Advances in Reliability, Safety and Security, Part 8 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-20-3 (printed), ISBN 978-83-68136-07-4 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Measures To Protect Nuclear Power Plants From Fraudulent Items

Jan Jirousek[a], Jan Prochazka[b], Dana Prochazkova[b]

[a]*State Office for Nuclear Safety, Praha, Czech Republic*
[b]*Czech Technical University, Ptaha, Czech Republic*

Abstract

The article summarizes knowledge about the issue of fraudulent items that disrupt the safety of industry, energy and other objects that are important for the life of human society. It states: the causes of occurrence of fraudulent items in nuclear power plants; principles for reducing the risk associated with fraudulent items; and measures applied by nuclear safety supervision in the Czech Republic in the area of ensuring the protection against fraudulent items. In conclusion, a checklist is provided to identify risks in the management system of the nuclear facility operator.

Keywords: nuclear power plant, risk, safety, fradulent items, checklist

1. Introduction

A fake, forgery, or forgery is an item that passes for another, usually an object of higher value. Its originator is a forger or falsifier and its activity is referred to as counterfeiting. Today, counterfeits can be found in many areas, from means of payment (counterfeiting), deeds and documents, through works of art, antiques and industrial goods, especially branded or very important ones. Nowadays, counterfeit and fraudulent items are a growing problem for the industry.

There are many places where counterfeits are created, it is the entire supply chain. Therefore, procedures for detecting and reporting the suspicious items must be put in place at nuclear installations in order to ensure safety. The article follows selected procedures for ensuring the protection of nuclear facilities against fraudulent items. Specifically, it states:

- the causes of the occurrence of fraudulent items in nuclear power plants;
- principles for reducing the risks associated with fraudulent items;
- methodology for assessing the acceptability of commercial quality items for nuclear installations;
- a specific example of a checklist used by the State office for Nuclear safety for targeted inspections focused on safety in the monitored area.

2. Present situation

Counterfeit and fraudulent items are a growing concern worldwide, especially for critical infrastructure, including the nuclear facilities. They often pose an immediate and potential threat to the safety of workers, the performance of facilities, the safety of the public and the environment, and have a great potential to adversely affect the costs of operation and maintenance of nuclear installations. The concerns in question go well beyond the level of the nuclear installations themselves and extend to the level of the semi-finished products used in the construction of nuclear installations and in the selection of chemical and other auxiliary substances to be used in such nuclear installations. Even in cases where an item for a nuclear facility is purchased from a certified original equipment manufacturer, there is a possibility that the materials or components or documentation used by the manufacturer may be counterfeit or fraudulent at some point in the supply chain (IAEA, 2016). Therefore, the monitoring of supply chains and procurement procedures at nuclear installations play a major role in detecting and preventing the introduction of such counterfeit or fraudulent items into nuclear facilities.

The current situation is illustrated by the following facts - according to (IAEA, 2016). The United States Department of Commerce states that there was a 140% increase in counterfeit items among suppliers of industrial parts to the United States Department of Defense between 2006 and 2009, and this meant problems not only in defense, but also in national safety. According to U.S. Customs, Border Protection, Immigration and Customs and Customs Enforcement, the retail value of counterfeit and pirated goods seized in 2012 was more than $1.26 billion, representing a more than 21% increase in the value of seized goods compared to 2011 values (Tannenbaum 2014).

Fraudulent items in nuclear facilities, e.g. according to (EPRI, 2014), have been detected in many areas: machinery; electrical equipment; apparatuses; software; certificates; services; and building blocks.

One obvious common element of fraud is the potential for profit (Tannenbaum, 2014). Counterfeiters can sell their products on the market at prices equal to or lower than the price of the original items without incurring the costs associated with: research and development in the field of materials, production and testing; licensing responsibilities; marketing; and other expenses that are usually incurred by legitimate producers. A particularly high flow of counterfeit materials and products is from Asia (Tannenbaum, 2014); Figure 1.

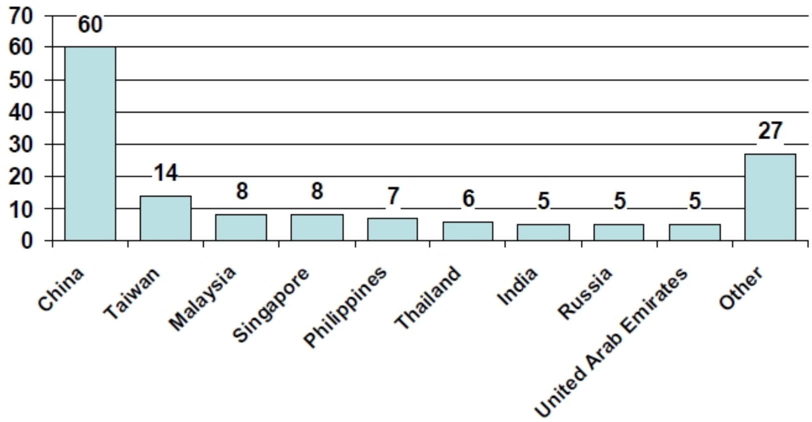

Fig. 1. Countries suspected of being sources of counterfeits - results of a survey conducted in January 2010 (Tannenbaum, 2014).

The results of detailed investigation of:

- problems connected with fraudulent items in nuclear power plants and in nuclear industry,
- good practice connected with identification of fraudulent items and prevention their location in nuclear power plants and nuclear industry

are summarized in work (Prochazkova and Prochazka, 2022).

3. The IAEA knowledge and guidance on fraudulent items

In the document (IAEA, 2016), the IAEA presents the facts that indicate the causes of the occurrence of fraudulent items in nuclear facilities, as well as protective measures:

- in recent years, nuclear installations have been affected by major events and facts related to public procurement. There have been temporary and permanent shutdowns of nuclear power plants due to the installation of counterfeit, fraudulent and suspicious items related to: increased reliance of nuclear power plants on digital devices and software components; computer security; increased globalization of the nuclear supply chain; obsolescence of items and ageing of nuclear power plant components; the gradual narrowing of the supply chain as a result of the interruption of nuclear construction in the 1990s; reduction of supply chains caused by changes in atomic legislation and subsequent insurance of nuclear damages; increasing the availability of technologies that can be used for the falsification of accompanying the technical documentation; increasing the availability of "reverse engineering" technologies; and requirements for the protection of personal data involved in the processes of production, testing and verification of items, and therefore, it is necessary for organizations engaged in the purchase (acquisition) of critical items for nuclear facilities to systematically consider these facts;

- a significant number of nuclear power plants in some countries are approaching the end of their original design lifetime or are striving for an extended lifetime. With aging the equipment comes increased difficulties in sourcing the parts to support the maintenance and repair of critical components. More than 20% of nuclear power plant equipment in some countries is considered obsolete. The original suppliers of components have completely ceased their operations, consolidated with other companies, or made business decisions (usually due to reduced market demand) not to manufacture certain items or not to supply them with nuclear quality certificates (i.e. that they have the required safety) because it has become costly to maintain nuclear certificates from national regulators or nuclear damage reinsurers;
- the current situation is also complicated by the fact that there is only limited information available on the original procurement of original components for nuclear power plants. Due to changes over time, technical information and expertise related to some items is incomplete or lost. This is especially true for products that represent a small portion of suppliers' products. These facts are, therefore, a source of risks for safety and economics, which will manifest themselves during the operation. These risks lead to unplanned downtime because safety-related equipment is not available when it is required or is not of the required quality. As a result, an engineering function in the procurement sector has already been created in some countries. The main function of the engineering is to identify technical, qualitative and commercial requirements for critical items and to carry out conformity assessments (equivalence) of items, especially those that are obtainable from the commercial market;
- the procurement function for nuclear installations plays a key role in nuclear safety. Enquiries in public tenders can have a positive effect in terms of the price offered. At the same time, however, the same mechanism works against ensuring the high quality and safety when the 'minimum bid price' criterion is usually used. This application typically discriminates against manufacturers with a long tradition of production, who are burdened with the costs associated with developing technology and maintaining key personnel, technology and documentation that are necessary for production and verification of the quality/safety of the item. The purchase of items, especially critical ones, affects the lifetime of nuclear facilities. During the initial design, designers specify the materials to be used for the manufacture of a particular device. This specification has long-term implications for supply chain actors and for future operations. During the construction and the commissioning, service contracts are concluded in order to recruit personnel and related services. During the operation, spare parts for maintenance are purchased, engineering and other services are used, and even minor changes are made compared to the project (associated with related material purchases). The quality and size of the stock of materials and spare parts has an impact on the operating costs of the equipment. During the decommissioning process, important contracts are concluded in some countries, with the result that some parts that are not too worn, or surplus stocks, are brought back to the market, where they can be sold as new after a little modification;
- in a number of cases of nuclear installations, the best practice of procurement of supplies and activities related to the operation and maintenance of nuclear installations is not followed, which is to include the following activities for each lot: identification of needs; a description of requirements; performing a value analysis; conducting a supplier survey; negotiation on quality, production process, delivery dates and price; purchasing activities; setting the criteria for product acceptability; item inspection and test plan; contract management; inspections and inventories;, mode of transport; admission and acceptance tests; and storage requirements;
- supply chain management involves planning and managing all activities related to sourcing, procurement management, changes, and logistics. It also involves coordinating and collaborating with distribution partners who are not direct suppliers, intermediaries or service providers. Supply chain management integrates supply and demand within and across participating companies. In the context of nuclear installations, it is assumed that: procurement has an active role in supply chain management; and in the supply chain organization of the operational organization, i.e. the nuclear installation, and namely in contrast to the classic relatively passive role of the operational organization, which consists of simply issuing procurement specifications and responding to tenders. Therefore, for new nuclear construction projects, suppliers of Tier 1 technologies (i.e. critical items), it needs to set up and manage supply chains, while the procurement of spare parts related to operation and maintenance activities uses a commercial basis to the widest extent possible. These two activities are always linked, as purchasing decisions and choices made by a technology supplier (e.g., the choice and location of key suppliers) have implications for the entire supply chain throughout the lifetime of the equipment. The above-mentioned necessary measures, cultivating the environment of supply chains, can, if interpreted uninformed, give the non-professional public the wrong impression that their introduction distorts the free movement of goods and

services on the market, with the accompanying phenomena described below. From the point of view of valid legislation, the obligation to manage and control its supply chains lies with the operator. At the same time, the operator is significantly limited in this activity by other supranational provisions implementing the conditions for the movement of goods on the free market. Based on all these requirements and international experience from recent times, a number of suppliers and operators apply ČSN EN ISO 19 443 (2018) to increase the transparency of their chains;

- in general, the risks in the procurement process are: bribery; giving gifts; conflict of interest; ignoring the absence or falsification of documentation; money laundering; nepotism; blackmail; influencing the trade; reducing the apparent value of the purchase in order to avoid competition requirements; approval of an unfair practice (e.g. splitting and awarding projects or contracts as multiple consecutive contracts to the same contractor); pressure on workers (including subcontractors) through unfair labor practices to disregard industrial safety standards;
- to ensure safety, a clear risk management strategy must be focused on safety – ISO 31000, 31010. Risk management is a continuous and iterative process that includes risk documents and associated risk management plans. It also emphasizes the communication of risks and the measures taken to mitigate them. In the context of public procurement of goods and services, risks are monitored: technical; time; cost; and the impacts of phenomena that undermine the transparency and credibility of the supply chain. Organizations of facilities that are associated with critical infrastructure should have a defined risk management structure that includes: chain of powers; communication structure; and governance framework under which risk management and decision-making processes are carried out;
- examples of risks associated with public procurement are: underestimation of need; overestimating the need; insufficient funding to address needs; impractical target dates; failure to carry out a fair procurement procedure; misinterpretation of users' needs; the political or business environment (e.g. changes of direction by senior management or government); likely media interest; a narrow definition or commercial specification (e.g. a specific identified product or brand name and not a general requirement); definition of an unsuitable product or service; distortion of specification; insufficient specification of technical or quality requirements of a "special order" that require suppliers to carry out activities outside of their normal production processes; first-of-its-kind purchases, new items, customized items, or items that haven't been produced for a long time period; and insufficient contract specification or failure to request a statement of work (for services), including the insufficient specification: criteria and methods of inspection; examinations or conditions of admission; computer security measures; packaging; labelling; transport and storage requirements ; and unaddressed harmful impacts on the environment or on the reputation of a nuclear installation;
- risks associated with the procurement scenario: potential gaps in the source are not identified; an inappropriate method is chosen; it is collusion with the supplier; choosing a company that dominates the market; conditions unacceptable to service providers; provision of insufficient information (later questions of interpretation or disputes due to ambiguities or inconsistencies in documentation, requirements or contracts); failure to address service provider queries; actual or perceived favoritism in the provision of information; actual or suspected breach of confidentiality; not requiring an evaluation of quality service providers; failure to comply with effective evaluation procedures; safety or security breaches (e.g., unauthorized access to or disclosure of sensitive business or security matters, information); overlooking the fact that offers don't meet needs; a decision made for subjective reasons; selection of an unsuitable service provider; selection of an unsuitable product; the stalemate over the details of the agreement; failure to ensure binding conditions; unfair or onerous requirements for service providers in the terms and conditions; failure to take into account the terms offered and agreed in the contract; and inadvertently creating a contract without proper approval or for an unsuitable product;
- rights and contract performance risks: price fluctuations and foreign currency exchange; the reluctance of the service provider to accept the contract; lack of contract administration; poor coordination (e.g. delays in handover, poor communication, language or cultural issues); the absence of an effective dispute resolution procedure that causes delays in contractual activities; production pressures or pressures to comply with a schedule leading to non-compliance with the production process or test procedure and schedules; problems with implementing a quality management system at suppliers or a quality assurance program (especially for new or renewed programs); commencement of work by the service provider prior to the exchange of the contract or delivery of the letter of acceptance of the service; an unjustified or unexpected increase in the scope of work; loss of intellectual property; failure to meet third-party obligations (e.g., royalties or third-party property insurance); loss or damage to goods in transit; fraud or other unethical behavior (including delivery of counterfeit or fraudulent items); malicious cyber threats to electronic devices at the retailer's location, during the storage, or during the transportation; lack of

security during the production, including lack of a secure environment for computer development, supplier qualification, and on-site security inspections; disclosure of sensitive information or technology to vendors or subcontractors; key employees are not available (i.e. retirement, transfer to another company, reassignment of the company to another job); unavailability of labor or products (personnel or materials not available when needed, including the inability to fulfill larger orders than usual, incorrectly shipped product, or the impact of possible labor disputes); lack of transparency in supply chains or a significant change in scope, respectively acquisition of purchased items, supplier activities (including the termination of the supplier's activities or its acquisition or merger with another entity); technological failures (product or project does not work, design failure); the supplier is not familiar with the specified design standards (especially when purchasing internationally); the supplier does not have experience with the requirements for the identification of suspicious items, or the customer has not sufficiently specified the requirements for these specific activities; unusual or even normal (i.e. within the expected normal ranges for the location) weather conditions that lead to unplanned activities; unexpected operating conditions; slippages in the performance of subcontracts; poor productivity and performance of subcontractor; damage, theft, or tampering with an item in transit (including hijacking, piracy, or cyber-attacks) or improper storage; overlooking the industrial or radiation safety issues (i.e. procedural accidents, events, or near-miss accidents); improper disposal of waste (environmental impacts, items entering the counterfeit or fraudulent supply chain, and reputational impacts); non-evaluation of public procurement procedures and their management; failure to learn from problems and lessons learned, and failure to take corrective action (both internal and external); misinterpretation of supply chain stakeholder behavior caused by cultural differences; and lack of quality and safety culture;

- a key outcome of any risk management process is a properly compiled and documented risk management plan;
- incentives and penalties are usually not part of industrial contracts, leading to delays in deliveries or a reduction in the quality of items;
- insurance is used as a tool to mitigate risks, which in some cases can lead to a decrease in the quality of items;
- acceptance criteria and acceptance methods at a number of nuclear installations are not established in such a way as to provide assurance that the required technical and quality requirements have been met. Establishing the technical acceptance criteria is an engineering function. The acceptance criteria for an item are: a list of prescribed measurements; and a list of checks or test results that can be objectively verified. Since measurements can never be absolutely accurate, result tolerances must be provided for all criteria. A good rule of thumb is to select at least one acceptance criterion that addresses each safety feature. The established criteria, once verified, should provide reasonable assurance that the item complies with all the technical and quality requirements established at the time of awarding the contract. Factors to consider when developing acceptance criteria include: the possible consequences of the failure of the item for the nuclear safety, security and operability of the installation; the supplier's historical performance in providing items that meet the specified requirements; historical performance of the item in operation; complexity of the design; the complexity of the production or service process; industry experience; the effect that verification of acceptance criteria has on the dependability of item (e.g. the possibility of damage to the item as a result of testing); costs of verifying the acceptance criteria in relation to the increased assurance provided by the verification; access to suppliers' facilities if the item is available in stock or will be manufactured when the order is received; requirements, if the supplier is a manufacturer who has no experience or through an intermediary by a third party; availability of design information; applying the regular supervision and reviews; the ability of the organization’s operational staff to perform post-installation testing; trust in the supplier's documentation; the practicality of carrying out the source verifications; and inspection and ability to test the operation of the organization;
- inspection at source (i.e. material suppliers and manufacturers) is necessary when an item is procurement that is vital (critical) to the safety of the equipment, or is complex in design or manufacture, difficult to test or has difficult-to-verify acceptance criteria upon receipt (post-delivery), or when the supplier management system has not been directly audited. For critical equipment that is assembled far from the location of operating organization, consideration should be given to the establishment of resident supervisory personnel at the factory site during the production of components;
- a trustworthy supplier should have a sufficiently robust nonconformance management system in place that can not only identify but also eliminate counterfeit, fraudulent or suspicious items from the supply chain process in a timely manner. A non-conformance management system is meaningless in itself if the responsible personnel are not sufficiently familiar with its use and continuously trained in its use. Item inspectors must pay attention to receipt when they discover: altered or incomplete markings; overt

attempts to conceal the nature of previous processes; evidence of unauthorized marking (hand-cut characters); deviations in the appearance, packaging method and labelling of the packaging of goods from the same manufacturer; and discrepancies in the documentation or illegibility of some parts of the documentation;

- traceability of items from the manufacturer, through the carrier, through storage, transport to the storage location, installation in a specific facility is important, as is the monitoring of the processes associated with handling, transport and storage, as damage to the item, loss, deterioration or unintentional use must be prevented;
- particular attention must be paid to instruments and control elements (I&C) in procurement. Mainly, it is the acquisition of software and equipment with built-in software or firmware. This is particularly important for instrumentation, control and monitoring devices in electronics and computer technology. Lack of control over the software can: jeopardize the safety or operation of the equipment; interfere with the operation or maintenance of the equipment; allow unauthorized access to critical points or secret documentation; and provide information that could be used for attacks or add additional administrative burdens. Software errors can result either from poor or unclear specification of requirements (which leading to errors in logical design or implementation), or they can arise during the implementation phase or in operation.

4. Principles for reducing the risks associated with fraudulent items

According to the results contained in the documents (IAEA, 2019; Prochazkova, 2017), in order to protect against counterfeit and fraudulent goods, nuclear operators must have safety management programs that include measures aimed at: prevent suspicious and fraudulent items from entering and installing in a nuclear facility; identify, investigate and resolve suspicious and fraudulent items; manage, monitor, and review identified suspicious and fraudulent items; and share information with other potentially affected facilities, regulators, and other industry participants. These four sets of measures must be interlinked.

Based on the findings summarized in (IAEA, 2019; Prochazkova, 2017), the basic principles to mitigate the risk associated with the introduction of suspicious and fraudulent items into nuclear facilities are: establish, validate, and improve safety-enabled programs, processes, and tools; involve the management of the nuclear facility; early identification and intervention to promote safety; effective management, monitoring and controls; documentation and destruction of suspicious items; and information sharing.

Activities related to the procurement of critical items for nuclear installations have a key impact on safety. The proper use of a scaled approach underpinned by risk analysis allows operators to concentrate efforts on critical equipment and ensure that processes in the supply chain cannot adversely affect the safe operation of a nuclear power plant (IAEA, 2019; Prochazkova, 2017).

5. Safety management process in application of commercial items to nuclear facility

According to (Cermak, 2022; EPRI, 1999; IAEA, 2019), ensuring a safe commercial item starts in the procurement process and continues with monitoring its production and transportation, i.e. the safety of the entire supply chain. Quality verification is also important, for a commercial item; it is necessary to verify compliance with the requirements of nuclear facility operator upon acceptance of the commercial item, when it is necessary to verify: the properties of material (composition and structure) from which the item is made; the quality of material processing, including, for example, subsequent heat treatment; robustness of the item; item designation; whether the item's durability meets the requirements; and whether the functionality of the item corresponds to the design requirements of the higher systems in which it works and performs safety-related functions.

Preventing the insertion of counterfeit or suspicious items into a nuclear facility means Process Safety Management (PSM) at the insertion of an item into a nuclear facility when an item is replaced or when it is upgraded. Like any other process, this process is affected by risks that have the potential to reduce safety.

Process Safety is a set of measures and activities that ensure safe protected assets, e.g. in the case of chemical processes, they focus on preventing fires, explosions and leakage of hazardous substances from tanks into the environment. The specific discipline of Process Safety Management has been developing for the last 40 years and its goal is to ensure safe processes that take place in technologies. It is about the management of principles and systems for the identification of possible threats, understanding and mastering the processes leading to the implementation of threats (Prochazkova, 2017). It is advisable to use site-specific checklists and technical tests (EPRI, 2010; IAEA, 2019; USDOE, 2010; USNRC, 1989) for verification.

6. Example of a checklist used by SONS during an inspection

The State Office for Nuclear Safety (SONS) is the central body of the state administration of the Czech Republic, exercising state administration in the use of nuclear energy and ionizing radiation and in the field of non-proliferation of nuclear, chemical and biological weapons. The aim of SÚJB, as an inspection body, is to carry out inspections in order to ensure nuclear safety. In the case under review, this means that items that could endanger nuclear and overall safety cannot get into nuclear facilities. It should be noted that the methodology for ensuring the quality of a commercial item begins when the commercial item is ordered, and that checklists may vary according to the type of local conditions (Prochazkova, 2017). Therefore, "type" checklists cannot be used.

To detect dangerous items, SÚJB inspectors need tools. Therefore, as part of the research (Prochazkova and Prochazka, 2023), with regard to the findings presented in the already cited sources, checklists were compiled for SONS inspections:

- a checklist for identifying risks in a nuclear plant operator's management system;
- a checklist for identifying risks in the procurement of commercial items by a nuclear facility operator;
- a checklist to identify risks in the selection of a supplier of commercial items by a nuclear plant operator;
- a checklist to identify the risks involved in the acquisition of new items by a nuclear facility operator;
- a checklist to identify risks in the monitoring of the supply chain of commercial items by a nuclear plant operator;
- a checklist for identifying risks in the acceptance of commercial items by a nuclear facility operator;
- a checklist for identifying risks in the monitoring of a nuclear facility operator when monitoring the behavior of commercial items after they are inserted into a nuclear facility;
- a checklist for the identification of risks in the system of training of the nuclear operator with regard to the protection of the nuclear facility against hazardous items.

In addition, Table 1 provides a Checklist for assessing whether the management system of a nuclear facility operator has the ability to prevent the introduction of counterfeits into a nuclear installation, which applies to the conditions in the Czech Republic. The checklist in question is based on the findings of the IAEA, OECD, EPRI, US NRC, US DOE and others summarized in the paper (Prochazkova and Prochazka, 2023). The aim is to identify and value partial risks and overall (integral) risk in the management system of a nuclear installation, which reduce the ability of a nuclear facility operator to detect counterfeit and fraudulent items in cases in which it uses commercial items.

Table 1. Checklist to assess whether a nuclear facility operator's system has the ability to prevent counterfeits from being inserted into a nuclear installation. Y -yes, N – No, No-note.

Question	Y	N	No
Does the operator of a nuclear installation have an integrated safety management system of the TQM type (ISO 9000 as amended) and a management system for the entry and acceptance of commercial items incorporated into it?			
Does the operator of a nuclear facility have implemented a tool for monitoring the changes in supply chains - ČSN EN ISO 19 443 (2018)?			
Does the operator of a nuclear facility have an integrated safety management system that respects the principles of nuclear safety and safety culture according to the IAEA?			
Is the operator of a nuclear facility aware of counterfeit and fraudulent items on the market?			
Does the operator of a nuclear facility have procedures in place to prevent counterfeit and fraudulent items from entering the facility?			
Does the nuclear plant operator provide training on counterfeit and fraudulent items to personnel in purchasing, customer audit, acceptance and operation, as well as maintenance personnel associated with the item?			
Does the operator of a nuclear facility involve engineers who are confronted with the equipment, components or services being purchased in training on counterfeit and fraudulent items?			
Does the operator of a nuclear installation have acceptance criteria for the purchase and acceptance of commercial items in order to prevent counterfeit and fraudulent items from entering the facility?			
Does the operator of a nuclear facility require that critical items that may be counterfeit be tested?			
Does the operator of a nuclear installation ensure the protection of its intellectual property when handing over know-how documentation to the supplier?			
Does the nuclear operator prefer to purchase commercial critical items based on the best value rather than the lowest price purchase?			
How often, or on what basis, does the nuclear operator review the procedures for the entry and acceptance of commercial items in the case of critical items?			

Does the nuclear operator have a management system for the entry and acceptance of commercial critical items that is capable of detecting the suspicious or counterfeit items?

Does the nuclear operator have a robust safety culture throughout the facility (i.e. is there openness and transparency in communicating problems and gaining knowledge)?

Does the operator of a nuclear installation have clearly defined critical items that ensure safety at the nuclear facility or contribute to ensuring the safety?

Does the operator of a nuclear installation have clearly defined critical characteristics of the items that ensure safety in the nuclear installation or contribute to the safeguarding the nuclear installation?

Does the operator of a nuclear facility consider the issue of obsolescence when ordering the replacement critical items from commercial entities?

Does the nuclear plant operator have a methodology for verifying the quality of a commercial item?

Does the operator of a nuclear facility have a plan to ensure the replacement of critical items to avoid an emergency on this section when a commercially delivered item is defective?

Does the operator of a nuclear installation have qualified personnel to procure, accept and verify the quality of a commercial item?

Does the nuclear plant operator carry out quality verification of the commercial item upon acceptance on the basis of documentation?

Does the nuclear plant operator carry out quality verification of the commercial item upon acceptance by checking the external characteristics?

Does the nuclear operator verify the quality of the commercial item (mechanical, electrical, digital or software) upon acceptance on the basis of the test results set out in the tender documents?

Does the operator of a nuclear facility have a plan for what to do if serious deficiencies are found during the acceptance of a commercial item?

Does the operator of a nuclear facility have a methodology for controlling the quality (safety) of a safety-related commercial item?

Does the nuclear plant operator have a commercial item acceptance plan that includes requirements for the technical evaluation of the safety-related commercial item?

Does the nuclear plant operator have a plan to monitor the quality of the supplier's performance?

Does the operator of a nuclear facility have experts (persons who know the design, engineering problems, production and functionality of the facility) who procure, adopt and introduce commercial items to the nuclear facility?

Does the nuclear operator have a clear system for the technical evaluation of critical items that guarantees that each item is correctly classified and correctly specified?

Does the nuclear operator have a clear system of responsibilities for the procurement of critical commercial items for the installation?

Does the nuclear facility operator have a robust system for monitoring the production and transportation of critical commercial items for the facility?

Does the operator of a nuclear facility have a clear system for accepting the critical commercial items for the facility?

Does the nuclear facility operator have a clear system for testing the critical commercial items for the facility?

Does the operator of a nuclear facility have a clear system for monitoring the critical commercial items after they are inserted into a nuclear installation?

Does the nuclear operator have a clear system for the return of unacceptable commercial critical items?

Is it clear how the management procedures of the management of items are modified and verified by the operator of the nuclear facility, according to reports of fraudulent and suspicious supplied critical items to the State, IAEA, WANO and others?

Does the operator of a nuclear installation have a clear distinction between design characteristics and critical characteristics?

Note: *Critical properties (selected for acceptance) are typically a subset of the design characteristics and are based on the safety function(s) and complexity of the item*.

Does the operator of a nuclear facility have sufficient insight into testing methods, standards and inspections of critical items?

Does the operator of a nuclear installation have acceptance requirements for both destructive and non-destructive testing of commercial items (method of sampling, size and number of samples, homogeneity of the sample set, documentation requirements)?

Does the operator of a nuclear facility have a say in critical items purchased commercially such as circuit breakers, relays, contactors, motor starters, sensors, etc. A system for specifying and verifying requirements for functionality under normal and abnormal conditions and, where appropriate, critical conditions?

Does the nuclear plant operator have a methodology for performing the non-destructive testing of commercially delivered critical items?

Does the nuclear plant operator have qualified (accurate, reliable and calibrated) equipment to perform non-destructive and acceptance functional tests of the types of items?	
Does the operator of a nuclear installation have verified that, when non-destructive tests and functional tests of commercially supplied critical items are carried out by a contracted organization, that it uses its own measuring equipment that is qualified (accurate, reliable and calibrated) and verified?	
Does the nuclear plant operator have a robust procedure for accepting the critical commercial items and monitoring their insertion behavior into the facility?	
Does the operator of a nuclear installation have a procedure in place if serious defects are discovered during the acceptance of a commercial item (e.g. clerical errors in documents; missing parts of documents, invalid documents e.g. on accreditation...)?	
Does the nuclear operator use the purchase of critical items directly from the producer or does it use middlemen (i.e. the supply chain)?	
Does the operator of a nuclear facility have a policy that addresses the issue of suspicious or counterfeit items?	
Does the operator of a nuclear facility have a system to ensure fairness and ethics in the procurement of commercial items that will eliminate bribery, corruption, deliberate disregard of quality defects, blackmail, etc.?	
Does the operator of a nuclear facility have a system that does not allow dealing with an unethical supplier of commercial items or conflicts of interest?	
Does the nuclear operator have a risk management plan for the procurement of critical commercial items?	
Does the nuclear operator have a risk management plan for receiving the critical commercial items?	
TOTAL	

Table 2. Value scale to determine the level of risk n/N, where n is the number of NO responses and N is the total number of items in Table 1.

Risk rate n/N	Values in **% N**
Extremely high – 5	More than 95%
Very high – 4	70–95 %
High – 3	45–70 %
Medium – 2	25–45 %
Low – 1	5–25 %
Negligible – 0	Less than 5%

If the result of the assessment, i.e. the level of risk, belongs to the following categories:

- 0 and 1, the risk is acceptable and no action is required;
- 2 and 3, the risk is conditionally acceptable and appropriate further corrective action is required;
- 4 and 5, the risk of counterfeits being introduced into a nuclear facility is unacceptable and immediate corrective action is required.

Inspections so far have shown that the operator of nuclear power plants in the Czech Republic (ČEZ) has measures (Volf, 2023), so it is only a matter of increasing safety.

7. Conclusion

Research (Prochazkova and Prochazka, 2023) has shown that fraudulent items can compromise both, the nuclear and the integral safety of nuclear and other important facilities. A critical analysis of the causes of the insertion of hazardous items into nuclear facilities has shown the relevant sources of risk on the part of the plant operator. Therefore, it is necessary to insert into the legislation an obligation for operators:

- improve and implement policies, programs, procedures, processes and practices to: eliminate the risks posed by suspicious and counterfeit items currently in nuclear facilities; prevent any further introduction, installation, or use of suspicious and counterfeit items; ensure that the goods and services supplied meet the specified requirements; ensure the detection, control and reporting of the handling of suspicious and counterfeit items; and provide training and information for managers, supervisors, engineers, and workers on processes and inspections for suspicious and counterfeit items;
- apply the basic principles to prevent the insertion of suspicious and counterfeit items into nuclear facilities, i.e. in practice: if possible, to buy only from authorized (long-term verified) manufacturers and suppliers; to put in place appropriate and effective programs, processes and tools; to involve management in the solution; to involve engineers in (procurement, receipt of items, inspection and testing, maintenance, replacement or modification of equipment); to determine and place technical and quality

assurance requirements in procurement specifications; to indicate processes with acceptability/compliance acceptance criteria (accepting only those items that comply with procurement specifications, consensus standards and generally accepted industry practices); to ensure the timely identification, investigation and disposition of the items in question; to ensure effective management, monitoring and control, documentation, segregation and evaluation of the items concerned; and introduce the obligation to share information and create reports on the items in question.

According to the results of the research (Prochazkova and Prochazka, 2023), it is necessary for the supervision of the safety of nuclear installations in this area to carry out: review the commercial item acquisition proposal; checking the tender documentation for the purchase of a commercial item; inspection of purchased materials, equipment and services; identification and inspection of material, parts and components; inspection of the handling of non-conforming materials, parts or components; and a review of corrective actions and the effectiveness of the programs.

References

Chermak, V. 2022. V. Counterfeit, fraudulent and suspect items (CFSI) also known as suspect/counterfeit items (S/CI). IAEA, Vienna.

EPRI. 1999. Guideline for sampling in the commercial-grade item acceptance process. TR-017218-R1. RPRI, Palo Alto.

EPRI. 2010. Counterfeit and fraudulent items: a self-assessment checklist. EPRI, Palo Alto.

EPRI. 2014. Plant engineering: guideline for the acceptance of commercial-grade items in nuclear safety-related applications. Revision 1 to EPRI NP-5652 and TR-102260. EPRI, Palo Alto.

IAEA. 2016. Procurement engineering and supply chain guidelines in support of operation and maintenance of nuclear facilities. No. NP-T-3.21. IAEA, Vienna.

IAEA. 2019. No. NP-T-3.26. Managing counterfeit and fraudulent items in the nuclear industry. IAEA, Vienna.

Prochazkova, D. 2017. Principles of risk management of complex technological facilities. ČVUT, Praha. Doi: 1014311%2FBK.9788001061824

Prochazkova, D., Prochazka, J. 2022. Good practice connected with identification of suspicious and fraudulent items and protection of their location in nuclear installations. ČVUT, Praha.

Prochazkova, D., Prochazka, J. 2023. Tools for the inspection of a nuclear installation aimed at assessing the quality of its protection against suspicious and fraudulent items in the event of the replacement of components or parts thereof in a nuclear installation. ČVUT, Praha.

Tannenbaum M. 2014. Plant support engineering: counterfeit and fraudulent items mitigating the increasing risk. Revision 1 of 1019163. EPRI. Palo Alto.

US DOE. 2010. DOE G 414.1-3 - Suspect/counterfeit items guide for use with 10 CFR 830 subpart a, quality assurance requirements. US DOE, Washington.

US NRC. 1989. Information notice 89-70, possible indications of misrepresented vendor products. US NRC, Washington.

VOLF, T. 2023. Defending against the risks associated with open technology. In: Řízení rizik procesů, zařízení a složitých technických děl zacílené na bezpečnost 2023. ČVUT, Praha. Doi: 10.14311/BK.9788001072394