WORLD NUCLEAR ASSOCIATION

Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain

Supply Chain Working Group

Title: Countering Counterfeit,
Fraudulent and Suspect Items in the
Nuclear Supply Chain
Produced by: Supply Chain Working Group,
World Nuclear Association
Published: August 2019
Report No. 2019/005

Contents

Executive Summary 1

1. CFSIs and the nuclear supply chain 3

2. The CFSI issue in context 5

3. International Guidance 7

4. Addressing the risk 8

5. Conclusions 12

6. References 13

Executive Summary

There has been growing concern over the possible infiltration of counterfeit, fraudulent and suspect items (CFSIs) into the nuclear supply chain in recent years. This report describes the steps that the world nuclear industry has taken, as well as the market context and known extent of CFSI infiltration. It draws upon a consultation with the World Nuclear Association's Supply Chain Working Group and member companies, including plant operators, reactor vendors, component suppliers and inspection services, on the actions they have put into place over the last five years to address this risk.

Globalized commerce has brought about greater competition to the benefit of customers. But if the rules protecting intellectual property are weak or not enforced then counterfeiters can take advantage of the premium that companies charge for proprietary products and profit from another company's marketing of its own genuine products. No part of the world is free from attempts to defraud customers and all industries have examples of such malpractice.

A small but concerning number of cases of irregularities in the certificates issued by nuclear equipment vendors have come to light in the last few years. In some cases fraudulent test certificates were issued and revealed failings in safety culture and professionalism at established nuclear vendors. Nuclear safety regulators were understandably concerned and halted work while they investigated the circumstances. Installation schedules were at best delayed and sometimes construction projects were halted for several years.

The civil nuclear industry recognizes the potential hazard posed by the infiltration of CFSIs, particularly into nuclear safety systems, and has strengthened procurement, quality assurance, custody arrangements and installation processes where necessary. Of fundamental importance in deterring and uncovering irregular manufacturing and quality control practices is strengthening an organization's safety culture. Several of the examples of fraudulent activity by companies came to light as a result of whistle-blowing to senior management or to regulatory bodies.

Many industries in which product safety is a prime consideration have adopted international quality assurance arrangements. An international quality assurance system for the nuclear sector would be the foremost line of defence against CFSI infiltration. An effective and consistent process of supplier certification across national boundaries would be an important element of such a system.

World Nuclear Association member companies recognize that it is in their interest to reduce the industry's vulnerability to the risk from CFSIs and in recent years have provided training to their staff and to their suppliers on preventing and detecting CFSIs. Training and awareness raising on detecting suspect items and certificates has also been stepped up at third-party certification and inspection bodies.

1 CFSIs and the nuclear supply chain

Over the last decade the infiltration of counterfeit, fraudulent and suspect items (CFSIs) within the global marketplace has become more prominent. During this period, the nuclear industry has given increasing attention to preventing, detecting and correcting the potential hazard posed by the infiltration of CFSIs into the nuclear supply chain, particularly regarding safety systems. Although very few cases where safety was an issue have been discovered, nuclear safety regulators, operators and vendors have adopted robust measures to mitigate this risk.

This report draws upon a consultation with World Nuclear Association's Supply Chain Working Group and member companies, including plant operators, reactor vendors, component suppliers and inspection bodies, on actions they have put into place over the last five years to address this issue.

CFSIs in nuclear applications have been detected in all types of equipment and materials and in inspection, testing and certification services over the last decade[1].

In recognition of the problem, industry and regulators have sought to find a common approach and terminology. The International Atomic Energy Agency (IAEA) has adopted the following definitions[2]:

- Genuine: items produced and certified without intent to deceive.
- Non-conforming (sub-standard): items that do not meet intended requirements or function, and may be provided by legitimate suppliers without intent to deceive.
- Suspect: items where there is an indication or suspicion that they may not be genuine.
- Fraudulent: items that are intentionally misrepresented with intent to deceive, including items provided with incorrect identification, falsified or inaccurate certification. They may also include items sold by entities that have acquired the right to manufacture a specified quantity of an item but produce a larger quantity than authorized and sell the excess as legitimate inventory.
- Counterfeit: items that are intentionally manufactured or refurbished or altered to imitate original products without authorization in order to pass themselves off as genuine.

Kobe Steel admitted in 2017 that 605 customers had been misled as a result of falsification of quality inspection data for aluminium and copper products over the past 50 years. The altered data provided information on the strength and other material properties and aimed to show that the products met customers' specifications. Carmakers and aircraft manufacturers were mainly involved but some products were also supplied to the nuclear power industry, including material for used fuel casks. The falsified data did not pose safety issues.

In South Korea in 2012, eight companies were accused of supplying 60 forged quality control certificates covering 7682 non-safety critical components to Korea Hydro and Nuclear Power (KHNP) since 2002. The affected equipment comprised mainly fuses, switches and cooling fans. Another case discovered in 2013 involved false test certificates for safety-related cabling. One hundred people were indicted in 2013, including some senior management at KHNP. In a parallel case, prosecutors investigated KHNP's procurement functions and uncovered corruption among suppliers, brokers and company personnel.

Over 7500 reactor parts were replaced at nuclear power plants on the orders of the Nuclear Safety and Security Commission at an additional cost of about $90 million. The Korean government and KHNP established and implemented countermeasures in 2013 to prevent a recurrence of corruption at nuclear power plants.

The relationship between these types of item is illustrated in Figure 1.

All non-conformances must be managed within an organization's non-conformance process. Suspect items may prove to be genuine. Counterfeits and fraudulent items are a subset of non-conforming items. Counterfeits, or fakes, by their nature cannot be genuine; however, some frauds may involve genuine items, for example where equipment is supplied with false test certificates.

A South Korean investigation examined hundreds of thousands of documents relating to equipment supplied to operating plants and reactors under construction since 2003. The investigation found 3817 (1.3%) out of 276,000 domestically-issued quality verification documents to be either falsified or non-verifiable, due to non-cooperation from the original supplier or because the supplier had gone out of business. It also found 700 (0.3%) out of 290,000 foreign-issued quality verification documents to be either falsified or non-verifiable. In terms of equipment qualification reports, of the 2699 domestically-issued reports that were investigated, 62 (2.3%) were found to be falsified. None of the 733 foreign-issued equipment qualification reports were found to be falsified or non-verifiable[4].

In the American aircraft industry, where more statistical information is available, only 5% of non-conforming items are counterfeits[5]. The survey of World Nuclear Association member companies in 2018 indicated that there are very few cases of CFSIs detected in a year. It is likely that there is more counterfeiting in the aircraft supply chain than in the nuclear supply chain because the volumes of production are far larger than those in the nuclear sector. The survey also suggested that there has not been a noticeable increase in CFSI cases detected in the nuclear industry over the past five years.

US Department of Transportation and the Federal Bureau of Investigation uncovered a conspiracy to supply fraudulent aircraft parts to the US Air Force and Navy. The owner of The Airborne Group pleaded guilty in April 2010 to supplying parts manufactured by unauthorized suppliers and was sentenced to 30 months of incarceration and ordered to pay $2 million in compensation. The owner of a manufacturing company Zerene Aerospace was sentenced to 37 months of incarceration as was a parts broker and another intermediary, a Federal Aviation Administration-certified repair station owner, who was found guilty of falsifying the authenticity of the parts.

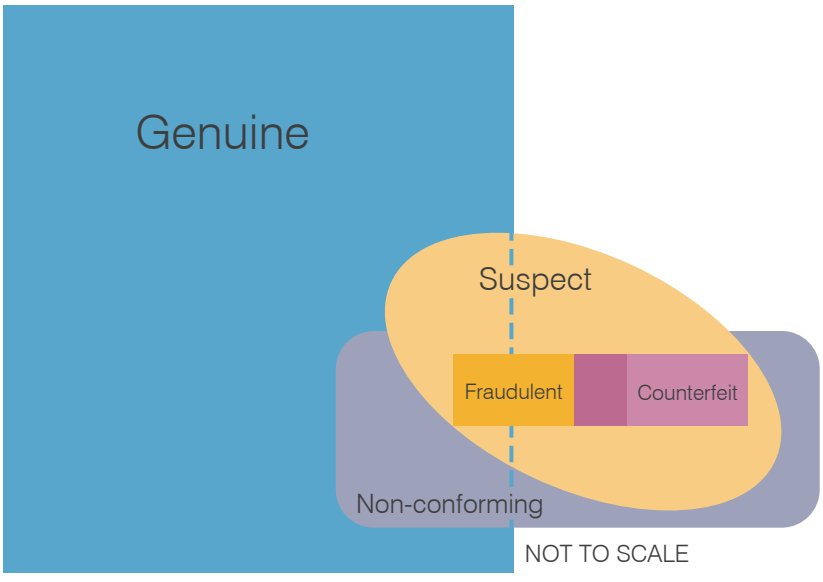

Figure 1: Classification of CFSIs [3]

2 The CFSI issue in context

According to the Organisation for Economic Cooperation and Development (OECD), international trade in counterfeit and pirated goods more than doubled from around $110 billion in 2000 to $250 billion in 2007, and nearly doubled again to reach $465 billion in 2013. While this represents only 2.5% of international trade in goods, it demonstrates a worrying trend[6]. A UK government report states that counterfeiting and piracy "has spread from cottage industries producing poor quality, counterfeit fashion accessories and goods, to massive manufacturing plants that can produce cheap copies of everything from home entertainment products and electrical appliances to medicines, car parts and household goods"[7]. Asian countries account for the largest number of counterfeit and pirated goods exported according to the OECD. Other locations of counterfeiting activity are to be found in Europe and North America, which are also the largest markets for the sale of counterfeits[8].

Attempts to defraud customers occur across the globe and all industries have examples of such malpractice. These cases show that there are a number of common factors that may be involved in attempts to sell CFSIs. These include corrupt procurement practices as well as failures in quality control. Another common element is the use of brokers by customers and suppliers, probably to obscure traceability and disguise bribery under the guise of brokerage fees. However, by no means all cases of CFSIs involve corruption or wrongdoing, as is often the case for intellectual property infringement.

A report by the OECD and European Union Intellectual Property Office (EUIPO) stated: "Gaps in governance, especially high levels of corruption and gaps in intellectual property rights enforcement, are the crucial factor for trade in fakes"[9]. These factors facilitate the supply of CFSIs but poor governance by states does not provide a full explanation.

In 2013 the Irish food safety authority announced that it had found that British and Irish retailers were selling beef adulterated with horsemeat and pork in their own brand ready-made meals. Ten million beef burgers were removed from supermarket shelves in Great Britain and Ireland. Prosecutors in the Netherlands and France uncovered similar cases involving widespread use of brokers.

From an economic perspective one of the key drivers of the supply of CFSIs is the opportunity to take advantage of the premium that companies can charge for proprietary products and to profit from another company's marketing of its own genuine products. Proprietary products can be protected by a registered trademark or brand name, copyright or patent. Counterfeits are items that are imitations of a genuine proprietary product. Fraudulent products may be counterfeits that are misrepresented as genuine products. Fraudulent products may also include an item where a legitimate producer wishes to cover up some non-conformity in production to avoid loss of sales.

Intellectual property (IP) is protected by national laws and the international Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) originally signed in 1994 and amended in 2017. TRIPS provides scope for World Trade Organization member states to decide for themselves on the balance between protecting IP to encourage creativity and innovation, and encouraging competition for the benefit of consumers. Normally the monopoly afforded by a patent or copyright expires after a prescribed number of years. In some countries, the owner of a trademark must apply to renew its registration periodically. A monopoly derived from IP cannot be protected forever.

Variations in national laws and their enforcement thus offer a range of legitimate and illegitimate opportunities for competitor companies to take advantage of good ideas. Reverse engineering, for example, is not necessarily illegal although, clearly, selling a counterfeit product is unlawful. In some sectors, such as automotive, aftermarkets exist to provide items that mimic an original product and which can be used safely and legitimately when the original item has to be replaced. If original equipment manufacturers (OEMs) no longer supply replacement parts because these OEMs are pursuing business strategies using planned obsolescence to encourage customers to update their product regularly, they cannot be surprised if other suppliers step in to fill the gap in the market[10]. Many suppliers of electronic components design obsolescence into their products and as a result a large industry has grown up to recycle still viable electronic components such as integrated circuits. These items may then find their way back into legitimate components and systems but because they have been recycled they will lack a product warranty. It is estimated that 80-90% of counterfeit electronic items have been recycled from legitimate products[11].

Age-related obsolescence, as a result of technical improvement or the exit of an OEM from the marketplace, has also created problems. When a genuine component is no longer manufactured, surplus stocks can be divested to non-franchised distributors who make them available on the so-called grey market. This type of obsolescence poses less opportunity for counterfeiting in the nuclear sector, however, because of the exceptionally long operational timescales at nuclear power plants. After a decade or more since production ceased, replacements have to be manufactured in one-off production runs that are less attractive to counterfeiters[12].

In general, for industries where product safety is important, the problem arises when there is no traceability of the items' provenance and thus there will be an absence of quality assurance. In competitive tendering a specification will often include the words "or equivalent" to permit procurement from a range of suppliers. Not only does this encourage price competition but it offers a benefit in terms of supplier diversity. Like-for-like replacement of components is normally permitted by nuclear safety regulators but obtaining the necessary permission can be a drawn-out and expensive procedure, the costs of which outweigh any price advantage. The key is to ensure that the suppliers of substitutable components are manufacturing to the same standard, with proper traceability and effective customer oversight.

It is likely that custody issues play a role in enabling illicit transfers of shipments at ports and warehouses. A summary brochure of the OECD-EUIPO report cited earlier notes that entrepôts, such as Hong Kong and Singapore, enjoy "great logistics and trade policies, excellent governance, low corruption and respect for IP", yet are "important nodes for the trade in fake goods"[13]. The same report also highlighted the role of free trade zones in counterfeit trade.

Customs fraud has been evolving in complexity and is linked to organized crime, according to the World Customs Organization, even as international customs cooperation has deepened and the use of electronic systems has increased[14]. Groups undertaking customs fraud, such as the mispricing of imports and exports, would have the capability and networks to generate the false documentation necessary for the shipment of counterfeits to markets.

Because counterfeiting is itself a complex activity with its own supply chain, the enterprises involved are frequently part of, or pay protection money to, an organized crime group (although this is not always the case). Such groups are thought to be headed by apparently legitimate business persons (kingpins), who also act as arbiters in disputes involving gang members further down the hierarchy. Their activities therefore involve a mix of legitimate and illegal manufacturing businesses as well as racketeering, money laundering, financial fraud and customs fraud[15].

Shutting down illicit trade routes is clearly a government responsibility but nuclear operators and vendors can reduce the likelihood of CFSI infiltration by relying upon reputable shippers and agents in their business activities.

3 International Guidance

The International Atomic Energy Agency (IAEA) has suggested that nuclear licence holders adopt a number of tools to counter CFSI infiltration[16]. These include:

- Involving the engineering function in procurement and product acceptance, including in the definition of important physical and performance characteristics to be verified at product acceptance.
- Obtaining detailed knowledge of suppliers, including undertaking effective supplier audits and reducing the use of independent distributors and parts brokers.
- Using supplier audit checklists that include questions regarding counterfeit and fraudulent item identification methods and programmes.
- Identifying 'at-risk' procurement scenarios, such as:
  a) Procurement of components that are known to have counterfeits in industry or from locations with a large number of reported issues.
  b) Procurement of items that have long been considered unavailable on the open market.
  c) Use of new suppliers, equipment brokers, independent distributors or Internet exclusive suppliers.
  d) Buying from unauthorized distributors.
  e) Expedited schedules.
  f) Highly discounted pricing.
  g) Supplier refusals to offer a traceable source, or refusals to provide or be accountable for certification.

These scenarios should prompt the customer to undertake a formal supplier risk assessment before purchasing an item.

- Introducing procurement clauses and standard contract language addressing counterfeit and fraudulent items.
- Undertaking thorough receipt inspection.
- Implementing contractual arrangements for independent testing.
- Providing training programmes on recognizing counterfeit parts.
- Following procedures for addressing suspected counterfeit and fraudulent item incidents, which include engagement of original equipment manufacturers.
- Establishing industry databases of CFSI incident data.
- Reporting to regulators of discovered CFSIs.
- Offering whistle-blower protection and rewards.

Many of these recommendations are simply good practice that any customer would undertake to ensure that the right goods and services are procured.

4 Addressing the risk

The nuclear industry has responded to heightened concerns notwithstanding the relatively lower incidence of CFSIs in the sector. Nuclear utilities, technology vendors and original equipment manufacturers (OEMs) have adopted regulatory guidance regarding the risk posed by CFSI infiltration by strengthening procurement, quality assurance, custody arrangements and installation processes where necessary. They have also recognized the links between CFSI vigilance and their organizations' safety culture.

Procurement

Enhanced communication with suppliers is central to preventing CFSI infiltration. As customers, utilities and reactor vendors are obliged to raise awareness of the issue among their suppliers and explain how their product will be used in the nuclear facility. This is much easier in the case of companies that are on a utility's or a reactor vendor's qualified supplier list. Utilities and reactor vendors usually organize dialogue events for their qualified suppliers and these have been the forums to discuss the CFSI problem.

Lower tiers in the supply chain are more likely to have information about the risk of CFSIs as they affect them directly in their corner of the marketplace.

The Electric Power Research Institute has suggested that utility and reactor vendor customers should include in contracts a standard clause requiring suppliers to notify the customer of any exceptions to specification and replace any suspect or counterfeit items discovered by the customer with those specified (see Box)[17]. Not all nuclear power plant operators and reactor vendors include such a clause in their standard terms of contract according to the survey by

Generic Clause for Commercial Nuclear Power Plants[17]

Delivery of suspect/counterfeit items

Seller is hereby notified that the delivery of suspect/counterfeit items is of special concern to (Utility Name). If any items specified in this Order are described using a part or model number, a product description, and/or industry standard referenced in the Order, Seller shall assure that the items supplied by Seller meet all requirements of the latest version of the applicable manufacturer data sheet, description, and/or industry standard unless otherwise specified. If the Seller is not the manufacturer of the goods, the Seller shall make reasonable efforts to assure that the items supplied under this Order are made by the original manufacturer and meet the applicable manufacturer data sheet or industry standard. Should Seller desire to supply an alternate item that may not meet the requirements of this paragraph, Seller shall notify Purchaser of any exceptions and receive Purchaser's written approval prior to shipment of the alternate items to Purchaser.

If suspect/counterfeit items are furnished under this Order or are found in any of the goods delivered hereunder, such items will be dispositioned by (Utility Name) and/or the original manufacturer, and may be returned to the Seller in accordance with the warranty provisions applicable to the Order. The Seller shall promptly replace such suspect/counterfeit items with items meeting the requirements of the Order. In the event that the Seller knowingly supplied suspect/counterfeit items, the Seller shall be liable for reasonable costs incurred by the Purchaser for the removal, replacement, and reinstallation of said goods in accordance with the warranty provisions applicable to the Order.

the World Nuclear Association due to jurisdictional factors. For example, in many countries, state-owned enterprises are required to use a standard set of contract conditions in their purchasing activities and these companies are not free to change these terms.

In addition to the recommended procurement clause, some customers draw the attention of their suppliers to the potential sanctions under criminal law that could be applied in cases where deliberate fraud is suspected.

Products may be divided into two types: differentiated products and commodities. OEMs supply differentiated products made to their own design with a defined brand name. They have a direct interest in halting counterfeiting activity and helping their customers to avoid purchasing equipment, components and parts from unauthorized dealers and brokers. They rely on their customers for repeat business but aggressive procurement practices may get in the way of maintaining an established long-term relationship. As noted already, the line between an authorized substitute and a cheaper illegitimate copy may be a blurred one due to variance in the way IP is treated in different jurisdictions. Globalized commerce has brought about more intense competition to the benefit of customers. But if the rules protecting IP are weak or not enforced then quality assurance is sacrificed in the name of price. Counterfeiters will actively evade quality controls in order to escape detection.

Procurement of commodities creates different issues. Commodities have a high degree of substitutability (or fungibility). Materials and other primary products are an obvious example, but many other standardized goods can also be considered to be commodities, such as steel products. Customers often buy a commodity from an intermediary, such as a broker, distributor or agent, where there can be less traceability back to the originator. Lower tier suppliers tend to manufacture or assemble sub-components from commodities, which carries a greater risk of CFSI infiltration unless there is good traceability, quality control and secure custody.

Furthermore, when a good idea has diffused around the world and the original IP is no longer protected, then a differentiated product becomes a commodity. This is a predictable outcome of growing international trade and investment that is well underway. The increasing volume of CFSIs in world trade, especially in electronic goods, is an aspect of globalization.

Quality Assurance

A global supply chain without consistent quality assurance across countries increases the risk of CFSI infiltration. The nuclear industry has developed standards for quality management that aim to prevent the infiltration of CFSIs and these procedures have been strengthened at reactor vendors and nuclear power plant operators in recent years (see Box).

Quality Assurance Procedures

Requirement 8: *Identification and Control of Items* in the nuclear industry quality management system standard ASME's NQA-1: 2015 [18] states: Controls shall be established to assure that only correct and accepted items are used or installed.

Section 705 on Determining Authenticity in Subpart 3.1-7.1: *Implementing Guidance for Part I, Requirement 7: Control of Purchased Items and Services* of NQA-1: 2015 outlines "measures to ensure products are authentic and reduce the risk of introducing counterfeit or fraudulent items." These include:

- Procedures for detection and prevention.
- Providing inspection staff with information on incidents that have been received or experienced by others.
- Purchasing directly from the manufacturer or authorized distributor or confirmation from the manufacturer.
- Inspection upon receipt of items for signs of potential counterfeiting or fraud.

In the newer ISO 19443: 2018 standard[19], the equivalent clauses are as follows:

8.1.1 Provisions for Counterfeit, Fraudulent or Suspect (CFS) items

The organization shall prevent CFS items at all levels of operations including:

- Selection of external providers.
- Specific information to external providers, including requirements for control of their sub tier providers.
- Control of externally provided processes, products and services.
- Monitoring and measurement activities.

When CFS items are detected, they shall be managed as nonconformities and relevant parties, including the customer, shall be informed without delay.

ISO 19443 provides definitions of CFSIs that are practically identical to those given by the IAEA.

During 2016, AREVA (now Framatome) undertook a review of irregularities in the paperwork on some 400 components manufactured at Creusot Forge in France. Some dated back to 1965, when the facility was owned by Schneider Electric. Tests had not been performed or recorded correctly and there had been quality assurance failures. Irregular practices had continued after 2006 when AREVA purchased the facility and were not identified until 2015. After discovery, EDF analysed all discrepancies and the components affected were in due course cleared for continued use by the French nuclear safety authority.

US nuclear operator Exelon Corporation established the Parts Quality Initiative (PQI) in 2006 as a preventative measure to improve equipment reliability. Before parts are issued to a nuclear power plant for installation, the company performs pre-receipt inspections and testing of the inbound parts at its testing laboratories. Only those parts that pass the PQI requirements make it to inventory. Parts that are rejected are returned to the supplier for replacement under the supplier's warranty. Since its inception, PQI has tested more than 27,000 parts and prevented over 2000 (7%) deficient parts from being stocked in advance of scheduled maintenance. It has significantly reduced the number of equipment failures. All PQI data for the Exelon fleet is held in a central database, which enables Exelon's nuclear fleet, and the American nuclear industry as a whole, to identify key performance indicators and trend reliability issues due to specific parts and/or manufacturing deficiencies[20].

Quality assurance requirements such as those developed by ASME and ISO cover every step of product realization and delivery. Suppliers of items important for safety must either hold a recognized certificate or be subject to equivalent oversight by their customer. Ensuring the appropriate level of quality management through the supply chain is more straightforward if all the companies involved are working to the same or similar standards, which calls for an industry-wide approach.

Inspection procedures during production and on delivery to the customer offer an opportunity to verify that the product conforms to requirements and that the accompanying documentation is authentic. Customers should follow up suspected cases with the original supplier to check that product documentation was actually issued by the supplier concerned.

Customers have strengthened their controls at the point of receipt. In addition to checking that the goods and accompanying paperwork match the specification, some nuclear power plant operators carry out further testing at their premises to assure conformity.

Many industries where product safety is a prime consideration have adopted international quality assurance arrangements. The civil nuclear industry has been a late starter because of its strong domestic focus and nationally-based regulatory environment. An international quality assurance system for the nuclear sector would be the foremost line of defence against CFSI infiltration. An effective and consistent process of supplier certification across national boundaries is an important element of such a system.

Custody

Maintaining secure custody of components and systems while they are transferred between companies during manufacturing and transport is crucial. It is clear from CFSI cases that illicit substitution occurs where custody arrangements are insecure. Vulnerabilities exist at the point of trans-shipment or warehousing where intermediary agents are involved and these vulnerabilities can be exploited by organized crime groups to create a false paper trail.

Nevertheless, World Nuclear Association members have not found any CFSI cases where custody arrangements were a factor.

Installation

Ensuring that only genuine parts and components are incorporated or installed is the last line of defence against CFSI infiltration, which depends on the experience and knowledge of the workers involved. In many cases, installation of replacement equipment and parts is carried out by contracted personnel at licenced nuclear facilities, while maintenance is undertaken by direct employees. In the US aircraft industry, the largest source of reports on suspected unapproved parts are repair stations and mechanics, rather than suppliers or airlines[21]. Installation personnel should be empowered through training and authority to report suspicions even if this means holding up the work they are engaged on.

Reporting systems and databases

A number of industry associations in North America and Europe have established reporting systems and databases to keep track of CFSI incidents, primarily in the electronics sector. The Electric Power Research Institute (EPRI) set up a database of CFSI events in 2011, which is accessible to its members (which are mainly electricity utilities but also include government agencies). The US Department of Energy has a process for identifying

unintentionally defective items and suspect/counterfeit items deemed safety-significant at its facilities and for communicating information to its contractors. Information on counterfeits is also available under the Canadian-US Government-Industry Data Exchange Program, a joint activity that provides access to sensitive information gathered by government agencies as well as contractors. The Russian Federal Anti-Monopoly Service manages a registry of unscrupulous suppliers and such suppliers can be excluded from bidding for public tenders for up to three years.

Nuclear safety regulators are working together to share information on non-conformances or irregularities, where items are discovered to not meet purchase or design specifications or their intended function. An irregularity should prompt the licensee of the nuclear facility to evaluate the instance as a possible CFSI. The OECD-Nuclear Energy Agency has established a reporting and dissemination protocol between nuclear safety regulatory bodies at the detection stage and after investigation to establish whether the event has safety significance. This activity is aimed at assisting nuclear safety regulatory bodies to keep track of incidents and it is then up to each of these national bodies to communicate relevant information to its domestic industry. Although not all countries with civil nuclear facilities are members of the Nuclear Energy Agency, its recently-created database is the only international one at the present time.

Safety culture

An organization's culture and procedures help shape the behaviour of personnel, including personnel hired through other parties. Problems can arise if the organization's corporate culture or an individual's ethics come into conflict with the commitment to safety. The tendency to cover up mistakes is common to both organizations and individuals.

In its guide on Leadership and Management for Safety, the IAEA states that managers at all levels should foster a strong safety culture, encourage the reporting of safety-related problems and develop questioning and learning attitudes within their organization. Managers have a personal responsibility to ensure that they take action to "correct acts or conditions that are adverse for safety"[22].

World Nuclear Association member companies have provided training to their staff and to their suppliers on preventing and detecting CFSIs in recent years. Training and awareness raising on detecting suspect items and certificates has also been stepped up at third-party certification and inspection bodies.

The IAEA also recommends that regulatory bodies "shall review and assess relevant information — whether submitted by the authorized party or the vendor, compiled by the regulatory body, or obtained from elsewhere — to determine whether facilities and activities comply with regulatory requirements and the conditions specified in the authorization". The regulator should also "exercise its authority to intervene in connection with any facilities or activities that present significant radiation risks"[23]. These two requirements imply that a tip-off from a whistle-blower that has nuclear safety implications should be investigated even if provided anonymously, as should media reports of corporate wrongdoing. Several of the examples of fraudulent activity by companies came to light as a result of whistle blowing to senior management or to regulatory bodies.

In 2012 the owner and president of Pentas Controls, pleaded guilty at an Arizona court to making false statements to the US Nuclear Regulatory Commission (NRC). Pentas had replaced a broken display on a steam leak detector monitor for a nuclear power plant with another one and had filed down the serial number to disguise the switch. The owner was put on probation for five years and required to fulfil NRC stipulated quality management and safety culture improvements at his company.

Volkswagen (VW) admitted in 2015 that it cheated diesel emission tests by installing software that allowed its vehicles to meet US and European clean air standards under testing but did not operate under normal driving conditions. Nitrogen oxide (NOx) emissions worsen respiratory diseases and contribute to acid rain. VW pleaded guilty to a US court for cheating NOx emission tests and lying to regulators. Reported fines and penalties were in excess of €27 billion.

5 Conclusions

Counterfeiting and commercial fraud are global problems that require a coordinated response from enterprises and governments. Poor governance by states facilitates the supply of CFSIs but part of the problem lies in the nature of a global economy and variable protection of IP between jurisdictions. No part of the world is free from attempts to defraud customers and all industries have examples of such malpractice. Rooting out counterfeiting and commercial fraud is made more difficult by their links to organized crime groups, many of which operate transnationally. CFSI infiltration represents a particular risk in operations where a high level of safety is demanded but also because the economic impact and reputational damage can be significant.

The extent of CFSI infiltration in the nuclear industry is relatively small and there has been no noticeable increase in cases detected at nuclear power plants over the past five years. Very few of these cases posed any risk to safety.

The civil nuclear industry recognizes the potential hazard posed by the infiltration of CFSIs, particularly into nuclear safety systems, and has strengthened procurement, quality assurance, custody arrangements and installation processes where necessary. Of fundamental importance in deterring and uncovering irregular manufacturing and quality control practices is strengthening an organization's safety culture.

Nuclear safety regulatory bodies are working closely through the OECD-Nuclear Energy Agency to keep track of CFSI incidents and to collect reports of such incidents and the results of national investigations. There could be further consultation with nuclear facility operators and reactor vendors around the collection of CFSI data in order to generate better analysis and intelligence by both enforcement agencies and companies.

World Nuclear Association member companies recognize that it is in their interest to reduce the industry's vulnerability to the risk from CFSIs and in recent years have provided training to their staff and to their suppliers on preventing and detecting CFSIs. Training and awareness raising on detecting suspect items and certificates has also been stepped up at third-party certification and inspection bodies.

6 References

[1] *Procurement Engineering and Supply Chain Guidelines in Support of Operation and Maintenance of Nuclear Facilities*, International Atomic Energy Agency, NP-T-3.21, pp. 128, 132, 133-153 (September 2016)

[2] *Ibid*. p. 128

[3] Figure adapted from IAEA NP-T-3.21 (*ibid*.) p. 127

[4] Walter Kim, Korea Institute of Nuclear Safety, *Regulatory Actions and Follow-suit Measures Against the Korean NPPs' CFSI Issues*, presented at Nuclear Supply Chain Management Workshop organised by the OECD Nuclear Energy Agency and held in Boulogne-Billancourt, France on 5-6 November 2018

[5] See analysis of US Federal Aviation Administration data cited by Roy Resto in *CAVU Café: Royboy's Prose & Cons*, Aviation Suppliers Association website (4 August 2017)

[6] *Magnitude of counterfeiting and piracy of tangible products: An update*, Organisation for Economic Co-operation and Development (November 2009)

[7] *Supply Chain Toolkit*, National Intellectual Property (IP) Crime Group, p. 5 (11 July 2014)

[8] Ernesto U. Savona and Michele Riccardi (eds.), *From Illegal Markets to Legitimate Businesses: the Portfolio of Organised Crime in Europe*, Final Report of Project OCP – Organised Crime Portfolio, Trento: Transcrime – Università degli Studi di Trento, p. 69 (2015)

[9] *Why Do Countries Export Fakes? The Role of Governance Frameworks, Enforcement and Socio-economic Factors*, Organisation for Economic Co-operation and Development (OECD) and European Union Intellectual Property Office (EUIPO) (2018), and summary brochure

[10] An obsolescent product is one that is unfashionable or no longer usable; see Tim Hindle, *The Economist Guide to Management Ideas and Gurus*, Profile Books (2008)

[11] IAEA NP-T-3.21 (*op. cit*.) p. 132

[12] *Plant Support Engineering: Counterfeit and Fraudulent Items – Mitigating the Increasing Risk*, Revision 1 of 1019163, Electric Power Research Institute, p. 5-5 (July 2014)

[13] OECD-EUIPO 2018 (*op. cit*.) p. 15 of summary brochure

[14] Michel Danet, *International Customs Day 2005*, World Customs Organization

[15] Glenn E. Curtis *et al*, 2003, *Transnational Activities of Chinese Crime Organizations*, A Report Prepared by the Federal Research Division, Library of Congress under an Interagency Agreement with the Crime and Narcotics Center, Directorate of Central Intelligence, pp. 1-3 (April 2003); Roderic Broadhurst and Lee King Wa, *The Transformation of Triad 'Dark Societies' in Hong Kong: The Impact of Law Enforcement, Socio-Economic and Political Change*, Security Challenges, Vol. 5, No. 4, pp. 1-38 (Summer 2009)

[16] IAEA NP-T-3.21 (*op. cit.*) pp. 154-164

[17] EPRI Rev. 1 of 1019163 (*op. cit.*) p. B-1

[18] ASME NQA-1 – 2015, *Quality Assurance Requirements for Nuclear Facility Applications*, The American Society of Mechanical Engineers (2015)

[19] ISO 19443:2018, *Quality management systems – Specific requirements for the application of ISO 9001:2015 by organizations in the supply chain of the nuclear energy sector supplying products and services important to nuclear safety* (ITNS), International Organization for Standardization (May 2018)

[20] *Exelon's Entry for Parts Quality Initiative wins NEI TIP Award!*, Exelon PowerLabs website (2018)

[21] See Roy Pesto 2017 (*op. cit.*)

[22] *Leadership and Management for Safety*, General Safety Requirements Part 2, International Atomic Energy Agency, pp. 7-8 (June 2016)

[23] *Governmental, Legal and Regulatory Framework for Safety*, General Safety Requirements Part 1, International Atomic Energy Agency, pp. 20, 27 (September 2010)

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain by the World Nuclear Association's Supply Chain Working Group describes the steps the nuclear industry has taken to address the risk of infiltration from fakes and other non-conforming parts and components.

A small but concerning number of cases of irregularities in the test certificates issued by nuclear equipment vendors have come to light in the last few years. Other cases discovered involved the supply of counterfeit goods. Globalized commerce has brought many benefits but if the rules protecting intellectual property are weak or inadequately enforced then counterfeiters can take advantage of the situation to defraud customers. The extent of such infiltration into the nuclear supply chain remains relatively small according to the most recent information. Nevertheless, nuclear operators and their suppliers recognize the potential hazard involved and apply rigorous quality assurance processes, undertake supplier awareness programs, and train their staff to detect and prevent the installation of counterfeit, fraudulent and suspect items.

World Nuclear Association is the international organization supporting the people, technology and enterprises that comprise the global nuclear energy industry.

Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain