maintenance Costs

Frequent Repairs and Downtime: Substandard components typically fail sooner than expected, leading to unplanned outages and an increased need for repairs. This not only drives up operational costs but also reduces plant reliability. As noted in IAEA-TECDOC-1105, the use of inadequate materials can shorten the lifespan of critical systems, requiring frequent interventions, unscheduled shutdowns, and more extensive maintenance.

Inspection and Replacement Costs: Identifying and replacing CFSIs, especially post-installation, is both costly and time-consuming. Additional testing and inspection are required to detect counterfeit items, often necessitating system shutdowns. This is reinforced by IAEA's GS-G-3.1, which emphasizes the importance of quality assurance measures in the nuclear industry. The expenses associated with re-certification, quality testing, and component replacement can substantially impact operational budgets.

Regulatory Non-Compliance

Violation of Nuclear Safety Standards: The use of CFSIs can directly lead to violations of national and international safety standards, such as those set by the IAEA or the U.S. Nuclear Regulatory Commission (NRC). These regulatory bodies require that components used in nuclear facilities meet strict quality and traceability criteria. IAEA Safety Guide GS-R-3 highlights the importance of adhering to safety and quality management systems. Non-compliance due to the presence of CFSIs may result in severe penalties, fines, or even the revocation of licenses to operate nuclear facilities.

Licensing and Certification Issues: The integrity of licensing and certification processes can be severely undermined by counterfeit or substandard components. IAEA-TECDOC-1169 outlines the necessity of proper documentation, traceability, and quality certification in nuclear facilities. When CFSIs infiltrate these processes, project timelines may be delayed, or plants may be forced to shut down until the compromised components are identified and replaced.

Supply Chain Vulnerabilities

Infiltration at Multiple Stages: CFSIs can enter the nuclear supply chain at various stages, from procurement and manufacturing to maintenance. Suppliers may falsify certifications or pass off non-compliant items as genuine, making it difficult for operators to ensure the integrity of the components they receive. IAEA Safety Standards GSR Part 2 stresses the importance of stringent supplier oversight and verification procedures to prevent such risks.

[2] NIS2 references to Network and Information Security (NIS) Directive. It is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States.

Difficulty in Traceability: Once CFSIs are introduced into the supply chain, tracing them back to their source becomes a major challenge. This complicates the process of identifying all affected systems and components, increasing the risk of further failures. The IAEA Nuclear Security Series No. 13 provides guidance on securing the supply chain, emphasizing the need for enhanced traceability measures to ensure component authenticity.

Undermining Public Confidence

Erosion of Trust in Nuclear Safety: Public trust in nuclear energy is largely predicated on the assumption that the highest safety standards are maintained. The discovery of CFSIs in nuclear plants, especially if they lead to failures or accidents, can severely erode public confidence. IAEA Bulletin 60-2 discusses the need for transparency and the public's role in nuclear safety. If such incidents occur, the perception that the nuclear industry is not adequately safeguarding against these risks could have lasting impacts, including resistance to future projects or delays in the adoption of new technologies.

Potential for Increased Scrutiny: The discovery of CFSIs could lead to intensified regulatory scrutiny and negative media attention. As a result, the industry may face heightened inspections and audits, increasing operational costs and creating a general perception that nuclear operators are failing to maintain rigorous safety and quality standards.

Security Concerns

Vulnerability to Sabotage: In certain cases, counterfeit components may be deliberately introduced into the supply chain by malicious actors with the intent to sabotage nuclear facilities. The IAEA's Nuclear Security Series No. 12 highlights the importance of protecting nuclear installations from both physical and cyber threats. The introduction of fraudulent components could compromise the reliability of critical systems, posing a significant national security threat.

Cybersecurity Risks: CFSIs can also pose cybersecurity risks, particularly if they involve electronic components. Counterfeit software or hardware can introduce vulnerabilities that may be exploited to disrupt operations or gain unauthorized control over nuclear systems. The IAEA Technical Document on Computer Security at Nuclear Facilities emphasizes the need for robust cybersecurity protocols to mitigate these risks.

ROLE OF NUCLEAR QUALITY MANAGEMENT (NQM) IN CFSIS MITIGATION

As above mentioned, the IAEA has published several documents addressing the issue of CFSIs, reflecting their approach to mitigating these risks within the nuclear sector. There recognized that Nuclear Quality Management (NQM) is essential in safeguarding nuclear facilities from the risks posed by CFSIs. By adhering to internationally recognized practices such as ASME NQA-1 and ISO 19443, organizations can implement robust quality management systems that emphasize preventive measures, detection, and continuous improvement. These frameworks ensure that suppliers are properly scrutinized, materials are traceable, and non-conformances are addressed promptly, thereby maintaining the safety and integrity of nuclear operations.

In general, each NQM (Nuclear Quality Management) system typically addresses the challenge of CFSIs in three main ways: through preventive measures, by process of detection and subsequent response, and establishing a continuous improvement program.

Preventive Measures

Essential role of NQM is to implement robust preventive measures that detect and prevent the entry of CFSIs into the nuclear supply chain. It includes supplier qualification and audits that thorough evaluation of suppliers to ensure they meet the necessary quality and regulatory standards. Auditing processes can help identify any potential CFSIs at an early stage, mitigating risks before they escalate.

Another critical aspect of prevention is the implementation of strict procurement controls. These controls ensure that only certified and verified items are purchased for use in nuclear facilities. NQM enforces procedures such as requiring authenticated documentation and establishing clear traceability for all components. This guarantees that every item meets the necessary standards and helps prevent the introduction of counterfeit items into the supply chain.

Material traceability is also a key preventive measure. By maintaining a robust system that tracks materials and components from the supplier to their final use, NQM ensures that any defective or suspect items can be quickly identified and isolated. This approach minimizes the impact of potential risks and strengthens the overall integrity of the supply chain.

Detection and Response

If counterfeit or fraudulent items (CFSIs) manage to bypass preventive measures, the NQM system is designed to enable rapid detection and response. This ensures that any issues are identified quickly and addressed appropriately, minimizing risks associated with defective components.

One of the key components of this system is Non-Conformance Reporting. Organizations are required to establish a system that allows for the reporting and handling of non-conformances, including CFSIs. This mechanism ensures that corrective actions can be taken immediately, preventing the further use or deployment of faulty or compromised items.

In addition to reporting, continuous inspection and testing play a crucial role in detecting CFSIs. Materials and components are subjected to thorough inspections upon arrival and periodic testing throughout their lifecycle. This constant vigilance ensures that any potential issues are identified as early as possible.

When CFSIs are detected, performing a detailed root cause analysis becomes essential. By identifying the underlying cause of the issue, organizations can implement strategies to prevent similar occurrences in the future, enhancing overall system reliability and safety.

Continuous Improvement

Nuclear Quality Management (NQM) frameworks prioritize continuous improvement to address the evolving risks associated with counterfeit and fraudulent items (CFSIs). As counterfeit methods become more sophisticated, it is essential for organizations to adapt and enhance their detection and prevention strategies by specific programmes.

One key aspect of continuous improvement is employee training and awareness. Regular training programs are essential to keep staff informed about the latest risks and signs of CFSIs. By ensuring that employees remain vigilant and knowledgeable, potential issues can be identified and addressed more quickly.

Another critical element is updating supplier evaluation processes. It is important to continuously revisit and revise supplier audits, incorporating new risks and technological advancements in the detection of counterfeit materials. This ensures that organizations stay ahead of potential threats and maintain the integrity of their supply chains.

Comparison between approaches of ASME NQA-1 and ISO 1943 how is recognize and dealing CFSI issue, are summarized in the matrix, see following Table. Specific differences are highlighted there.

Key Aspects	ASME NQA-1	ISO 19443
Procurement Requirements:	· Requires that procurement documents clearly identify technical and quality requirements, including any CGI dedication activities. It ensures that the supplier provides items that meet the safety classification requirements. · CGI dedication in ASME NQA-1 follows a prescriptive approach, where specific activities must be performed to verify that items meet the design and safety requirements.	· Focuses on ensuring that suppliers understand and meet nuclear-specific requirements. The procurement requirements include the need to ensure conformity with both regulatory and contractual requirements. · The standard encourages suppliers to adopt a risk-based approach when considering procurement, with an emphasis on the quality management system.
Control of Purchased Items	Establishes controls to ensure that purchased items and services meet specified requirements. This involves acceptance testing, supplier evaluation, and verification processes, especially when dealing with CGI dedication.	Requires suppliers to ensure that items and services are delivered according to the agreed requirements. ISO 19443 emphasizes performance monitoring, including verification and validation activities that suppliers must conduct for critical components.
Non-conformance and Corrective Actions	Non-conformances must be identified and documented, with corrective actions implemented to prevent recurrence. This includes a requirement to investigate the root cause and determine the necessary steps for resolving the non-conformance.	There is a focus on continual improvement, and suppliers must have a system in place to manage non-conformances. Corrective actions should follow a risk-based approach, and it encourages a culture of proactive identification and prevention of issues.
Quality Audits	Requires the establishment of a formal audit program, including audits of suppliers and subcontractors, to verify that quality assurance requirements are met.	Similar to NQA-1, ISO 19443 requires audits of the quality management system and emphasizes supplier performance in nuclear safety. However, it places additional focus on continual improvement and risk-based thinking during audits.
Risk-based Approach	ASME NQA-1 does not explicitly emphasize a risk-based approach but mandates rigorous control processes, especially in procurement, testing, and supplier evaluations. Risks are managed through prescriptive quality assurance measures.	Strongly emphasizes a risk-based approach across all processes. Risk assessment and mitigation are integrated into supplier evaluation, procurement, and non-conformance handling, ensuring that nuclear-specific risks are addressed systematically.
Supplier Assessment and Qualification	Suppliers must be evaluated and qualified based on their ability to meet nuclear safety and quality requirements. The qualification process involves audits, reviews, and tests to verify the supplier's capability.	Supplier assessment and qualification are based on the supplier's ability to meet the requirements of the nuclear quality management system. ISO 19443 incorporates a risk-based approach in evaluating suppliers and encourages ongoing performance reviews to ensure that safety and quality requirements are met.
Documented Information and Traceability	Requires comprehensive documentation to ensure traceability throughout the lifecycle of items and services, especially with regard to CGI dedication. Detailed records are maintained to demonstrate compliance with safety and quality requirements.	Requires suppliers to maintain documented information that provides traceability of materials, components, and services. ISO 19443 emphasizes the importance of controlling documents, ensuring traceability from procurement to delivery, and maintaining records that support nuclear safety.
Engagement and Communication	Focuses primarily on ensuring that all parties involved in the procurement, production, and supply chain processes follow the set quality assurance guidelines. Communication between contractors, suppliers, and the purchaser is emphasized to ensure adherence to safety standards.	Engagement and communication are emphasized more explicitly in ISO 19443. The standard promotes open communication between all parties in the supply chain, particularly in managing risks, addressing non-conformances, and ensuring that nuclear safety requirements are clearly understood and implemented by suppliers.

LESSONS LEARNED

In recent years, there have been notable instances of counterfeit, fraudulent, and suspect items (CFSIs) affecting the nuclear industry, and changing the attitude and intensify efforts to protect nuclear market to control the infiltration of substandard components. In 2012, a major scandal revealed that several South Korean nuclear reactors used components with forged safety certificates. This led to the shutdown of multiple reactors and extensive investigations, which uncovered that companies supplying KHNP had provided over 7,000 non-safety-critical parts with falsified documentation. These parts included fuses, switches, and cooling fans, though none were directly involved in reactor safety systems [2].

More broadly, the presence of CFSIs is not confined to South Korea. A 2022 report from the U.S. Nuclear Regulatory Commission (NRC) found evidence of CFSIs in several U.S. nuclear power plants. These items ranged from pump shafts to breaker switches, which are critical in safety-related functions. Despite efforts to prevent such occurrences, the NRC found that reporting requirements and detection systems still have gaps that could allow CFSIs to go undetected [8].

Lessons learned include:

- Strengthening Supply Chain Oversight: The incidents in both South Korea and the U.S. highlight the critical need for robust oversight of the nuclear supply chain. In the KHNP case, counterfeit parts entered the system due to insufficient scrutiny of suppliers, revealing a vulnerability in certification processes. To address this, nuclear operators must enhance supplier vetting procedures, enforce rigorous audits, and mandate third-party verification of safety-critical components. Additionally, tracking the origin of parts in real-time can prevent similar lapses, ensuring that only certified, safe components are used.
- Improving Reporting Mechanisms: The U.S. Nuclear Regulatory Commission's 2022 report [9] underscored deficiencies in reporting systems that allowed counterfeit, fraudulent, and suspect items (CFSIs) to evade detection. Even though mechanisms for identifying such items existed, gaps in mandatory reporting delayed their discovery. To combat this, regulators and plant operators should implement more comprehensive reporting protocols that require the immediate disclosure of CFSIs, regardless of their perceived impact on safety. Enhanced transparency will play a crucial role in the early identification and mitigation of these risks [12].
- Increasing Regulatory Vigilance: The South Korean case demonstrated the significant financial and operational consequences of inadequate regulatory oversight, as multiple reactors had to be shut down. This scandal exposed both supplier malpractice and the regulatory system's failure to detect these issues early. To prevent recurrence, regulatory bodies should continually update and strengthen guidelines for CFSI detection, conduct surprise inspections, and collaborate with international agencies to share information about potential threats in the nuclear supply chain.

- Fostering a Culture of Safety: The incidents in both countries revealed that components, even those not directly linked to reactor safety, can still compromise the integrity of nuclear power plants if they lack proper certification. This disregard for safety protocols undermines the culture of safety that is essential in high-risk industries like nuclear power. Operators and suppliers must cultivate a strong safety culture where all staff, from engineers to contractors, prioritize long-term safety and feel empowered to report any suspicious activities or violations of safety standards.
- Leveraging Technology for Detection: The presence of CFSIs in nuclear power plants highlights the need for advanced technological solutions to improve detection and prevention. Detection gaps suggest that existing systems are not sufficient. Investments in technologies like blockchain, which can ensure transparency and traceability in supply chains, and AI-based tools that detect irregularities in procurement processes, could significantly reduce the risk of CFSIs entering nuclear facilities.
- Enhancing Global Collaboration: These cases illustrate the value of international cooperation in mitigating the risks associated with counterfeit and fraudulent items in the nuclear industry. Sharing lessons learned, case studies, and information on suspect suppliers across borders can strengthen the global nuclear industry's defenses. Governments and regulatory bodies should encourage joint safety audits, create shared databases, and establish international regulatory standards to prevent similar incidents from occurring in other regions, ultimately bolstering the safety of the global nuclear infrastructure.

CHALLENGES IN IMPLEMENTING NQM MEASURES

Implementing nuclear quality management (NQM) measures to prevent counterfeit, fraudulent, and suspect items (CFSI) presents several challenges. These challenges are critical to address because of the high safety and operational risks that CFSI pose in nuclear power plants. Below are some of the key issues:

Complexity of Supply Chains

Global Sourcing: Nuclear power plants often rely on complex global supply chains, involving numerous vendors and sub-suppliers across multiple countries. Ensuring that all suppliers adhere to strict quality management standards, including preventing CFSIs, becomes increasingly difficult. For example, tracing the origin and authenticity of materials or components in such a diverse network can be challenging, especially when suppliers use multiple layers of subcontracting [4].

Supplier Variability: Suppliers within the nuclear industry range in size and sophistication. Smaller suppliers may lack the resources or expertise to implement rigorous NQM processes, increasing the risk of non-compliant components entering the supply chain. This variability complicates efforts to standardize quality management across all levels of the supply chain [7].

High Cost of Comprehensive Quality Assurance

Expensive Testing and Inspections: Comprehensive quality assurance measures, including advanced material testing and detailed audits, can be prohibitively expensive. Particularly for smaller vendors, maintaining the necessary testing facilities and resources for continuous inspection increases costs, which may lead to resistance or shortcuts that open the door for CFSIs.

Continuous Monitoring: NQM systems require ongoing monitoring of suppliers and components, which can be resource-intensive. With the increased volume of parts being used in large-scale nuclear projects, performing real-time monitoring, especially on components that may not appear safety-critical at first glance, is difficult [1].

Evolving Threats and Standards

Changing Nature of CFSI Threats: As detection methods improve, counterfeiters adapt their tactics. For example, the falsification of safety certificates or the production of high-quality counterfeits makes it harder to detect fraudulent parts. Regulatory frameworks and standards need to be continuously updated to address these evolving threats, requiring frequent updates in training, auditing processes, and technological detection methods [4].

Updating Industry Standards: ISO 19443 and other relevant standards require periodic revisions to keep up with emerging CFSI risks. However, updating and implementing these standards across global supply chains is slow, and organizations must invest in continuous training and system upgrades to stay compliant. This lag in adaptation creates vulnerabilities where outdated practices may allow CFSI to infiltrate the supply chain [1].

Cultural and Organizational Resistance

Resistance to New Processes: Suppliers and internal teams often resist the adoption of new, stricter NQM measures due to the increased administrative workload and perceived impact on profitability. This is especially true for suppliers who may not fully understand the critical importance of these measures in the nuclear industry. Overcoming this resistance requires significant effort in training and culture change [6].

Human Factors: Even with rigorous processes in place, human errors and oversight can lead to CFSI slipping through quality control. For instance, inadequate training of personnel in recognizing counterfeit components, or fatigue in auditing long supply chains, can compromise the effectiveness of NQM efforts [2].

Inconsistent Regulatory Oversight

Varied Enforcement Across Jurisdictions: While nuclear regulatory bodies like the IAEA and NRC provide global standards, enforcement and oversight of CFSI-related regulations can vary significantly between regions. Some countries may have more robust auditing and quality control practices than others, creating inconsistencies in how CFSI risks are managed within the global supply chain [1].

Regulatory Gaps: In some cases, regulatory bodies may not require mandatory reporting of CFSI incidents unless a failure has a significant impact on safety. This means that near-misses or smaller failures caused by CFSIs may go unreported, leading to an underestimation of the scale of the problem [11].

RECOMMENDATIONS FOR ENHANCING NQM EFFECTIVENESS

To address the critical risks posed by counterfeit and fraudulent substandard items (CFSIs) in the nuclear industry, the following recommendations are proposed, focusing specifically on industry-specific challenges:

- **Enhanced Collaboration**:

Strengthening cooperation between nuclear industry stakeholders, regulatory bodies like the Nuclear Regulatory Commission (NRC), and international organizations such as the International Atomic Energy Agency (IAEA) is crucial for ensuring safety and reliability in nuclear operations. Nuclear-specific collaborations allow for the sharing of best practices, incident reports, and technical data, fostering a unified global approach to mitigating CFSIs. For example, partnerships between nuclear operators and regulatory authorities have been proven to prevent counterfeit components from entering critical systems [3]).

- **Advanced Technologies for Nuclear Traceability**:
  The adoption of advanced technologies like blockchain and AI can be particularly transformative in the nuclear industry, where the integrity and traceability of components are paramount. Blockchain can ensure tamper-proof tracking of nuclear-grade materials and components throughout the supply chain, significantly reducing the risk of counterfeit parts entering nuclear facilities. Similarly, AI can enhance the detection of substandard or fraudulent items by using predictive models to assess the quality and authenticity of components [5]. Implementing these technologies aligns with the industry's stringent safety and quality standards, enhancing operational security.
- **Regulatory Oversight and Enforcement**:
  In the nuclear sector, stringent regulatory oversight is non-negotiable. Regulatory bodies such as the NRC and IAEA need to enforce stricter compliance with Nonconforming Quality Management (NQM) standards to ensure that all components meet the highest safety requirements. The enforcement of penalties for non-compliance is critical in deterring suppliers from introducing CFSIs into the nuclear supply chain. Effective regulatory oversight in nuclear industries includes regular audits, supplier verifications, and component testing, all of which are essential to maintaining safety and preventing catastrophic failures [6].
- **Global Supply Chain Monitoring in the Nuclear Industry**:
  Given the global nature of nuclear supply chains, establishing robust networks for real-time monitoring is vital. International organizations such as the IAEA and the World Nuclear Association (WNA) are already working on initiatives to strengthen supply chain monitoring to detect CFSIs early. These networks would enable the identification of counterfeit components before they can enter nuclear facilities, ensuring that only certified, high-quality materials are used in construction and maintenance [10]. Enhanced global monitoring reduces the risk of substandard materials compromising the safety of nuclear plants.

CONCLUSION

The infiltration of counterfeit, fraudulent, and substandard components (CFSIs) poses a serious threat to the safety and operational integrity of nuclear power plants. As demonstrated throughout this article, Nuclear Quality Management (NQM) plays a pivotal role in preventing these risks by implementing robust measures such as supplier qualification, rigorous inspection protocols, and employee training. Although there are challenges in executing these strategies, such as complex supply chains and evolving threats, the case studies discussed underscore the importance of maintaining stringent quality standards.

By enhancing collaboration, leveraging advanced technologies, and strengthening regulatory oversight, the nuclear industry can further protect its operations from the dangers posed by CFSIs. Continuous improvement in NQM practices is essential to safeguarding public health and ensuring the safe, reliable operation of nuclear power plants in the future, and maintain public trust in the safety of nuclear energy.

Artykuł recenzowany, wpłynęło 26.11.2024

CITATION LIST

[1] American Nuclear Society. „WNA Publishes Report on the World's Nuclear Supply Chain." Last modified June 21, 2023, https://www.ans.org/news/article-5275/wna-publishes-report-on-the-worlds-nuclear-supply-chain/.

[2] Counterfeit Parts Blog. „Korean Industry Perspective on Counterfeit, Fraudulent & Suspect Items (CFSI)." Last modified June 17, 2014, https://counterfeitparts.wordpress.com/2014/06/17/korean-industry-perspective-on-counterfeit-fraudulent-suspect-items-cfsi/.

[3] International Atomic Energy Agency (IAEA): International Atomic Energy Agency. „Combatting Counterfeit and Fraudulent Items in the Nuclear Supply Chain: Best Practices for Industry Collaboration." Vienna: IAEA Publications, 2021.

[4] International Atomic Energy Agency. „Management of the Nuclear Supply Chain." Accessed October 23, 2024, https://www.iaea.org/topics/management-systems/management-of-the-nuclear-supply-chain.

[5] Nuclear Energy Institute (NEI): Nuclear Energy Institute. „Blockchain and AI in Nuclear Safety: Technologies for the Future." Washington, D.C.: NEI Reports, 2022.

[6] Nuclear Regulatory Commission (NRC): Nuclear Regulatory Commission. „Regulatory Oversight in the U.S. Nuclear Sector: Ensuring Compliance with Quality Standards." Washington, D.C.: NRC Publications, 2019.

[7] OECD Nuclear Energy Agency. „Working Group on Supply Chain (WGSUP)." Accessed October 23, 2024, https://www.oecd-nea.org/jcms/pl_87531/working-group-on-supply-chain-wgsup.

[8] Securing Industry. „OIG Report Confirms Fake Parts Found in US Nuclear Plants." Last modified June 28, 2023, https://www.securingindustry.com/electronics-and-industrial/oig-report-confirms-fake-parts-found-in-us-nuclear-plants/s105/a14225/.

[9] U.S. Nuclear Regulatory Commission. „Counterfeit, Fraudulent, and Suspect Items (CFSI)." Accessed October 23, 2024, https://www.nrc.gov/about-nrc/cfsi.html.

[10] World Nuclear Association (WNA): World Nuclear Association. „Global Nuclear Supply Chains: Strengthening Monitoring to Mitigate Risks." London: WNA Reports, 2020.

[11] World Nuclear News. „Report Sees Opportunities for Nuclear Supply Chain." Last modified July 12, 2023, https://www.world-nuclear-news.org/Articles/Report-sees-opportunities-for-nuclear-supply-chain.

[12] World Nuclear News. „US Watchdog Investigates Counterfeit Component Issues in Nuclear Plants." Last modified June 22, 2023, https://www.world-nuclear-news.org/Articles/US-watchdog-investigates-counterfeit-component-iss.

INTERNATIONAL REFERENCES:

- NRC Regulatory Issue Summary 2015-08. „Oversight of Counterfeit, Fraudulent, And Suspect Items In The nuclear Industry"
- ANSI/ANS-3.2-2012. „Managerial, Administrative and Quality Assurance Control for Operational Phase of Nuclear Power Plants"
- ASME NQA-1, „Quality assurance Requirements for Nuclear Facility Application"
- EPRI NP-6629 „Guidelines for the procurement and receipt of items for nuclear power plant", May 1990.
- EPRI TR-1019163, „Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items", October 2009.
- EPRI TR-1021439 „Plant Support Engineering: Counterfeit and Fraudulent items - A Self- Assessment checklist", October 2010
- IAEA-TECDOC-1169, „Managing Suspect and Counterfeit Items in the Nuclear Industry", August 2000.
- INPO Event Report, IER L4-12-86, "Counterfeit Parts and Equipment Vulnerability"
- US Department of Energy (DOE) G 414.1-3, „Suspect/Counterfeit Items Guide for Use with 10 CFR 830 Subpart A, QA Requirements, and DOE O 414.1D, QA"
- IAEA NP-T-3.26, „Managing Counterfeit and Fraudulent Items in the Nuclear Industry", 2019.
- IAEA NP-T-3.21, „Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities", 2016 r.

Publikacja artykułu została zrealizowana na zlecenie Ministerstwa Przemysłu w ramach realizacji przez Izbę Gospodarczą Energetyki i Ochrony Środowiska szkolenia dla polskiego przemysłu pod kątem wykonywania prac dla energetyki jądrowej.

IGEOS nuclear Ministerstwo Przemysłu polskiatom