CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

Securing the Nuclear Supply Chain:

A Handbook of Case Studies on Counterfeit, Fraudulent and Suspect Items

Professor Christopher Hobbs, Zoha Naser,
Dr Daniel Salisbury and Dr Sarah Tzinieris.

2024

About the Centre for Science & Security Studies

The Centre for Science & Security Studies (CSSS) is a research centre in the Department of War Studies at King's College London. Created by a grant from the John D. and Catherine T. MacArthur Foundation in 2003, CSSS brings together a multidisciplinary team of scientists and social scientists with backgrounds in physics, nuclear engineering, international relations, politics and history, among other disciplines. Members of the centre conduct academic and policy-relevant research on nuclear non-proliferation, nuclear disarmament, arms control, verification, open-source intelligence, space security and mass effect terrorism, including the chemical, biological, radiological and nuclear (CBRN) dimension.

Acknowledgements

The authors are grateful to the International Atomic Energy Agency (IAEA) for sponsoring the production of the report. The authors are also grateful for the support provided by the Professional Services staff at King's.

Compiled by Professor Christopher Hobbs, Zoha Naser, Dr Daniel Salisbury and Dr Sarah Tzinieris.

Published by King's College London in the Centre for Science & Security Studies.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS

Hobbs, C., Naser, Z., Salisbury, D. and Tzinieris, S. (2024) 'Securing the Nuclear Supply Chain: A Handbook of Case Studies on Counterfeit, Fraudulent and Suspect Items'. London: King's College London.

ISBN: 978-1-908951-52-6
https://doi.org/10.18742/pub01-164

Contents

Foreword

This document, *Securing the Nuclear Supply Chain: A Handbook of Case Studies on Counterfeit, Fraudulent and Suspect Items*, is the product of a nine-month period of desktop and investigatory research. It was funded through an International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP). It is envisaged that this guide on CFSIs, utilising real-life case studies, will be a valuable source for governments, industry and others around the world to help prevent CFSIs, or at least mitigate their effects, within the nuclear supply chain.

Compiled by researchers and academics at King's College London, the objective is to provide comprehensive, evidence-based and objective information about CFSIs and the implications for nuclear security. Through probing a number of case studies, the handbook explores known cases of CFSIs found in the nuclear supply chain where there are particular nuclear security aspects identified or if the events can be extrapolated logically to demonstrate nuclear security risks. In addition, the handbook provides policy recommendations to the IAEA and its Member States for preventing the entry of CFSIs into the nuclear supply chain, mitigating the risks and consequences of their presence, and facilitating their detection and removal.

Glossary

AIASN	Nuclear Safety Authority (France)
APU	Auxiliary power unit
BNFL	British Nuclear Fuels Plc
CFSIs	Counterfeit, fraudulent and suspect items
Covid-19	Coronavirus disease 2019
DOE	Department of Energy (United States of America)
EDF	Électricité de France
EDG	Emergency diesel generator
EPRI	Electric Power Research Institute
EU	European Union
EUIPO	European Union Intellectual Property Office
EUROPOL	European Union Agency for Law Enforcement Cooperation
FTZ	Free trade zone
IAEA	International Atomic Energy Agency
ISO	International Organization for Standardisation
KEPCO	Korea Electric Power Company Ltd.
KHNP	Korea Hydroelectrical and Nuclear Power Company
LOCA	Loss of coolant accident
LOOP	Loss of onsite power
LWR	Light water reactor
MOX	Mixed oxide (fuel)
NII	Nuclear Installations Inspectorate (United Kingdom; merged into the ONR)
NRA	Nuclear Regulation Authority (Japan)
NRC	Nuclear Regulatory Commission (United States of America)
NSSC	Nuclear Safety and Security Commission (Republic of Korea)
CPPNM	Convention on the Physical Protection of Nuclear Material
OECD	Organisation for Economic Co-operation and Development
OEM	Original equipment manufacturer
ONR	Office for Nuclear Regulation (United Kingdom)
OSINT	Open-source intelligence
TEPCO	Tokyo Electric Power Company
UN	United Nations
WANO	World Association of Nuclear Operators
WNA	World Nuclear Association

Executive Summary

The issue of counterfeit, fraudulent and suspect items (CFSIs) is a persistent and growing problem worldwide. According to a 2023 study by the Organisation for Economic Co-operation and Development (OECD), trade in counterfeit and pirated goods counts for around 2.5% of world trade.[1] Counterfeit and fraudulent items do not undergo rigorous quality assurance procedures, as legitimate items do, and deviate from prescribed specifications. As such they can pose immediate and extended threats to work safety, security and operations at industrial facilities, the impact of which may extend beyond these boundaries.[2] This is particularly relevant in the nuclear sector, where the undermining of key systems by CFSIs could lead to potential radiation release, impacting on human health and the environment. Even if detected, removed and replaced before a negative event, CFSIs may lead to a temporary suspension of operations, driving up the costs of doing business.

The inadvertent or malicious insertion of CFSIs into the nuclear supply chain can diminish the integrity of a wide range of equipment, systems, structures, components, or devices, with risks to nuclear security and safety. As a result of past incidents, the nuclear industry is increasingly aware of the need to develop measures both to mitigate the impact of CFSIs that have infiltrated the nuclear supply chain, and to prevent their introduction altogether.[3] However, this is a challenging endeavour which requires robust procurement procedures, with checks and balances that go beyond the manufacturer or supplier, through the extended supply chain.

The authors adopt the definition of 'nuclear security' applied by the International Atomic Energy Agency (IAEA):

'The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities'.[4]

Part One of this handbook provides an introduction to the issue of CFSIs, explaining what they are and how they may infiltrate the nuclear supply chain. It also discusses the impact that CFSIs can have on nuclear safety and security, and how an integrated approach to these issues can help tackle counterfeits in the nuclear sector. This section ends with an overview of existing guidance, legislation and key initiatives related to CFSIs at the operational, national and international levels, shedding light on what has been done so far and the gaps that need to be addressed.

Part Two of the handbook delves further into the actors, goods and geographical regions where CFSIs are most common. This involves a discussion of the types of products and services that are vulnerable to counterfeiting, including nuclear-relevant items, safety and security products and a wide variety of electronics. This section also conceptualises the multiple threat actors involved in the process at all stages of the supply chain and discusses, among other things, the factors shaping CFSI network behaviour, the different means of deception that actors use, and the type of counterfeiting methods they employ. The geographies and regions where counterfeiting is most prevalent, are also explored, with a focus on how free-trade zones (FTZs) and particular jurisdictions can help enable CFSI networks.

Part Three explores a series of detailed case studies of actual CFSI incidents from nuclear and non-nuclear industries, highlighting the different ways that counterfeits have made their way into critical infrastructure (with a focus on transport, aerospace and defence). As the majority of cases currently available in the public domain are safety-related, this handbook also explores the potential security-related implications of these incidents. These include the infiltration of fraudulent construction materials, safety equipment with illegitimate quality assurance certificates, and manufacturers falsifying records to sell substandard parts. The cases presented in this part of the handbook illustrate the key findings discussed in the previous sections.

The handbook concludes by providing a series of practical recommendations based on the case studies and evidence analysed earlier. The advice provided seeks to be relevant to stakeholders across the industry, including at both the domestic and international levels.

Key findings from the research presented in the handbook are summarised briefly below:

CFSIs pose a significant threat to both nuclear safety and security. Fraudulent parts and services can diminish the integrity of key equipment and infrastructure at a nuclear facility, putting operations at risk. In addition, the synergy between these two key concepts mean that counterfeits installed in safety infrastructure can have security implications, and vice versa. The complexity of nuclear facilities means that a counterfeit part, no matter how seemingly small or insignificant, could create a potential issue.

Counterfeits can infiltrate the nuclear supply chain in various ways, be it at the initial manufacturing level, by traders or by the final customer. The ability of counterfeits to permeate the supply chain in this way can make them harder to detect, highlighting the need for vigilance from stakeholders at all stages of the supply chain. Different actors involved in the supply of CFSIs may also use different methods in accordance with their capabilities, locations, and motivations.

Historical incidents have proven that despite efforts to mitigate the risk of CFSIs, certain organisations can still be vulnerable to this threat. There are a number of reasons for this, including weak organisational culture, poor procurement methods, and weak or limited training on CFSI risks. These factors have been observed in the case studies as significantly contributing to the infiltration of CFSIs.

New technologies can create additional opportunity for CFSI infiltration, but also new methods to help identify them. New technological services, like online communication services and online marketplaces, can help counterfeiters more effectively falsify their parts, sell them undetected, and reach a larger global audience. On the other hand, new technologies and scientific methods can help better detect CFSIs through means such as destructive and non-destructive testing.

References

1 OECD and EUIPO, 'Illicit Trade: Risks of Illicit Trade in Counterfeits to Small and Medium-Sized Firms', 2023. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Risks_of_Illicit_Trade_in_Counterfeits_to_SMEs/Risks_of_Illicit_Trade_in_Counterfeits_to_SMEs_FullR_en.pdf

2 International Atomic Energy Association, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

3 For further information, see: https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

Part I
Introduction to CFSIs in the Nuclear Sector


TARE WGT.

1. Research Approach

This handbook uses a series of case studies to investigate the presence of counterfeit, fraudulent, and suspect items (CFSIs) within the nuclear supply chain, including the safety and security impacts of such events. It also utilises case studies from other critical national infrastructure[1] to learn lessons from other sectors, and to determine whether any of the knowledge gained from these incidents can be transferred and can shed light on CFSIs in the nuclear industry. Examples of the critical infrastructure sectors explored in this book include the defence, aerospace and transport sectors.

The case studies have been collated through the use of open-source information and are derived from a wide range of publicly available sources. These include using online databases, government archives, news reports, and legal documents, including court proceedings. Here it should be noted that due to the sensitive nature of nuclear operations and facilities, disclosure of information on CFSIs is often limited and, consequently, open sources may not be able to bridge all gaps in knowledge. However, combining government statements with news reports, database records, testimonies and other information available can help fill certain contextual gaps and create better conceptualisation of the issue. The approach taken in this handbook is to collect information that is already available but scattered across the public sphere, and transforms it into coherent, digestible information in a single document that is accessible to a wider audience.[2]

The use of case studies is an important pedagogical tool in helping readers critically engage and better understand the issue of CFSIs. Case study usage builds on the theory of the 'Learning Paradigm' developed by Robert Barr and John Tagg in 1995.[3] This theory puts students at the centre of teaching, and emphasises the importance of critical thinking, problem solving, and helping students make new discoveries. Case studies help bridge the gap between theoretical topics and real-life events, helping readers ground the knowledge they gain in practical and clear examples. This method also encourages readers to critically engage with the events of the case, with lessons that could be drawn from the incident and applied to other occasions. For an issue like CFSIs, which is a persistent threat, but relatively unexplored area of research, case studies help readers conceptualise CFSIs in a more informed and nuanced manner and demonstrate the true extent of the issue.

2. Understanding CFSIs

2.1. What Are CFSIs?

Unlike legitimate items, counterfeit goods do not undergo rigorous quality assurance procedures and deviate from prescribed specifications, making them unreliable and potentially defective. Counterfeit and fraudulent items are present in almost every commercial and industrial sector, including fashion, electronic appliances and car parts. In critical infrastructure sectors, the use of these items is particularly worrying as they potentially could have a severe impact on an industrial plant and its performance, workers and their health, the environment, and even the general public.

It is important to be vigilant about counterfeit and fraudulent items at all stages of the manufacturing process. They are not just a concern as the final itemised product, but also at earlier stages of assembly and production. This includes a wide variety of goods, from raw materials and chemicals to mechanical and electronic components. Seemingly legitimate items purchased from manufacturers could be made up of counterfeit or fraudulent components and materials that were introduced earlier in the supply chain.

Terminology around counterfeit and fraudulent items has not been standardised across different sectors. Given the focus here on the nuclear sector this publication makes use of a series of definitions from guidance published by the International Atomic Energy Agency (IAEA)[4] and the Organisation for Economic Co-Operation and Development (OECD)[5] to establish the following terms:

- **Counterfeit:** Items or goods that are intentionally altered, created or restored to imitate original products, without legal authorisation.
- **Fraudulent:** Items or goods that are intentionally misrepresented to be something they are not. In industry, fraudulent products are often those with incorrect identification or falsified certification.
- **Suspect:** Items or goods that are suspected to be non-genuine, or to meet certain standards, specifications, or technical requirements. There is often indication of this via methods like visual inspection, testing or other disclosed information. These items could be knowingly or unknowingly counterfeit or fraudulent and require further investigation from relevant stakeholders, including operators and authorities.

Collectively we refer to these terms as counterfeit fraudulent and suspect items (CFSIs) in this handbook. While there appears to be some overlap between counterfeiting and fraudulent items, industry papers tend to focus on physical features of an item in 'counterfeiting', and falsified information or certification when discussing 'fraudulent' goods. In a security context, the crucial difference between CFSIs and non-conforming or substandard items is that CFSIs are produced with the intention to deceive.

2.2. Why Do CFSIs Pose a Risk?

CFSIs can be found in various sectors and commercial environments, but they present a particular risk in critical industries like the nuclear sector.

CFSIs could contribute to the negative performance of the nuclear power plant (NPP), impacting facility costs and financial gain. The use of a fraudulent item could not only produce costly damage to the NPP and equipment itself, but also could mean the plant has to shut down operations to replace the fraudulent item. This impacts the economic output of the facility and is likely to be very damaging in terms of productivity. A range of stakeholders in these industries stand to lose profit, as delays to replace CFSIs and potential reputational costs could impact the wider industry.

Where there are safety implications of CFSIs, workers could potentially lose their jobs or even risk their lives. For example, unsafe scaffolding may lead to workplace accidents while defective bolts on a steam pipe may lead to scalds and burns. Additionally, if a NPP is shut down to be replaced for fraudulent and counterfeited parts, contractors could be at risk of losing paid work, especially if the plant does not reopen for a significant period of time.

In particularly serious cases, the use of CFSIs in industry could even have a detrimental impact on the environment and general public. In the nuclear industry, the operating system is incredibly complex and defective parts could potentially start a catastrophic chain reaction, leaving room for potential incidents and even serious accidents that might lead to a radiological release. For example, faulty items in the system could lead to failure of a critical aspects like the coolant system of a reactor or fire safety systems.

2.3. How Do CFSIs Infiltrate Supply Chains?

There are multiple reasons for the introduction of CFSIs into the nuclear supply chain. The initial driver behind the manufacture of CFSIs is often where producing fraudulent goods provides significant financial benefit for the supplier. Trademarked, genuine products are often sold at a premium by manufacturers who have a reputation behind their brand and a legal right, such as a copyright or trademark, to protect it. CFSIs are imitations or fraudulent items that suppliers wish to sell with the benefit of being associated with the genuine, registered brand. By producing counterfeit or fraudulent goods under the name of the original brand, they can charge similar prices for a product that is not up to the same standards or quality as the original.[6]

Industry may then unwittingly purchase CFSIs for a variety of reasons. For example, an urgent replacement of a key component to the system may be required, but no immediate part is available from the original manufacturer. This is a particularly pressing issue in industries like the nuclear sector, where products have long life cycles and need to be frequently updated and replaced with specific components and parts to keep them operational. This may result in industry purchasing an item from an unknown supplier or broader marketplace, which turns out to be a CFSI.

Other explanations for the use of CFSIs include:[7]

- The goods are difficult to verify or not usually verified
- Technical specifications and procurement requirements are not defined properly
- Verification mechanisms are inadequate
- The qualifications of the supplier are rushed, leading to lack of proper checks
- The item comes from a single source with inconsistent and unconfirmed performance
- A lack of a strong safety culture within the organisations involved

3. The Significance of CFSIs for Nuclear Security

Nuclear security requires mitigating the risk of intentionally unauthorised acts involving nuclear material, facilities, and related items and activities.[8] To this end nuclear facilities deploy a range of technology aimed at detecting, delaying and responding to the actions of adversaries. CFSIs can serve to degrade these measures by diminishing the integrity and functionality of security-related equipment, systems, structures, components or devices.[9] This can allow adversaries to exploit nuclear materials, infrastructure and information in a number of ways.

One example of a potential nuclear security scenario involving a CFSI could be the insertion of a fraudulent integrated circuit by an adversarial actor at a nuclear facility. The concern with such items is that malicious actors could install these objects in IT devices and open a 'backdoor' through which they could gain access to the wider system. This could then allow the actor to manipulate security systems and other protective measures to gain access to the facility and exploit it. Counterfeited and malicious chips have been a topic of concern for many states for several years. In a 2005 report, for example, the US Department of Defense raised the issue of circuits embedded with 'trojan horse' malware finding their way into key national security infrastructure.[10] Additionally, a 2020 investigation into counterfeited Cisco devices by Finnish cybersecurity firm F-Secure found that the fraudulent circuits were able to bypass security functions and authenticity checks.[11] Although no backdoors were detected, the ability of the chip to evade security checks meant potential adversaries could gain easier access to the network through such chips.

Another example of potential nuclear security risks that could come from CFSIs include fraudulent services and certifications, such as in the case of falsified security services at a facility. In such a case, inadequate training of security personnel and substandard monitoring by individuals could leave a facility vulnerable to attacks and infiltration by adversaries. Here parallels can be drawn with the actions of the Wackenhut and Babcock & Wilcox security firms in the lead-up to the 2012 incident at the Y-12 National Security Complex at Oak Ridge, Tennessee in the United States.[12] During this time period, guards from these firms were found to be cheating on exams and thus providing falsified security test results to managers at the facility.[13] These overconfident assessments served to mask the reality of the ineffectiveness of security at the facility. The security weaknesses were vividly illustrated by the incursion of an unarmed group of elderly anti-nuclear weapons protestors who were able to bypass various security measures and roam undetected at the facility for several hours.[14] This example serves to demonstrate the serious implications of certificate and results falsification, and the impact this can have on nuclear security.

4. Nuclear Safety-Security Interface

The interface between nuclear safety and nuclear security has gained increasing traction in nuclear policy and practice in recent years, with a 2021 report by the IAEA stressing the importance of recognising this overlap, and of developing existing knowledge and policy on safety and security to address this nexus.[15]

Historically considered as separate concepts, 'nuclear safety' is focused on the prevention or mitigation of nuclear accidents, through achieving proper operating conditions, mitigating the risk posed by human actions such as an error by an operator, as well as equipment malfunction.[16] 'Nuclear security', on the other hand, focuses on preventing or mitigating malicious actions in nuclear and radiological contexts.[17] The term 'nuclear safety-security interface' refers to the shared goals of these measures in protecting life, health and the environment, and how addressing the commonalities between the two concepts can help create a more effective response to incidents.[18]

Despite their differences, nuclear safety and security share a common objective in the protection of people and the environment, and many of the same protection measures and principles. For example, nuclear reactor containment structures are designed to contain immense internal pressures in the event of an incident. This structure can help mitigate the impact of a serious nuclear event, whether it is has a safety or security driver.[19]

The installation of CFSIs in a nuclear or radiological setting creates a potentially significant risk to both nuclear safety and security, and hence requires an integrated response. In fact, the introduction of CFSIs can have negative security consequences even if the supplier did not have harmful intentions. For example, an electronic component that does not meet quality assurance specifications and is installed in a NPP surveillance system could cause the system to become defective or less operable. If separate adversarial actors become aware of this, the weakness could be exploited and result in a security breach. Similarly, a malicious actor or insider adversary could purposefully install a counterfeit component within a safety system at a NPP, with the intention of triggering a radiological release.

5. Existing International Guidance

There exists a range of guidance and recommendations available on CFSIs from international and industry bodies, such as the IAEA and the US Electric Power Research Institute (EPRI).

5.1. Early Guidance and Discussions on CFSIs in the Nuclear Sector

The issue of CFSIs in the nuclear supply chain became apparent in the mid-20th Century amid the expansion of the civilian nuclear industry – albeit initially in the form of quality assurance protocols. Japan, for example, was an early country in recognising the importance of adequate quality measures, imposing tough controls on the standards of items installed during construction and maintenance of NPPs.[20] For example, Article 43 of Japan's 1957 Act on the Regulation of Nuclear Source Materials, Nuclear Fuel Material and Reactors entrenches the duty of licensees to seek adequate permission before making changes to parts, and only install parts or licence services that meet the quality standards of the country's Nuclear Regulation Authority (NRA).[21]

Attention given to quality assurance protocols grew sharply in the 1980s, triggered by the 1979 Three Mile Island incident in the US which was attributed in part to poor quality assurance standards.[22] The US authorities first flagged the specific issue of CFSIs (then labelled 'nonconforming items') in 1989, with a circulatory letter to domestic nuclear operators and constructors. The move followed a series of inspections by the US Nuclear Regulatory Commission (NRC) over a period of two years which had uncovered numerous instances of counterfeit parts being installed, in some cases in safety-related installations.[23] A 1990 report by the US General Accounting Office found that at least 72 of the 113 NPPs operating in the US at the time had or were suspected of having counterfeit and non-conforming parts, prompting the authorities and NRC to take a more direct approach.[24]

The Convention on Nuclear Safety of 1994 enshrined the issue of quality assurance in its text. Article 13 highlights the duty of countries to ensure plants and the parts that go into them meet adequate quality assurance standards, and Article 12 mentions the importance of controlling for human factors throughout the lifecycle of a nuclear facility. In addition to this, Clause II of Article 18 emphasises the importance of ensuring that all parts installed in the construction of a nuclear facility meet proper quality controls, and Clause III of Article 19 urges parties to ensure that these controls are also maintained during operation and maintenance of plants and facilities.[25]

5.2. Recommendations by Organisations and International Standards

Industry groups and international organisations have developed targeted, specialist guidance on CFSIs. For example, EPRI's 2014 guidance document on the use of commercial-grade items in nuclear safety-related contexts.[26] This is an important document in the case of CFSIs as licensees often use commercial-grade items in nuclear facilities, and these items do not undergo some of the testing that nuclear-grade items might. This can mean that CFSIs could enter the system, as was seen in the early 2000s with Square-D circuit breakers at US nuclear plants.[27] Professional organisations, formed of industry members themselves, can thus provide more targeted and up-to-date information about these events as they occur, and guidance on what to do in these instances. For example, EPRI's 2014 guidance document is an update to pre-existing guidance based on newer incidents, lessons learned, and industry changes.[28]

International organisations like the IAEA have produced a number of guidance documents related to the issue of CFSI regulation. In 2000, the IAEA published its first substantiative document on CFSIs in the form of IAEA-TECDOC-1169, titled 'Managing Suspect and Counterfeit Items in the Nuclear Industry'.[29] This was updated in 2019 with the publication 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', which collates updated examples, background information, and guidance on the issue of CFSIs for Member States. The document also incorporates findings from other papers published by the IAEA on issues like supply chain security and procurement engineering.[30] Another organisation that provides guidance on CFSIs is the OECD, which assists member states in better understanding the risk and addressing CFSIs. The OECD has established a task group to examine the risk of CFSIs to the nuclear supply chain and has published a series of reports and recommendations based on their findings. One example is its report on Recommendations of Regulatory Oversight of CFSIs, published in February 2013, which helps member states better understand and identify CFSI risk factors in their countries.[31]

These guidance documents are supported by standards set by groups like The International Organisation for Standardisation (ISO) which published a set of requirements regarding the nuclear energy supply chain in 2018. ISO19443 created the standards to complement existing guidance from the IAEA and seeks to adapt its pre-existing quality management standards for nuclear safety-specific contexts in the nuclear energy sector.[32]

These international groups are aiding nations and industry in addressing the risk of CFSIs in the nuclear supply chain, as well as helping in identifying the goods, actors and geographies involved in these counterfeiting missions. Despite these efforts, however, CFSIs are still not very well-understood by many involved in the sector, and this handbook seeks to further educate a global community of nuclear stakeholders on the importance of tackling the CFSI threat.

References

1 In the United Kingdom, Critical National Infrastructure (CNI) refers to industries, facilities, networks, and processes that are necessary for the country to function or could severely impact local populations (eg hazardous chemicals or nuclear). More information can be found at https://www.npsa.gov.uk/critical-national-infrastructure-0

2 Michael Duitsman and Margarita Kalinina-Pohl, 'Open Source Intelligence and Investigative Techniques for Locating Radioactive Sources', in Christopher Hobbs, Sarah Tzinieris and Sukesh K. Aghara (eds.) The Oxford Handbook of Nuclear Security, Oxford: Oxford University Press, 22 May 2023. https://doi.org/10.1093/oxfordhb/9780192847935.013.3

3 Robert B. Barr and John Tagg, 'From Teaching to Learning – A new Paradigm for Undergraduate Education', Change: The Magazine of Higher Learning 27(6), 1195, 12-26. https://doi.org/10.1080/00091383.1995.10544672

4 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

5 Organisation for Economic Co-operation and Development, 'Regulatory Oversight of Non-conforming, Counterfeit, Fraudulent and Suspect Items (NCFSI)', 2012. https://www.oecd-nea.org/upload/docs/application/pdf/2020-01/cnra-r2012-7.pdf

6 World Nuclear Association Supply Chain Working Group, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', World Nuclear Association, 2019-005, August 2019. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

7 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

8 International Atomic Energy Agency, 'Nuclear Security: IAEA Nuclear Safety and Security Glossary', undated. https://vocabulary.iaea.org/iaea-safety-glossary/1185

9 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, NP-T-3.26, March 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

10 Defence Science Board Task Force, 'High Performance Microchip Supply', Office of the Under Secretary of Defence for Acquisition, Technology, and Logistics, Washington, DC, February 2005. https://dsb.cto.mil/reports/2000s/ADA435563.pdf

11 Dmitry Janushkevich, 'The Fake Cisco: Hunting for backdoors in counterfeit Cisco devices', F-secure Consulting Hardware Security Team, 15 July 2020. https://labs.withsecure.com/publications/the-fake-cisco

12 US Department of Energy Office of Inspector General, 'Inspection Report: Protective Force Performance Test Improprieties', DOE/IG-0636, January 2004. https://www.energy.gov/sites/default/files/igprod/documents/CalendarYear2004/ig-0636.pdf; Matthew L. Wald, 'Exam Said to Be Leaked to Guards at Nuclear Site', The New York Times, 31 October 2012. https://www.nytimes.com/2012/11/01/us/guards-at-breached-nuclear-site-in-tennessee-cheated-on-exam-report-says.html

13 US Department of Energy Office of Inspector General, 'Inspection Report: Protective Force Performance Test Improprieties', DOE/IG-0636, January 2004. https://www.energy.gov/sites/default/files/igprod/documents/CalendarYear2004/ig-0636.pdf; Matthew L. Wald, 'Exam Said to Be Leaked to Guards at Nuclear Site', The New York Times, 31 October 2012. https://www.nytimes.com/2012/11/01/us/guards-at-breached-nuclear-site-in-tennessee-cheated-on-exam-report-says.html

14 Fissile Material Working Group, 'Security at Y-12 nun too good', Bulletin of the Atomic Scientists, 2 October 2012. https://thebulletin.org/2012/10/security-at-y-12-nun-too-good/

15 International Atomic Energy Agency, 'The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences', Technical Reports Series No.1000, Vienna, March 2021. https://www-pub.iaea.org/MTCD/Publications/PDF/PUBDOC_1000_web.pdf

16 International Atomic Energy Agency, 'IAEA Nuclear Safety and Security Glossary: Terminology used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness Response', Vienna, 2022. https://www-pub.iaea.org/MTCD/Publications/PDF/IAEA-NSS-GLOweb.pdf

17 International Atomic Energy Agency, 'IAEA Nuclear Safety and Security Glossary: Terminology used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness Response', Vienna, 2022. https://www-pub.iaea.org/MTCD/Publications/PDF/IAEA-NSS-GLOweb.pdf

18 European Atomic Energy Community, Food and Agriculture Organization of the United Nations, International Atomic Energy Agency, International Labour Organization, International Maritime Organization, OECD Nuclear Energy Agency, Pan American Health Organization, United Nations Environment Programme, World Health Organization, 'Fundamental Safety Principles', IAEA Safety Standards Series No. SF-1, Vienna, November 2006. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1273_web.pdf

19 US National Research Council, 'Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report', Washington, DC: The National Academies Press, 2006. https://doi.org/10.17226/11263; UK Parliamentary Office of Science and Technology, 'Assessing the risk of terrorist attacks on nuclear facilities', POST Report 222, London, July 2004. https://www.parliament.uk/globalassets/documents/post/postpr222.pdf

20 Japan Nuclear Regulation Authority, 'Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors', Act No. 166 of 10 June 1957. https://www.nra.go.jp/data/000067232.pdf

21 Japan Nuclear Regulation Authority, 'Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors', Act No. 166 of 10 June 1957. https://www.nra.go.jp/data/000067232.pdf

22 J. Samuel Walker and Thomas R. Wellock, 'A Short History of Nuclear Regulation, 1946-2009', Office of the Secretary, US Nuclear Regulatory Commission, October 2019. https://www.nrc.gov/docs/ML1029/ML102980443.pdf

23 US Nuclear Regulatory Commission, 'Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products', Generic Letter 89-02, 21 March 1989. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/gen-letters/1989/gl89002.html

24 United States General Accounting Office, 'Nuclear Safety and Health: Counterfeit and Substandard Products are a Governmentwide Concern', Report to the Chairman, Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, 16 October 1990. https://www.nirs.org/wp-content/uploads/reactorwatch/counterfeitparts/counterfeitpartsgao10161990.pdf

25 International Atomic Energy Agency, 'Convention on Nuclear Safety', IAEA INFCIRC/449, 5 July 1994. https://www.iaea.org/sites/default/files/infcirc449.pdf

26 Electric Power Research Institute, 'Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications', Technical report, California, September 2014. https://www.epri.com/research/products/000000003002002982

27 US Nuclear Regulatory Commission, 'Counterfeit Parts Supplied to Nuclear Power Plants', NRC Information Notice 2008-04, 7 April 2008. https://www.nrc.gov/docs/ML0807/ML080790266.pdf

28 Electric Power Research Institute, 'Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications', Technical report, California, September 2014. https://www.epri.com/research/products/000000003002002982

29 International Atomic Energy Agency, 'Managing Suspect and Counterfeit Items in the Nuclear Industry', IAEA-TECDOC-1169, 2000. https://www-pub.iaea.org/MTCD/publications/PDF/te_1169_prn.pdf

30 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

31 Organisation for Economic Co-operation and Development, 'Regulatory oversight of Non-conforming, Counterfeit, Fraudulent and Suspect Items (NCFSI): Final NCFSI Task Group Report', Nuclear Energy Agency Committee on Nuclear Regulatory Activities, 15 February 2013. https://one.oecd.org/document/NEA/CNRA/R(2012)7/en/pdf

32 International Organization for Standardization, 'ISO 19443:2018 Quality Management Systems – Specific requirements for the application of ISO 9001:2015 by organisations in the supply chain of the nuclear energy sector supplying products and services important to nuclear safety (ITNS)', May 2018. https://www.iso.org/standard/64908.html

Part II
Threat Landscape, Goods, Actors and Geographies

Studies indicate that CFSIs are both present and growing within a wide range of sectors. Using data from 2016, a 2019 report by the Organisation for Economic Co-operation and Development (OECD) and European Union Intellectual Property Office (EUIPO) noted that counterfeit goods could amount to US$509 billion, accounting for 3.3% of global trade.[1] This was an increase from a previous study by the OECD and EUIPO, which estimated the trade was worth US$461 billion or 2.5% of the global economy based on data from 2013.[2] Furthermore, the US Department of Homeland Security (DHS) has reported that seizures of counterfeit goods at US borders increased 10-fold between 2000 and 2018.[3]

The actors and networks coordinating, facilitating and profiting from the production, sale and transfer of CFSIs are diverse, depending on the sector in which they are operating. However, what they all have in common is their use of the legitimate channels, infrastructure and modalities of international trade to run their operations, their use of deception to pass off CFSIs as authentic items, and their ability to adapt their operations to continue to profit.

This section of the handbook takes a deeper dive into the networks involved in disseminating CFSIs and their modus operandi. Rather than focusing only on those technologies that could jeopardise nuclear security, it takes a broader view by drawing on examples that are from adjacent or relevant industries (for example industrial goods, electronics and security equipment) which could feed into the nuclear industry.

The first sub-section considers the 'what' – what types of goods, products and services might be most vulnerable to being CFSIs. Considering this first allows for more specific analysis of the actors, geographies and supply chains involved. The second sub-section considers the 'who and where': the actors and networks, and where they are located. The third sub-section considers CFSI supply chains – essentially the 'how' from production to the customer: the geography of these supply chains including the distribution hubs and the means by which goods are moved to the target markets.

1. What? Goods, Products and Services That Are More Vulnerable

The types of goods that have seen CFSI equivalents is broad – encompassing most types of commodities. Studies in recent years have highlighted the growing scope of products in global supply chains. As a report by the US Government Accountability Office (GAO) noted in 2018, counterfeiters are increasingly producing a 'wider variety of goods' that may be sold alongside authentic products.[4] CFSI producers can quickly adapt, as the OECD-EUIPO report has noted, 'Trade in fake goods is a very dynamic activity, as counterfeiters look very aggressively for new profit opportunities.'[5]

1.1 CFSIs – A Growing Range of Items

As the OECD and EUIPO have noted, 'Infringed products are found in numerous industries'.[6] Data used by the OECD and EUIPO based on seizures provides a list of the top industries that are targeted by CFSI producers – the top 10 being: [7]

- Footwear;
- Clothing;
- Leather products;
- Electrical machinery and equipment;
- Watches;
- Optical photographic and medical instruments;
- Perfumery and cosmetics;
- Toys;
- Jewellery;
- And pharmaceutical products.

CFSI networks also adapt to take advantage of new opportunities, which may lead to increased interest in particular sectors – for example, there was a huge growth in counterfeit medicines, facemasks and other personal protective equipment (PPE) during the Covid-19 pandemic.[8] The OECD-EUIPO report noted several new product areas in which counterfeits had been detected, including: fur skins and artificial fur; salt; sulphur; earth and stone; lime and cement; and ores, slag and ash; with particular growth in counterfeit guitars and construction materials.[9]

Even more concerningly, CFSIs have frequently been found among goods that are feeding into defence and critical infrastructure supply chains. The DHS in the US noted that in 2018, '12 percent of DHS seizures included counterfeit versions of critical technological components, automotive and aerospace parts, batteries, and machinery.'[10] In 2008, a US government researcher looking into counterfeit chips suggested that as many as 15% of the chips that the US Department of Defense (DOD) procures were CFSIs rather than genuine.[11]

1.2 CFSIs in Nuclear Facilities

CFSIs have been considered previously in the context of the nuclear industry – although these reports have mostly focused on their impact on safety. There have been efforts to explore what broad types of products areas – as well as specific items – might be vulnerable to counterfeiting. In addition, situations in which CFSIs might make their way into the nuclear industry are typically a product of factors both on the suppliers' and customers' ends. The IAEA's Technical Report 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry' has identified conditions where CFSIs are likely to appear:[12]

- There is significant financial benefit for the counterfeiter;
- The items are difficult to verify or not typically verified;
- Procurement requirements (technical specifications) are poorly defined;
- Methods or criteria for verifying that procurement requirements are met are inadequate;
- Urgent replacement of an item is required (ie there are schedule pressures);
- Supplier qualifications are expedited;
- The item is supplied from a single source with unreliable or unverified performance;
- There is not a strong safety culture within the organisations involved.

Information provided by the US Department of Energy (DOE) in an August 2016 handbook – which builds on a 1990 information notice – provides a list of characteristics that makes goods particularly vulnerable to counterfeiting – or 'misrepresentation' by vendors.[13] Products are more likely to be misrepresented in these contexts:

- Items or components are moderate or low-cost items with high turnover usage rate;
- Items or components that can be easily copied by secondary market suppliers;
- Items or components that are often drop shipped to the customer, with minimal engagement with the supplier;
- Items or components that are substantially lower priced than market value or competitors pricing;
- Items or components for which special processes may be subcontracted (heat treating, testing, and inspections for ASME materials, for example);
- Items or components for which there is a viable salvage market;
- Items or components where there is a small or declining number of original equipment manufacturers;
- Items and components that are obsolete or hard to obtain;
- Items or components that are manufactured by a company that is no longer in business;
- Items or components with documentation from a plant where construction has been suspended, cancelled, or deferred;
- Items or components that can be reproduced with high-profit potential.[14]

The DOE handbook also provides a list of types of specific products deemed vulnerable to counterfeiting – building on the 1990 notice (see Box 1).

Box 1. Nuclear-Relevant Products Vulnerable to Counterfeiting[15]

i. General Items

- Spare/replacement kits from vendors other than the original equipment;
- Manufacture;
- Elastomer – 'O' rings, seals;
- Lubricants;
- Adhesives;
- Electrical connectors;
- Metal Framing components (ie flat plate fittings, post bases, beam clamps, channel); and
- Flanges.

ii. Electrical Items

- Motor control centers – complete units;
- Components;
- Starters;
- Starting coils;
- Contactors;
- Contactor kits;
- Overload relays;
- Starter control relays;
- Overload heaters;
- Protective/control relays;
- DC power supplies/chargers;
- AC inverters;
- Current/potential transformers;
- Exciters/regulators;
- Bus transfers/auto bus transfers;
- Motor generators sets;
- Generators;
- Rewindable motors;
- Printed circuit boards;
- Fuses;
- Splices Vacuum breakers (BWR);
- Indicators/controllers;
- Panel lights/switches;
- Transmitters/instrument switches; and
- Isolation devices.

iii. Mechanical Items

- Welding Materials;
- Rods;
- Wires;
- Fluxes;
- Small piping products;
- Small structural members (pipe supports);
- Spent fuel pool cooling pumps and similar pumps;
- Ultimate heat sink supply manual valves and similar valves; and
- Valves.

iv. Diesel Generator Items

- Diesel speed governors;
- Diesel fuel transfer pumps; and
- Diesel injection pumps.

v. Lifting Materials

- Slings;
- Hooks;
- Cables; and
- Shackles.

1.3 CFSI and Security Equipment

Due to the safety focus of this prior analysis of CFSI risks, security-related items have not been considered in the nuclear context. Nuclear sites use many security-related technologies and items that could be CFSIs. Particular areas of vulnerability could include:

- **Electronic equipment:** Electronic components represent an enormous risk area for CFSIs. Counterfeit electronic components could make it into electronic security equipment – cameras and surveillance systems, x-ray machines and scanners, and systems used to maintain cyber security.

- **Security barriers and related materials:** Barriers and materials that have been tested to withstand certain impacts, forces and stresses could potentially be mislabelled. There have been other cases of materials quality inspection data being falsified that have affected the nuclear industry.[16]

- **Detection equipment:** Handheld detectors used to search for contraband – such as metal and explosives – can also be CFSIs. One of the most well-known brands of handheld metal detectors is known to have been counterfeited.[17] A case involving a British fraudster saw thousands of fake ADE651 and GT200 bomb detectors – a non-viable technology based on junk science – sold to a wide range of countries around the world between the mid-2000s and 2013.[18]

- **Communications equipment:** Counterfeit radio equipment, including handheld radios used by security personnel, has been found in circulation.[19] A further example in 2019 saw the US Navy Seals procure 450 counterfeit radio antennas.[20]

- **Armed response equipment**: Equipment used by armed responders is also vulnerable to counterfeiting. This includes body armour, with a 2018 case involving a business selling mislabelled body armour which included plates not tested to military specifications to a US government agency.[21] There are further examples of mislabelled body armour with less protective steel plates in circulation.[22] Examples have also shown that ammunition can be mislabelled by individuals seeking to fulfil government contracts.[23]

1.4 Counterfeit and Fraudulent Services

The CFSI abbreviation suggests tangible items, but counterfeit or fraudulent services and service providers could also present risks. These may be services provided by those without the necessary certification, qualifications, expertise or knowledge. Several examples have been seen of manufacturers fraudulently certifying goods to higher specifications than they were – including through falsifying or fabricating inspection and testing data.[24] There have also been examples of service providers claiming to have completed testing and other work, signing off on it when that was not the case.[25] External technical service providers could potentially do the same in providing testing and other services – for example, relating to security equipment and systems. There is also scope for providers of training and other consultancy related to the human aspects of security systems and processes to be providing fraudulent services. For example, training could be provided by organisations overselling their relevant experience or qualifications.

2. CFSI Threat Actors: Manufacturers and Intermediaries: Who and Where?

A wide range of actor types are involved in the multi-billion-dollar industry surrounding the production and distribution of CFSIs. Given the wide range of CFSI goods produced and disseminated globally, there are a hugely diverse set of actors involved, with each industry or network drawing on a different set of manufacturers and intermediaries. The types of goods that might be counterfeit and fraudulent and be of use in the nuclear industry suggests that a narrower sub-set of these broader CFSI producing and disseminating actors would likely be involved.

2.1 Conceptualising the Actors in CFSI Supply Chains

Key to all passing off all CFSIs as genuine to achieve a sale is deception (see Box 2). At some point in each CFSI supply chain there is at least one actor – and often more – that are knowingly passing off counterfeits as genuine. These actors involved in deception could be as far back in the chain as the manufacturer, or as far down the supply chain as a witting insider based within the recipient organisation who turns a blind eye to clearly falsified paperwork.

Box 2. Common Means of Deception – The Products Themselves

To pass off counterfeit or substandard goods as an authentic item, those involved in these networks need to deceive customers. There are several ways that deception can occur that relate to the products themselves, with multiple means of deception potentially being used in an individual case.

Manipulating the goods. The goods themselves – whether these are handbags, industrial goods or semiconductors – can be manufactured or changed to look like the authentic item. For example, through adding or altering logos, serial numbers, or other identifiers on the goods, or through manufacturing them in similar colours, actors can manipulate CFSIs to resemble the real thing.

There are several means of deception that relate to the product that are more specific to the counterfeit semiconductor industry. These are steps that are often taken to make newly manufactured lower grade chips or recovered/refurbished chips to make them look of a higher grade or new. Much of this activity relates to manipulating the chip's markings, which typically include information such as model, origins and certification. Specific actions include:

- Removing markings: This can occur in a variety of ways – through sanding, sand blasting, laser ablation, acid washing or exposure to open flames.
- Layering over markings: 'Blacktopping' sees a thin layer of black epoxy coating applied to the top of a component so that it can be remarked with a new part number and date code.
- Remarking: New markings are added after the older ones have been removed using lasers, digital printing, and other techniques.
- Disguising: The soldering of integrated circuits can be reworked, components removed or substituted to make the product look like something it is not.

Manipulating attached paperwork. Paperwork included with the goods – everything from product manuals, warranty paperwork or associated testing paperwork could be forged or falsified.

False advertising. The goods can be advertised as the authentic item – either online or in more traditional means. Pictures of the authentic items can be used rather than the counterfeit item.

False labels and packaging. Goods can be packaged to look like the authentic item – with false printed packaging and labels produced for this purpose. Goods can also be re-packaged in transit to make them look like a higher-grade or higher-quality version than that manufactured.

Figure 1 provides a notional CFSI supply chain to facilitate discussion of the types of actors involved; in any given CFSI supply chain, there could be multiple layers of each different type of actors involved. For example, there could be multiple manufacturers involved in the production of a CFSI (witting and unwitting of the deception), multiple (or no) intermediaries, and a diverse set of actors that constitute the customer (especially in the case of counterfeit chips which can be integrated into circuits, sub-systems and systems). Deception could occur within any or more than one of these three stages.

Figure 1. Notional Supply Chain for Tangible CFSIs

Factors Shaping CFSI Network Behaviour and Capability

The actors and networks involved in producing CFSIs look for and identify potential business opportunities and are largely driven by financial incentives. As the aforementioned OECD-EUIPO report has outlined, the behaviour of these networks is ultimately shaped by several core decisions:

1. What products will be counterfeited or pirated;
2. Where the products will be produced;
3. Where the [intellectual property] infringement will take place;
4. Which geographic markets will be targeted; and
5. How products will be shipped to end markets without being intercepted.[26]

Decisions surrounding these factors will be shaped by perceived benefits – mainly how profitable these opportunities are – and also perceived costs. The economic benefits of the revenue generation from producing and distributing CFSIs are clear: CFSIs are often cheaper to produce; they utilise cheaper materials, labour and facilities; they do not require the purchase of intellectual property; and they may be manufactured in facilities that do not face high costs of compliance in areas such as health and safety, legal compliance and other areas.

However, the financial benefits of producing fake or counterfeit products are less certain or long-lasting than they are for legitimate producers. Holders of the original intellectual property (IP) are more likely to be recognised for their high standards and quality and therefore more likely to see repeat business. As discussed, those producing CFSIs ultimately rely on means of deception to pass fake products off as authentic (see Box 2). They are less likely to build long-lasting business relationships due to concerns over the product's quality, the deception required to pass them off, potential disruption to supply caused by law enforcement attention or interest, or legal action of the companies who they are trying to deceive or emulate.

The potential costs will include those relating to the production and movement of the goods as in any industry, but also those emanating from risks that are more specific to the CFSI – for example, the risk of fakes being identified and removed from the supply chain, the risks of operating in certain jurisdictions, or the risks of schemes being uncovered and the deceived customers finding new suppliers, or disrupted by law enforcement.

The concept of 'competitive adaptation' – used in the literature on counterterrorism and counternarcotics – is useful for understanding how illicit networks adapt in competition with law enforcement.[27] In competitive adaptation, networks seek to exploit opportunities presented by ongoing developments in the legal and enforcement environment. CFSI producers are constantly looking for new ways to undertake their activities, enhance profits and reduce costs, as well as avoid enforcement activities.

The scope of entities that are capable of manufacturing and disseminating CFSIs for the nuclear industry and particularly nuclear security systems is a niche area of the market. Producing CFSIs specifically for the nuclear industry has high technological barriers to entry and limited opportunities to profit, as compared to manufacturing fake handbags, for example. There are, however, a range of ways that manufacturers producing for adjacent sectors could fraudulently label or pass off lower grade goods to nuclear customers.

Those producing CFSIs tend to adapt their activities to outcompete those trying to detect the counterfeits that they are manufacturing. As a semiconductor industry executive noted in testimony to US Congress in 2011, 'The counterfeiters are most certainly monitoring our level of detection expertise and quickly evolving newer processes to introduce into the global supply chains. Many of the current counterfeiting techniques are already beyond the in-house detection capabilities of most open-market suppliers.'[28]

Recent technological developments also have shaped the evolving capabilities of CFSI producing networks, whose abilities are becoming more sophisticated over time. Computer hacking provides opportunities to steal IP to replicate goods that was previously only available to those with insider access.[29] Manufacturing advances also provide opportunities, with technologies such as 3D printing and computer aided design (CAD) and manufacturing raising the counterfeiting capabilities of those with limited expertise. The ability to outsource design to freelancers online and remotely also aids the capability of these actors.

In addition, the broader growth of dual-use industrial capabilities has had an impact on the potential for CFSIs to make it into the nuclear sector. Dual-use industries are those with the capability to produce higher-grade goods (often export controlled goods) of use in both civil and military applications – and may have uses in the nuclear industry and its security functions. Greater dual-use industrial capacities in more countries around the world means that the number of entities capable of producing CFSIs posing a risk to nuclear safety and security has grown.

2.2 Manufacturers

In most cases, those involved in manufacturing CFSIs are aware the goods that they are producing are not the genuine article; an exception, however, might be where genuine goods are produced but later re-labelled as higher-specification or manipulated by intermediaries in other ways to become a CFSI. Deception frequently occurs at the manufacturing stage when counterfeit goods are produced in order to be deliberately passed off as genuine merchandise.

There is relatively little information about the CFSI manufacturing entities in the public domain; they avoid exposure for good reason. Nevertheless, several types of manufacturing operations involved in CFSI supply chains can be identified:

- **Small-scale CFSI manufacturing.** Some manufacturing involves only a small operation – either with a small number of individuals manufacturing counterfeit items, or individuals within an organisation who would wittingly try to pass off counterfeit items as the genuine article, perhaps without the broader organisation's knowledge.

- **Larger scale CFSI manufacturing.** Some operations will be larger in scale – for example factories that are pushing out counterfeit leather goods or counterfeit 'clone' semiconductor chips. Larger operations are required when goods are of such complexity to require multiple stages in the manufacturing process, or perhaps where counterfeits can be manufactured to be sold at volume to create greater profits.

- **Original Component Manufacturers.** Specifically in the electronics supply chain, genuine manufacturers of components are producing genuine chips. They may, however, be unwittingly dragged into CFSI production – for example with waste rejects being repackaged and sold as originals, or with components E-harvested later in the counterfeit chip supply chain.

- **Rogue semiconductor manufacturers/clone chip producers.** Specifically in the electronic supply chain, rogue semiconductor manufacturers can attempt to reverse engineer or steal IP in order to reproduce 'clone' semiconductor chips.[30] Contract foundries can also overproduce designs provided to them by legitimate semiconductor manufacturers and provide them to those seeking to produce CFSIs.[31]

- **Supporting manufacturing entities.** Those that make the actual CFSIs are supported by a wider network of supplier entities (see Box 3) – both witting and unwitting – including raw material suppliers and packaging manufacturers.

- Criminal organisations. Across the CFSI production spectrum – from consumer goods to electronics and beyond – criminal organisations are frequently involved due to the profitability of the enterprise. Europol has noted, for example, that Chinese criminal networks are 'heavily involved' in the production and distribution of counterfeit items, and that 'Mafia-style criminal networks are extensively involved in IP [intellectual property] crime.'[32] The Customs and Border Protection (CBP) federal agency in the US also notes that 'purchasing counterfeit goods often supports criminal activities, such as forced labor or human trafficking.'[33]

2.3 Where are Manufacturers Located?

A 2018 OECD-EUIPO study considered 'Why do countries export fakes?' – and identified five drivers that shape a jurisdiction's propensity to become 'an active actor in the trade in fake goods' (see Box 4). The report notes that, of the five drivers, 'gaps in governance, especially high levels of corruption and gaps in intellectual property rights enforcement, are the crucial factor for trade in fakes, multiplying the effects of free trade zones (FTZs), logistic facilities or trade facilitation policies.'[34] Many of these factors could also apply to the propensity to become an intermediary or 'third country' jurisdiction in illicit supply chains (see Box 4).

Box 3. Beyond the Manufacturers – Supporting Entities[35]

A recent DHS paper (using the example of a China-based CFSI manufacturer) highlights the wider networks surrounding the production and dissemination of CFSIs – including both those at the manufacturing and intermediary stages, and other stages of the supply chain.

1. Raw material suppliers
2. Freight agents smuggling controlled components 'in' the manufacturer
3. The manufactures who make the actual product
4. The printers who make the packaging
5. The China-based traders who link overseas buyers with the manufacturers
6. The international traders who manage the global trade and distribution
7. The logistics agents who bring the goods out of China to the end market
8. The corrupt government or local officials who allow the manufacture and export to go ahead unmolested
9. The end market wholesale buyer
10. Distribution in the end market
11. Commercial seller
12. The end buyer/final customer
13. Money laundering service providers

Box 4. Factors Driving Jurisdictions to Become Active in the CFSI Trade[36]

1. **Governance:** high levels of corruption and poor intellectual property protection are factors that greatly influence the degree of exports of fake goods from an economy.

2. **Free trade zones (FTZs):** FTZs offer a relatively safe environment for counterfeiters, with good infrastructure and limited oversight. The share of fake goods from economies hosting the 20 biggest FTZs is twice as big as from economies that do not host any FTZs.

3. **Production facilities:** low labour costs and poor labour market regulations are important drivers of trade in counterfeit and pirated goods. Improving working conditions, by raising the minimum wage or increasing paid leave, would decrease the share of counterfeit and pirated products exported, especially by economies with weak governance.

4. **Logistics capacities and facilities:** the ability to trace and track consignments is the key factor for reducing the share of counterfeit and pirated products in exports. However, other factors increase this trade, including: low shipping charges; fast, simple and predictable customs formalities; and good quality trade and transport-related infrastructure (eg ports, railroads, roads and information technology). These factors tend to be also much more important drivers in economies that are highly corrupt.

5. **Trade facilitation policies**: The way trade facilitation is implemented matters. Enhancing transparency is likely to reduce the likelihood that an economy will export fakes. This includes: the availability of detailed information on trade flows; the degree of involvement of an economy in the trade community; transparent and regular review of fees and charges imposed on imports and exports; and sound internal co-operation between border agency and other government units. Other factors tend to encourage counterfeit trade, such as advance rulings (ie where the administration asks traders about the classification, origin, valuation methods etc. applied to specific traded goods), and the possibility to appeal administrative decisions by the border agencies.

The complex supply chains and deception involved often make it difficult to ascertain the true origins of products – even more so when goods may have been manipulated or repackaged and documented during transfer. Because of this, the OECD-EUIPO reports have tended to use the term 'provenance economy', which encompasses originating jurisdictions, and sometimes transit or transshipment jurisdictions.

The greatest supply of counterfeit emanates from China, including the Hong Kong Special Administrative Region (SAR). According to most reports, both jurisdictions are prolific producers of CFSIs. According to the 2016 OECD-EUIPO study, China appears as 'the single largest producing market'.[37] This was further reflected in the OECD-EUIPO's 2019 report that identified China as the top producer of counterfeit goods in nine out of ten categories considered in further depth.[38]

Furthermore, a 2020 report by the US DHS notes of seizure data, 'Over 85 percent of the contraband seized by [US Customs and Border Protection] arrived from China and Hong Kong.'[39] This is certainly true of microelectronics, with a more recent DHS paper noting, 'the same regional centers that produce valid microelectronics are natural areas for counterfeit production because of access to feedstock, transportation infrastructure for import and export, and workers that may have experience in the electronics industry.' It goes on to identify major production areas as Beijing, Shandong, Fujian, Hong Kong and Shenzhen.[40]

Beyond electronics, there are multiple manufacturers in cases where sub-standard security technologies have been passed off as the authentic item, based in China. For example, a 2021 case involving the sale of fraudulent body armour to the US state department saw a Texas-based businessman import lower specification armour from China and claim to have produced it in a non-existent US-based factory.[41]

Chinese ammunition has also been relabelled and used by fraudsters to fulfil a US government contract.[42] Nevertheless, both these cases involved Chinese goods being re-labelled by those in the US, rather than items deliberately manufactured as CFSIs.

Beyond China, there are several other jurisdictions where CFSI production has occurred. As a 2019 OECD-EUIPO study notes, 'Several Asian economies, including India, Malaysia, Pakistan, Thailand, Turkey and Viet Nam are important producers in many sectors, although their role is much less significant than China's.'[43] A 2017 OECD-EUIPO report exploring different CFSI sectors noted that while China- and Hong Kong-origin CFSIs collectively accounted for around 90% of the value of global seizures from 2011-2013, other jurisdictions that were 'top provenance economies' accounting for the other around 10% of electronics CFSIs included the UAE, Canada, Korea, Ghana, Singapore, Mexico, Malaysia, India, Azerbaijan and Sri Lanka.[44]

To produce CFSIs relevant to the nuclear sector or nuclear security, manufacturing jurisdictions will likely require some level of capability in manufacturing similar items. For example, jurisdictions where there is limited manufacturing capability, or no existing manufacturing of lower specification detection equipment, communications equipment and armed response equipment are less likely to be involved in the production of CFSIs. States with extensive surveillance and security equipment industries may be more likely to be a source of mislabelled security equipment.

Here, some states may pose a particular risk. North Korea, for example, has historically been involved in the sale of nuclear technologies and a range of counterfeit goods including pharmaceuticals, cigarettes and others.[45] Recent acceleration of the North Korean nuclear programme raises the prospect of sales of nuclear or dual-use technology laundered through intermediaries in third countries.[46] North Korea has also sought to pass off military radios manufactured domestically as Malaysian products in the past.[47]

2.4 Intermediaries Peddling and Manipulating CFSIs

Beyond manufacturers, several types of intermediary CFSI threat actors either knowingly distribute CFSIs or manipulate already-manufactured goods in order to pass them off as a superior and/or more expensive product. Intermediaries could be brokers involved in buying and selling CFSIs. They could be electronics distributors who account for a large proportion of the trade in off-the-shelf semiconductor chips. They could also be intermediaries that act as distribution points in these supply chains – accepting larger container shipments and repackaging goods as small packages so that they more easily pass through customs and other checks on the way into more regulated market jurisdictions.

There are also other actors, that are not specifically-manufacturers, involved in reclaiming components from E-waste in order to sell them as new. These are intermediaries in some sense, but are also located much further down the supply chain, after the initial goods were purchased, used and discarded by the initial customers.

Relevant intermediaries include:

- **Brokers.** Those buying CFSIs to sell or distribute can be a variety of business types – from single person operation to a larger distribution centre – and located in the manufacturing, third country or target market jurisdictions.

- **Electronics Distributors.** In electronics supply chains – and for those of other goods – distributors are an important and prevalent actor, with a variety of types present. They may, or may not, be aware that they are distributing CFSIs. These distributors include franchise distributors (authorised by manufacturers and/or customers), independent distributors (these are also known as 'brokers') and wholesale distributors (these opportunistically speculatively purchase large quantities of components).

- **Manipulators.** Intermediaries involved in manipulating the product are also involved in the supply chains. They could perhaps be involved in taking legitimate items and relabelling or repackaging them, so that they appear to be something else, or even altering the products themselves through adding logos or in other ways altering their appearance. They could also be involved in basic assembly operations to make early shipments of disassembled parts less likely to be disrupted, for example.
- **E-waste harvesters.** Also loosely falling into this category are those involved in creating CFSI chips through harvesting E-waste (see Box 5). They take electronic waste and remove components or circuits of value for further manipulation. They are not manufacturers, yet they are further down the supply chain than the customers for the initial products. It has been estimated that 80-90% of counterfeit chips are recycled in some form.[48]

The location of these intermediary actors is considered in Section 3 when the supply chain is discussed in more details.

Box 5. E-Waste Harvesting

According to a 2020 report, 53.6 million metric tons of electronic waste was produced around the world in 2019 – the equivalent of around 7.3kg per person.[49] Beyond serious environmental and public health impacts, this creates huge opportunities for recycling, counterfeiters and organised criminal networks. E-waste contains many valuable materials such as gold and copper that can be extracted. However, some of this waste also includes useful semiconductors of various types that can be cut out, manipulated and re-inserted into supply chains.

China has traditionally been the most prominent region for E-waste harvester. For example, Guiyu, around 100 miles east of Hong Kong on the Chinese coast, used to be one of the largest E-waste recycling hubs in the world. The town hosted 5,000 small workshops and 60,000 workers dismantling electronic equipment.[50] More recently the town has made efforts to diversify from such a hazardous industry.[51]

Hong Kong has also been a prominent hub. A 2016 study that fixed 205 trackers to E-waste in the US found that 34% were exported with 31% to developing countries, and more than half of the exported trackers ended up in Hong Kong in 48 different electronics junkyards, with destinations in mainland China were a distant second.[52] Steps taken in recent years by the Chinese government have seen restrictions on the imports of different types of waste including electronic waste,[53] but there are clearly opportunities for smuggling, and Hong Kong's separate governance structure provides a significant loophole in implementing regulation.[54]

3. How? CFSI Supply Chains to the Customer

A variety of means are used to transfer the CFSIs from the manufacturer or manipulator to the customer. These transfers provide ample opportunities for deception (see Box 6). The wide range of types of CFSIs again means that the supply chains are very diverse.

Box 6. Common Means of Deception – Transfers to the Customer

Building on means of deception surrounding the products themselves (Box 2), deception is also used to move the CFSI goods to markets and customers. Many of these means of deception are similar to those used in other areas of illicit trade where networks move weapons, narcotics, strategic commodities and endangered wildlife products, for example. Some of these means of deception are listed in this box, and others are explored below: [55]

- Use of complex shipping routes to complicate detection by customs and law enforcement
- Shipping through jurisdictions with limited enforcement will and/or capacity
- Warehousing, repackaging through third country jurisdictions
- Warehousing, repackaging through FTZs
- Hiding products in containers behind other legitimate goods
- Shipping disassembled for assembly on route or at the destination
- Sending final products without logos or other trademark infringing materials
- Falsifying import/export declarations or other paperwork
- Using multiple layers of front companies to complicate the chain of custody
- Using opaque corporate structures and financial flows

3.1 Marketing and Finding Customers: The Rise of Online Marketplaces

To sell CFSIs, the producers must find a way to connect with potential customers – this can happen in more traditional ways, and more significantly now through E-commerce platforms. More traditional means are likely to involve sales through catalogues, at trade shows, and through distributors with which the sellers and customers build personal relationships. These means often involve more face-to-face contact – and are getting less common as compared to through electronic platforms. As a US official has noted on counterfeit chips, this is often opportunistic and taking advantage of customer needs considering shortages, of which there have been many in recent years: 'There is more incentive than ever to profit off of counterfeit components just by advertising that you have them available within the supply chain when no one else does.'[56]

The use of E-commerce platforms has expanded the opportunities for the marketing and sale of CFSIs. E-commerce platforms are largely laxly regulated and anonymous, designed for rapid and easy transactions with minimal concern for regulation and due diligence.

Sellers can create multiple online storefronts, opening new ones if it becomes apparent to buyers that the goods are counterfeit items. A 2023 case involving a network transferring counterfeit Cisco networking equipment saw a US-based individual run 15 Amazon and 10 eBay storefronts alongside 19 New Jersey and Florida companies.[57] Online stores are also low cost, requiring minimal investment in physical real estate. Marketing CFSIs online can even involve the use of descriptions, specifications and images of the authentic products that have been counterfeited. In short, the availability of the E-commerce option makes the job of deception easier in multiple ways (see Boxes 2 and 6).

The growth of E-commerce platforms has far outstripped the growth of other retail sales in recent years. Between 2018 and 2020, E-commerce sales grew by 41% in 'major economies', whereas regular retail sales grew by just 1%.[58] In 2019 E-commerce was estimated to account for US$26.7 trillion or around 30% of global GDP.[59] The OECD notes that in 2020 there were between 12 and 24 million E-commerce sites.[60] Such a large amount of trade allows those marketing CFSIs to easily blend in and avoid scrutiny among legitimate traders.

The link between E-commerce platforms and CFSIs has been identified by the OECD, which noted in 2018: 'E-commerce platforms represent ideal storefronts for counterfeits and provide powerful platform[s] for counterfeiters and pirates to engage large numbers of potential consumers.'[61] In a more recent 2021 report, the OECD noted 'positive and statistically significant correlation between the indicators of e-commerce activity in an economy, and imports of counterfeits to that economy.'[62] Others, such as the US DHS, have also noted the relationship: 'While the expansion of e-commerce has led to greater trade facilitation, its overall growth— especially the growth of certain related business models—has facilitated online trafficking in counterfeit and pirated goods.'[63]

While many of the counterfeit goods sold through E-commerce platforms are targeted at consumers, there is potential for goods relevant to the nuclear industry to be sold through these platforms. The OECD notes that electrical machinery and equipment accounted for 7% of EU detentions of counterfeits linked to E-commerce between 2017 and 2019.[64] Furthermore, there is ample evidence of goods subject to dual-use export control as well as tactical gear being sold through similar online platforms.[65]

3.2 Transfer to the Customers

The transfer of goods to the markets – either as a result of sale to a customer or as part of a transfer to intermediaries towards these markets – typically uses complex routings. In part this is a product of the complex nature of 21st century global trade flows. The deliberate use of complex shipping routes is a modus operandi of those seeking to launder goods, falsify documentation and make it more difficult to distinguish CFSIs from the genuine article.[66] As the OECD-EUIPO has noted, 'Counterfeit and pirated products continue to follow complex trading routes, misusing a set of intermediary transit points.'[67] These complex routes themselves act as a means of deception, making it more difficult for customs authorities and law enforcement to track the trade, and complicating any efforts to counter it.

In particular, the deliberate use of multiple transhipment or transit jurisdictions is a tactic used by those disseminating CFSIs. Goods transiting or being transhipped through multiple jurisdictions provides opportunities for the falsification of documentation and allows for minimal scrutiny by the authorities in these jurisdictions. As the OECD-EUIPO notes, the incentives for use of transshipment hubs includes 'the ability to camouflage the original point of departure, to establish distribution centers for counterfeit and pirated goods, and to repackage or re-label items.'[68]

Many of the key transshipment economies allegedly act as distribution hubs for CFSIs. These are often states with several characteristics – including large shipping hubs or ports and a lax regulatory environment to facilitate transshipment trade.[69] Many of these hubs are global nodes in international shipping networks – such as Hong Kong, Singapore and the UAE.[70] There are also more localised hubs that are used by these networks to serve certain markets – as the OECD notes:

[S]everal Middle Eastern economies (eg Saudi Arabia, the United Arab Emirates and Yemen) are important transit points for sending fake goods to Africa. Four transit points – Albania, Egypt, Morocco and Ukraine – are of particular significance for redistributing fakes destined for the EU. Finally, Panama is an important transit point for fakes on their way to the United States.[71]

The Role of Free Trade Zones

In these transshipment hubs, goods are often moved into FTZs where they are prepared for shipment on to the target markets in the smaller shipment modes discussed below. As the OECD-EUIPO has noted, 'Many of these transit economies host large free trade zones that are important hubs of international trade.'[72] Facilities in FTZs may also be used to manipulate goods – such as to conduct basic assembly or remarking.

FTZs are areas with more limited regulation as they are designed to facilitate trade and investment. FTZs are numerous and located in many countries around the world. In certain situations, they can account for significant proportions of national trade. For example, the Jebel Ali FTZ in the UAE – the world's largest FTZ – hosts 8,700 companies, including over 100 Fortune Global 500 companies, from over 130 countries, and provides 130,000 jobs.[73]

As of 2017 it accounted for more than 32% of the UAE's foreign direct investment and as of 2024 still accounts for almost a quarter.[74]

FTZs through lax regulation and oversight – as well as attracting many legitimate businesses – attract much illicit activity. The Financial Action Task Force (FATF) has noted the prevalence of fraud, money laundering and smuggling in and through FTZs.[75] Free Trade Zones have also been prevalent in the illicit transfer of strategic and dual-use commodities to weapons of mass destruction (WMD) programmes – including nuclear programmes.[76]

A 2018 OECD-EUIPO study noted that on average, the share of counterfeit products in exports from jurisdictions without FTZs is 50% lower than those with FTZs.[77] According to the report, 'Lightly regulated zones can be particularly attractive to parties engaged in illegal and criminal activities... many Free Trade Zones frequently feature among the list of transit points in illicit trade, including trade in counterfeit and pirated goods.'[78]

Use of Small Parcels

Small parcels – alongside E-Commerce – have also emerged as a prominent means for transferring CFSIs to the market and the customer, their use expanding recently in CFSI supply chains. As a 2019 OECD-EUIPO report notes, the use of small parcels sent by post and express services is growing. They are 'a way for criminals to reduce the chance of detection and minimise the risk of sanctions,' with smaller shipments raising the costs of checks and detention by customs bodies.[79] They also make seizures smaller and less costly for those seeking to transfer CFSIs.[80]

Of seizures of goods reported by World Customs Organization (WCO) members in 2022, 78% of them were of counterfeit goods transported by mail, although these only accounted for 5% of seizures by quantity, with larger interdictions accounting for the vast majority of the goods seized.[81] Similarly high rates of small parcel use were identified by others: 76% of fake goods intercepted by the EU in 2017 were courier or postal small shipments, and seizures in the US involving mail and express services 'were close to 90%' in the years running up to 2018.[82]

Entities disseminating CFSIs have become effective at evading postal checks. They have developed 'drop shipping' methods, 'using stickers/stamps from international postal services to give the impression that shipments have come from another EU member state, when in fact they may have arrived from Thailand or India.'[83] Such entities also conduct large imports into EU member states with lesser controls and then redirect the packages to other EU member states using an EU postal stamp or sticker. [84] Use of small parcels to move CFSIs has also been linked to the rise of E-commerce. As the OECD-EUIPO has noted, 'For criminals running illicit trade networks, small parcels sent by post become an attractive way of fulfilment of on-line transaction.'[85]

3.3 Target Markets

Once the CFSIs enter the target market jurisdictions they can either be transferred directly to the customer or can be subject to further manipulation and marketed there. Reporting tends to focus on economies where companies whose IP is being stolen are located, rather than the markets where CFSIs are being sold. As the OECD-EUIPO has noted,

The companies suffering from counterfeiting and piracy continue to be primarily registered in OECD countries; mainly in the United States, France, Switzerland, Italy, Germany, Japan, Korea and the United Kingdom. However, a growing number of companies registered in high-income non-member economies, such as Singapore and Hong-Kong, China, are becoming targets. In addition, a rising number of rights holders threatened by counterfeiting are registered in Brazil, China and other emerging economies.[86]

With regard to CFSIs that might jeopardise nuclear security, the customers of concern are located in countries hosting nuclear industries.

Distributors, Manipulation and Fraud in the Target Market

Distributors – both witting and unwitting to the fact that they are offering CFSIs – may help to provide CFSIs with access to the target markets. This is a particular issue for customers involved in more sensitive defence and critical infrastructure industries who benefit from dealing with domestic rather than overseas suppliers.

As a *Bloomberg* report about counterfeit chips in the US defence supply chain during the 1990s noted, changing requirements created by the Pentagon included those that encouraged the military to favour suppliers that qualified as 'disadvantaged'; and those that stopped requiring government contractors to certify that they were either original manufacturers or authorized distributors. As a result, a great number of smaller and informal distributors were able to enter the supply chains.[87] A 2012 US Senate report into counterfeit parts in the US defence supply chain noted that 80% of the 1,800 cases (involving over a million parts) identified were sourced from distributors with a presence in the US.[88]

In some cases, the point in the supply chain where the deception occurs is within the target market itself. This would involve suppliers remarking or selling goods as if they are higher-grade, more capable or higher-quality versions. This has particularly been seen among unscrupulous smaller companies selling security equipment. For example, there have been cases of US-based companies supplying the US government with bullet proof vests that is Chinese manufactured and relabelled as being manufactured elsewhere.[89]

Customers and End-Users of CSFIs

The end users of CFSIs that are unaware of the true nature of these goods may purchase the CFSIs themselves or may purchase goods such as electronics that include counterfeit components. Several factors might make organisations more vulnerable to accepting CFSIs (see Box 7).

Box 7. What Factors Make Organisations More Susceptible to Accept CFSIs?

- Use a large volume of goods that are frequently counterfeited
- Weak management and oversight structures
- Weak organisational culture and ethics
- Poor or non-existent training on CFSI risks
- Weak procurement function
- Weak receiving inspection function
- Weak checks to counter bribery and corruption
- Weak quality assurance, quality control, audit and inspection

Insider threats could potentially be present at the manufacturing stage (manufacturer stealing discarded products, illegally selling IP or falsifying test results, for example) but could also be present in the customer organisations. Insiders could accept CFSIs to make their job easier in the short term, could receive a financial incentive to do so, could turn a blind eye to obvious red flags, or be ineffective or negligent in conducting due diligence and other checks.

Conclusion

The actors and networks coordinating, facilitating, and profiting from the production, sale and transfer of CFSIs are diverse. They use the legitimate channels, infrastructure and modalities of international trade to run their operations, deception to pass off CFSIs as authentic items, and adapt their operations to continue to profit. This section has provided an overview of the types of goods, products and services that might be most vulnerable to being CFSIs, the types of actors and networks involved, where they are located, and the supply chains that move these goods from producer to the customers.

Those CFSIs that might be found in the nuclear industry – and could jeopardise the nuclear sector, and security in particular – are a much narrower sub-section of the broader CFSIs discussed above. There is particular concern surrounding areas such as electronics (including those in detection and communications equipment), physical protection technology and armed response equipment. The networks producing and transferring these technologies also represent a smaller subset of those involved in broader CFSI production. However, many of the same means of deception and transfer will be seen in these supply chains as those dealing in CFSIs more broadly – including use of complex supply chains, multiple transhipment hubs, FTZs and the extensive use of E-Commerce.

References

1 The report stated, 'This amount does not include domestically produced and consumed counterfeit and pirated products, or pirated digital products being distributed via the Internet.' See OECD and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 11. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

2 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact', 18 April 2016, p. 11. https://www.oecd.org/corruption-integrity/reports/trade-in-counterfeit-and-pirated-goods-9789264252653-en.html

3 From 3,244 seizures per year to 33,810. See US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States', 24 January 2020, p. 4. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods

4 US Government Accountability Office, 'Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market', Report to the Chairman, Committee on Finance, US Senate, GAO-18-216, January 2018, p. 0. https://www.gao.gov/assets/690/689713.pdf

5 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 30. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

6 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 15. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

7 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 31. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

8 Europol, 'Counterfeit and pirated goods get boost from pandemic, new report confirms', 7 March 2022. https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-and-pirated-goods-get-boost-pandemic-new-report-confirms

9 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 30. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

10 US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States', 24 January 2020, p. 20. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods

11 Brian Grow, Chi-Chu Tschang, Cliff Edwards and Brian Burnsed, 'Dangerous Fakes', Bloomberg Businessweek, 1 October 2008. https://www.erai.com/CustomUploads/ca/wp/2008_2_Dangerous_Fakes.pdf

12 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019, p. 4. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

13 US Department of Energy, 'Suspect/Counterfeit Items Resource Handbook', DOE handbook, DOE-HDBK-1221-2016, August 2016. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1989/in89070s1.html

14 This list is an edited version of the slightly different lists found in: US Department of Energy, 'Suspect/Counterfeit Items Resource Handbook', DOE handbook, DOE-HDBK-1221-2016, August 2016, p.41 https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1989/in89070s1.html; and 'Information Notice No. 89-70, Supplement 1: Possible Indications of Misrepresented Vendor Products', US Nuclear Regulatory Commission, 26 April 1990. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1989/in89070s1.html

15 US Department of Energy, 'Suspect/Counterfeit Items Resource Handbook', DOE handbook, DOE-HDBK-1221-2016, August 2016. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/1989/in89070s1.html

16 See the case in World Nuclear Association, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', Supply Chain Working Group report, August 2019, p. 3. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

17 Securex, 'Know the Difference: Real Vs Fake Garrett Handheld Metal Detectors', undated. https://www.securexafrica.com/know-the-difference-original-vs-fake-garrett-handheld-metal-detectors

18 Dominic Evans and Saif Hameed, 'From Beirut to Baghdad, "useless" bomb detectors guard against disaster', Reuters, 27 July 2016. https://www.reuters.com/article/us-mideast-security-detectors-idUSKCN1061VK

19 Icom UK, 'Beware of Counterfeit Icom Products', undated. https://icomuk.co.uk/Beware-of-Counterfeit-Icom-Products/4195/3306

20 Justin Rohrlich, 'How the Navy SEALs wound up buying 450 counterfeit radio antennas', Quartz, 15 January 2020. https://qz.com/1785156/how-the-navy-seals-wound-up-buying-450-counterfeit-radio-antennas

21 US Attorney's Office, East District of Virginia, 'Executives Convicted of Selling Falsely Labeled Body Armor to U.S. Government', Press Release, 8 February 2019. https://www.justice.gov/usao-edva/pr/executives-convicted-selling-falsely-labeled-body-armor-us-government

22 David Hambling, 'New Russian Soldiers Issued Fake Body Armor', Forbes, 19 October 2022. https://www.forbes.com/sites/davidhambling/2022/10/19/new-russian-soldiers-issued-with-fake-body-armor/?sh=343de4614f06

23 Tom Brown, 'Youthful bullet dealer charged with Pentagon fraud', Reuters, 20 June 2008. https://www.reuters.com/article/us-usa-afghan-ammunition/youthful-bullet-dealer-charged-with-pentagon-fraud-idUSN2013214720080620/

24 See for example the Kobe Steel case: US Nuclear Regulatory Commission, 'Quality Assurance Record Falsification at Kobe Steel and other International Vendors', IN 2018-11 S1, 1 December 2020. https://www.nrc.gov/docs/ML1935/ML19357A138.pdf

25 US Nuclear Regulatory Commission, 'Willful Misconduct/Record Falsification and Nuclear Safety Culture', IN 2013-15, 23 August 2013. https://www.nrc.gov/docs/ML1314/ML13142A437.pdf

26 This list is taken from the document, Organisation for Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 17. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html

27 Michael Kenney, Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation (Penn State University Press, 2006).

28 US Government Publishing Office, 'The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain', Hearing before the Committee on Armed Services, US Senate 112th Congress, 8 November 2011. https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm

29 US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States', 24 January 2020, p. 21. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods

30 'The Fake Chip Scourge', The Asianometry Newsletter, 18 April 2023. https://www.asianometry.com/p/how-optical-mems-won-an-oscar-c31

31 'The Fake Chip Scourge', The Asianometry Newsletter, 18 April 2023. https://www.asianometry.com/p/how-optical-mems-won-an-oscar-c31

32 Europol and EU Intellectual Property Office, 'Intellectual Property Crime Threat Assessment 2022', March 2022, p. 34. https://www.europol.europa.eu/publications-events/publications/intellectual-property-crime-threat-assessment-2022

33 US Customs and Border Protection, 'The Truth Behind Counterfeits', 16 May 2023. https://www.cbp.gov/trade/fakegoodsrealdangers

34 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Why Do Countries Export Fakes? The Role of Governance Frameworks, Enforcement and Socio-economic Factors', June 2018, p. 12. https://www.oecd.org/gov/why-do-countries-export-fakes-9789264302464-en.htm

35 US Department of Homeland Security, 'Dangerous Chinese Microelectronics don't always come with Balloons', outreach document prepared for 2023 Public-Private Analytical Exchange Program, 28 September 2023. https://www.dhs.gov/sites/default/files/2023-09/23_0915_oia_CCM_White_Paper_508_final.pdf

36 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Why Do Countries Export Fakes? The Role of Governance Frameworks, Enforcement and Socio-economic Factors', June 2018, p. 11-12. https://www.oecd.org/gov/why-do-countries-export-fakes-9789264302464-en.htm

37 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact', April 2016, p. 81. https://www.oecd.org/en/publications/trade-in-counterfeit-and-pirated-goods_9789264252653-en.html

38 These 10 sectors included: foodstuff; pharmaceuticals; perfumery and cosmetics; leather articles and handbags; clothing and fabrics; footwear, jewellery; electronics and electrical equipment; optical photographic and medical equipment; fake toys, games and sports equipment. Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 17. https://www.oecd.org/corruption-integrity/reports/mapping-the-real-routes-of-trade-in-fake-goods-9789264278349-en.html

39 US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States', 24 January 2020, p. 8. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods

40 US Department of Homeland Security, 'Dangerous Chinese Microelectronics don't always come with Balloons', undated industry briefing material c.2023. https://www.dhs.gov/sites/default/files/2023-09/23_0915_oia_CCM_White_Paper_508_final.pdf

41 Rachel Weiner, 'Contractor promised government U.S.-made body armor, then bought it in China', The Washington Post, 16 November 2021. https://www.washingtonpost.com/local/legal-issues/body-armor-contractor-plea/2021/11/16/3745ad1e-4700-11ec-b05d-3cb9d96eb495_story.html

42 Tom Brown, 'Youthful bullet dealer charged with Pentagon fraud', Reuters, 20 June 2008. https://www.reuters.com/article/us-usa-afghan-ammunition/youthful-bullet-dealer-charged-with-pentagon-fraud-idUSN2013214720080620/

43 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 15. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

44 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 80. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html

45 Daniel Salisbury and Darya Dolzikova, 'Profiting from Proliferation? North Korea's Exports of Missile and Nuclear Technology', RUSI Occasional Paper, December 2023. https://rusi.org/explore-our-research/publications/occasional-papers/profiting-proliferation-north-koreas-exports-missile-and-nuclear-technology

46 Daniel Salisbury and Darya Dolzikova, 'Profiting from Proliferation? North Korea's Exports of Missile and Nuclear Technology', RUSI Occasional Paper, December 2023. https://rusi.org/explore-our-research/publications/occasional-papers/profiting-proliferation-north-koreas-exports-missile-and-nuclear-technology

47 James Pearson and Rozanna Latiff, 'North Korea spy agency runs arms operation out of Malaysia, U.N. says', Reuters, 27 February 2017. https://www.reuters.com/article/idUSKBN1650YE/

48 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019, p. 7. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

49 V Forti, CP Baldé, R Kuehr and G Bel, 'The Global E-waste Monitor 2020: Quantities, flows and the circular economy potential', July 2020, p. 13. https://ewastemonitor.info/wp-content/uploads/2020/11/GEM_2020_def_july1_low.pdf

50 Tim Johnson, 'E-Waste Dump of the World', The Seattle Times, 9 April 2006. https://web.archive.org/web/20160105213950/http://old.seattletimes.com/html/nationworld/2002920133_ewaste09.html

51 Davor Mujezinovic, 'Electronic Waste in Guiyu: A City under Change?', Arcadia, Summer 2019. https://www.environmentandsociety.org/arcadia/electronic-waste-guiyu-city-under-change

52 Basel Action Network, 'Scam Recycling e-Dumping on Asia by US Recyclers', 15 September 2016. https://wiki.ban.org/images/1/12/ScamRecyclingReport-web.pdf

53 Aneesh Raj, Christine Crute, Connie Xiong, Elizabeth Lamb, Julia Murphy and Yan Sun, 'Electronic Waste in China: Regulation vs. Reality', Bass Connections, Duke University, 2019-2020. https://bassconnections.duke.edu/sites/bassconnections.duke.edu/files/site-images/EWasteChinaPolicyBrief.pdf

54 Aneesh Raj, Christine Crute, Connie Xiong, Elizabeth Lamb, Julia Murphy and Yan Sun, 'Electronic Waste in China: Regulation vs. Reality', Bass Connections, Duke University, 2019-2020. https://bassconnections.duke.edu/sites/bassconnections.duke.edu/files/site-images/EWasteChinaPolicyBrief.pdf

55 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 19. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html

56 Stephen Losey and Joe Gould, 'Fake parts: A Pentagon supply chain problem hiding in plain sight', Defense News, 5 December 2022. https://www.defensenews.com/pentagon/2022/12/06/fake-parts-a-pentagon-supply-chain-problem-hiding-in-plain-sight/

57 US Department of Justice, 'CEO of Dozens of Companies Pleads Guilty to Massive Scheme to Traffic in Fraudulent and Counterfeit Cisco Networking Equipment', Press Release, 6 June 2023. https://www.justice.gov/opa/pr/ceo-dozens-companies-pleads-guilty-massive-scheme-traffic-fraudulent-and-counterfeit-cisco

58 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

59 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

60 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

61 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Governance Frameworks to Counter Illicit Trade', March 2018, p. 84. https://doi.org/10.1787/9789264291652-en

62 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

63 US Department of Homeland Security, 'Combating Trafficking in Counterfeit and Pirated Goods: Report to the President of the United States', 24 January 2020, p. 7. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods

64 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

65 Bryan Lee, Margaret Arno and Daniel Salisbury, 'Searching for Illicit Dual Use Items in Online Marketplaces: A Semi-Automated Approach', CNS Occasional Paper, No. 27, April 2017. https://nonproliferation.org/op27-searching-for-illicit-dual-use-items-in-online-marketplaces-a-semi-automated-approach/

66 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 15. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

67 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 11. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

68 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 16. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.htmll

69 Daniel Salisbury, 'Exploring the Use of 'Third Countries' in Proliferation Networks: the case of Malaysia', European Journal of International Security 4(1), 2019, 101-122. https://doi.org/10.1017/eis.2018.11

70 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 15. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

71 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 15. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

72 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 11. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

73 Jebel Ali Free Zone, 'About', undated. jafza.ae/about

74 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 20. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html; Jebel Ali Free Zone, 'About', undated. jafza.ae/about

75 Financial Action Task Force, 'Money Laundering vulnerabilities of Free Trade Zones', FATF Report, March 2010. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingvulnerabilitiesoffreetradezones.html

76 Andrea Viski and Quentin Michel, 'Free Zones and Strategic Trade Controls', Strategic Trade Review 2(3), Autumn 2016. http://www.str.ulg.ac.be/wp-content/uploads/2016/10/Free-Zones-and-Strategic-Trade-Controls.pdf

77 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Why Do Countries Export Fakes? The Role of Governance Frameworks, Enforcement and Socio-economic Factors', June 2018, p. 52. https://www.oecd.org/gov/why-do-countries-export-fakes-9789264302464-en.htm

78 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trade in Counterfeit Goods and Free Trade Zones: Evidence from Recent Trends', 2018. https://read.oecd-ilibrary.org/trade/trade-in-counterfeit-goods-and-free-trade-zones_9789264289550-en#page75

79 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 11. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

80 Organisation For Economic Co-Operation and Development, 'Misuse of E-Commerce for Trade in Counterfeits', undated. https://www.oecd-ilibrary.org/sites/1c04a64e-en/1/3/6/index.html?itemId=/content/publication/1c04a64e-en&_p_=2e70d88e8b4568a334f9b81c73e9cb8e&itemIGO=oecd&itemContentType=book

81 World Customs Organization, 'Illicit Trade report 2022', 2022, p. 187. https://www.wcoomd.org/en/media/newsroom/2023/june/the-world-customs-organization-releases-the-illicit-trade-report-2022.aspx

82 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends', December 2018, p. 13. https://www.oecd.org/corruption-integrity/reports/misuse-of-small-parcels-for-trade-in-counterfeit-goods-9789264307858-en.html

83 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 18. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html

84 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Mapping the Real Routes of Trade in Fake Goods', June 2017, p. 18. https://www.oecd.org/en/publications/mapping-the-real-routes-of-trade-in-fake-goods_9789264278349-en.html

85 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Misuse of E-Commerce for Trade in Counterfeits', October 2021. https://www.oecd-ilibrary.org/sites/1c04a64e-en/index.html?itemId=/content/publication/1c04a64e-en

86 Organisation For Economic Co-Operation and Development and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 12. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

87 Brian Grow, Chi-Chu Tschang, Cliff Edwards and Brian Burnsed, 'Dangerous Fakes', Bloomberg Businessweek, 1 October 2008. https://www.erai.com/CustomUploads/ca/wp/2008_2_Dangerous_Fakes.pdf

88 'Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain', Report of the Committee on Armed Services, US Senate, 21 May 2012, p. 13. https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts

89 Rachel Weiner, 'Contractor promised government U.S.-made body armor, then bought it in China', Washington Post, 16 November 2021. https://www.washingtonpost.com/local/legal-issues/body-armor-contractor-plea/2021/11/16/3745ad1e-4700-11ec-b05d-3cb9d96eb495_story.html; Tom Brown, 'Youthful bullet dealer charged with Pentagon fraud', Reuters, 20 June 2008. https://www.reuters.com/article/us-usa-afghan-ammunition/youthful-bullet-dealer-charged-with-pentagon-fraud-idUSN2013214720080620/

Part III
Case Studies

Cases from the Nuclear Sector

The following section explores a series of detailed case studies exploring CFSI incidents from the nuclear industry, highlighting the different ways counterfeits have made their way into facilities and the security implications of these cases.

Case Study 1: Counterfeit Construction Materials Cause Fire and Outage at the Laguna Verde 2 Power Plant, Mexico

Background Context

Mexico's interest in nuclear energy began in the mid-20th century with the establishment of the National Commission for Nuclear Energy in 1956.[1] Construction of the Laguna Verde Nuclear Power Plant (LVNPP) began on Mexico's eastern coast in 1976 and the two boiling-water reactor units were in commercial operation by 1995.[2]

Today, Laguna Verde is Mexico's sole commercial nuclear power plant (NPP) and as of 2023, accounts for approximately 4.5% of the country's total electricity production.[3] There is interest from government executives in expansion of the nuclear industry in the country, and there have been a series of efforts for industry growth in recent years.

Incident Summary

In 2012, an urgent repair was identified at Laguna Verde Reactor 2, concerning Emergency Diesel Generator (EDG) 2. An EDG is a vital safety aspect of an NPP, the existence of a failsafe, independent power system.[4] EDGs are therefore critical as the main means of supplying onsite emergency electrical power to NPPs and maintaining operability of safety components. In the event of an emergency, these generators supply power to important features like the emergency core cooling system (ECCS) and help mitigate the risk of further escalation.

The generators at LVNPP were equipped to provide fuel for 176 hours and to deal with a loss of offsite power (LOOP) for 72 hours.[5] A fault to an important component like this therefore required timely attention, and so a maintenance repair company was contracted to fix the part on an urgent basis. Shortly after the repair was completed, an event occurred at LVNPP where EDG 2 failed and caught fire. The fire generated a large plume of smoke, leading to the activation of the onsite fire brigade and the triggering of automatic fire protection systems.

When investigators examined the recently repaired EDG 2, they found that the piston pin bearings in the generator had a slightly different design to other installed pin bearings although had the same part number.[6] This raised flags about the potential counterfeit or fraudulent nature of the parts. The subsequent findings revealed that the most likely cause of the fire was the material coating the piston pin bearing within the generator. Pistons are crucial internal components in combustion engines, helping control the immense stress and heat created within generators. Malfunction of this part can lead to excessive damage of the generator, as was seen at Laguna Verde. The piston bearing had silver coating and degradation of this silver damaged the EDG's lubricating veins. The wear from the degrading silver jammed the piston hole and the total loss of lubrication to the power assembly cylinder, damaging the generator and causing the fire.

In this case, the contractor had not necessarily installed the counterfeit part with malicious intention, but the part was urgently acquired and therefore its fraudulent nature had likely gone unnoticed due to the urgency of the repair work taking place. During a refuelling outage at the reactor unit in 2014, further investigation into the abnormal wear of EDG 2's pins found that different materials had been used in the construction of components installed in EDG 1, 2 and 3. The review led to EDGs 1 and 3 being declared inoperable and a 23-day extension to the outage at the reactor unit.

Preventative and Mitigation Measures

Measures were taken by the plant and the Mexican government to help address the issue at hand and to prevent such a case in the future. Following the 2014 outage, a workshop was held to help create an administrative procedure to set up requirements for the detection and mitigation of counterfeit, fraudulent and suspect parts.[7] Developments in recent years have included reports like the 2016 report on Mexico's progress with the Convention of Nuclear Safety, where the Department of Energy in Mexico provided specific details about quality assurance and safety measures it was seeking to implement to ensure better safety standards at its NPP.[8] This included better quality assurance programmes and standards when outsourcing repairs and jobs to maintenance contractors.

A 2022 International Atomic Energy Agency (IAEA) mission to review the safety of long-term operations at the plant was also satisfied with the improvements being made at the LVNPP.[9]

Broader Implications

This case is an important one in highlighting the strict attention to detail that is necessary in the industrial procurement process. The inability to determine where the faulty bearing coating was introduced in the supply chain and the difficulty in classifying items as counterfeit, fraudulent, or non-conforming also reveals improvements needed in knowledge of CFSIs from all stakeholders involved in the nuclear supply chain, be they vendors, maintenance contractors, or plant workers.

The nuclear safety implications of an incident of this nature are significant. EDGs are very important to the overall safety procedure of the plant, and the presence of counterfeit parts, be they intentionally inserted or not, would put a core safety mechanism at risk. The loss of a backup power supply in a LOOP or partial LOOP event puts the plant at risk of not being able to shut down safely and preventing overheating of the core and spent fuel pool, with implications for worker safety as well as financial loss suffered during an outage.

EDG failure also presents a potential nuclear security risk, as losing backup power supply could be exploited by adversarial actors to exacerbate an attack on nuclear facility. If an attack were to be executed and EDGs were unable to come online to restore power to a facility in the wake of an outage, it could exacerbate the impact of the attack and create further vulnerabilities for adversaries to exploit.

Case Study 2: Fraudulent Operational Amplifiers at a Nuclear Facility,[10] Canada

Background Context

Canada began its nuclear power industry with research starting in 1944 in Quebec on a pressurised heavy water reactor (PHWR). In 1952, the Canada's Atomic Energy of Canada (AECL) became a Crown corporation and was given a government mandate to explore and develop peaceful uses of nuclear energy. The country quickly became a global leader in nuclear energy and the AECL oversaw the development of the Canada deuterium uranium (CANDU) reactor, which produces the majority of the global supply of cobalt-60 radioisotopes for medical and sterilisation use.[11]

Today, Canada's 19 operational commercial reactors are responsible for roughly 15% of the country's electricity supply, and Canada is the world's second largest producer of uranium, providing this vital resource in the nuclear industry to nuclear countries across the world.[12] In 2023, Canada signed a joint pledge with 21 other countries to triple its nuclear capacity by 2050, indicating a strong government support for expanding the nuclear industry in the country.[13]

Incident Summary

In January 2007, a Canadian NPP unintentionally purchased 50 counterfeit Burr-Brown operational amplifiers via a third-party supplier. This supplier had bought the amplifiers from a vendor who had acquired them from an unauthorised distributor,[14] meaning the fraudulent items were introduced early in the supply chain and before they reached the plant.

Operational amplifiers are key electrical components that amplify the difference in voltage between two inputs, helping intensify weak electrical signals. In an NPP, they help ensure adequate electrical signals are provided to nuclear control systems. They are a small but crucial component of the wider nuclear system operating within a plant, and therefore it is crucial that they are quality assured and reliable.

Burr-Brown was an American electronics manufacturer that was acquired by Texas Instruments in September 2000, meaning Burr-Brown items were now manufactured and distributed by Texas Instruments. The same month the plant purchased the parts, coincidentally, a letter was issued by Texas Instruments to customers about its electronics. The letter stated that if electronics were not purchased from Texas Instruments' authorised sources, there was no assurance that they would be authentic and legitimate.

Between January and July 2008, five counterfeit and fraudulent operational amplifiers were put into service. In September 2008, workers noticed that one of the amplifiers had failed a safety system test that was conducted every three weeks. The fault occurring was with a neutron overpower amplifier which was tripping at 121.8%, higher than its normal trip point of 119.5%. Neutron overpower amplifiers are used in reactor shutdown systems of CANDU plants and help protect the reactor from loss of regulation (LOR) and loss of coolant (LOCA) accidents. The failure of a safety system test for such a crucial component thus raised concerns. Roughly a month after the failed test, an investigation uncovered that the Burr-Brown operational amplifier was the cause of the failure and was confirmed to be fraudulent.

Preventative and Mitigation Measures

The team at the NPP took a series of preventative measures following the failed safety test that helped them uncover the fraudulent part and deal with the effects. Firstly, they replaced the faulty neutron overpower amplifier in the plant's shutdown system 1 after being unsuccessful in determining why it failed testing and being unable to recalibrate the part.[15] They then followed procedure in documenting the event via its corrective action programme. A subsequent investigation confirmed that the operational amplifier was counterfeit and had contributed to the failed test. The team continued investigating and were able to confirm a total 50 operational amplifiers as CFSIs; they also removed from service the four that were presently installed.

Following immediate actions from the investigation, the NPP took a series of further measures to ensure safety. This included communicating the event to the CANDU Owners Group, and partner groups like the World Association of Nuclear Operators (WANO) and the Institute of Nuclear Power Operations (INPO). They also temporarily removed the third-party supplier from the approved suppliers list to help ensure further CFSIs were not introduced into the supply chain.

Broader Implications

This incident demonstrated the importance of monitoring for CFSIs at all levels of the nuclear supply chain. Although the third-party supplier did not intentionally supply a CFI and the licensee did not purposefully buy fraudulent parts, stakeholders at all stages of the process should be vigilant. Nuclear supplies and materials are vulnerable to forgery by vendors earlier in the process, and this should be recognised and regulated. Canada experienced a similar incident roughly eight years later when materials in valves installed in various Canadian plants were identified as not meeting the required certifications. Here, a third-party steel supplier earlier in the procurement process had altered and populated data for several tests, meaning some materials were not even tested in the first place.[16] This indicated a clear problem in identifying CFSIs earlier in the supply chain that had still not been adequately addressed after the Burr-Brown operational amplifiers incident.

Case Study 3:
Counterfeit Circuit Brakers Across Various Nuclear Power Plants, United States

Background Context

The US is the world's largest producer of nuclear power, accounting for roughly 30% of global nuclear electricity generation.[17] The Atomic Energy Act of 1954 was a pivotal part of early US nuclear power endeavours, later assigning the responsibility of exploring peaceful nuclear energy to the Atomic Energy Commission (AEC). The AEC was abolished in 1974, and independent regulation of the safety and licensing of NPPs and facilities was assigned to the Nuclear Regulatory Commission (NRC). Today, there are 93 reactors in operation and the NRC continues to oversee commercial power plant operations in several ways, including in monitoring CFSIs.

Incident Summary

On three separate instances between 2006 and 2007, the US Consumer Product Safety Commission (CPSC) announced three different firms recalling counterfeit circuit breakers with the label 'Square D'.[18] The first case reported was raised in November 2006 and concerned circuit breakers distributed by Pennsylvanian firm Scott Electric Co., which reported it had supplied roughly 30,000 counterfeit units to distributors nationwide.[19] A similar case was reported in October 2007, when the Washington state-based company Connecticut Electric estimated that about 64,000 counterfeited circuit breakers had been sold across the country and needed to be recalled.[20] Two months later, North American Breaker Company shared that an estimated 50,000 counterfeit Square D breakers had been sold through distributors and retailers between 2003 and 2006 in the US.[21]

Further investigation into the incidents by the NRC showed that it was not just domestic consumers who were at risk from purchase of the counterfeit parts. A purchase database search conducted by the NRC found that three NPPs had purchased Square D circuit breakers during the periods of concern between 2003 and 2006: Catawba NPP, McGuire NPP and Oconee NPP.[22] Upon further investigation, the Oconee and McGuire plants were able to confirm that its breakers were genuine. However, there remained doubt about four breakers at Catawba NPP that could not be confirmed to be legitimate. As a result, Catawba NPP removed these circuit breakers from its stock.[23]

Although were no incidents related to the counterfeit breakers reported, both in nuclear facilities and in the domestic market, the risk associated with these breakers was serious, necessitating their recall and removal. Regarding the counterfeit breakers, there was a risk they might not have the appropriate electric current interrupting capacity required by a breaker to function properly, as well as potentially lacking proper containment features.[24] This could pose a risk as the breakers could fail to trip, potentially causing a fire.[25] The Los Alamos National Laboratory estimated that by 2008, as many as half-a-million counterfeit Square D circuit breakers had entered US markets since 2005.[26]

Preventative and Mitigation Measures

The legitimate firm associated with the product, Square D, launched a series of lawsuits between 2006 and 2008 aimed at stopping the sale and distribution of fraudulent circuit breakers under its trademark. For example, Square D launched a case against Scott Electric, the distributor in the first case mentioned, alleging that they had discovered records that indicated Scott Electric was involved in the counterfeiting process, alongside two other firms.[27]

Square D's parent company, Schneider Electric, also works to raise awareness of counterfeiting in the industry and the violation of trademark rights of Schneider Electric products. They highlight that there have been 189 cases of illegitimate companies in Hong Kong that illegally sell fraudulent parts, impacting the work of Schneider Electric's China branch.[28] In the three instances mentioned in this case study, the counterfeit circuit breakers are believed to have come from China.[29]

Broader Implications

Electronic counterfeiting has become a major source of concern as electronic items are increasingly subject to counterfeiting but difficult to detect. In sensitive sectors, like the nuclear industry, operators are potentially at risk of being targeted for industrial or military espionage.[30] Indeed, there have been allegations made by journalists at *Bloomberg* that spies from the People's Republic of China were supposedly able to gain access to major firms like Apple and Amazon through the alleged insertion of counterfeited chips and integrated circuits into the US supply chain.[31] Although this has been refuted by multiple representatives of the American government and the Chinese government,[32] as well as individuals from the companies involved,[33] it highlights a real concern in industry, government and civil society of the security threat that counterfeited electronic components can pose to critical national infrastructure.

Case Study 4:
Certificate Falsification Scandal Leads to Multiple Reactors Shutting Down, Republic of Korea

Background Context

The Republic of Korea is a prominent nuclear energy producer and the most reactor-dense nation (defined as number of reactors per square mile) in the world.[34] As of 2024, there are 26 operating nuclear reactors located primarily in the south and southeast of the country and they supply roughly a third of Korea's electricity.[35] The Republic of Korea is also working in partnership with other states and exporting nuclear power technology to its allies, with primary areas of cooperation including nuclear research and development (R&D), safeguards, emergency preparedness and safety measures.[36]

Incident Summary

In April 2012, the Korea Hydro & Nuclear Power (KHNP) Company, one of the country's largest operators, received an anonymous tip-off about the fraudulent quality of parts at Korean NPPs.[37] A subsequent investigation completed in November 2012 found that between 2003 and 2012, eight suppliers had sold the company a total of 7,682 items with fraudulent quality assurance certificates.[38] Findings by the Korea Institute for Nuclear Safety revealed that 2,114 test certificates had been falsified during this timeframe by equipment manufacturers and material suppliers. In addition, 2.3% of all environment and seismic equipment documentation had been forged between 1996 and 2012; they also found that 3,461 reports were unclear or unverifiable, and therefore treated as suspicious.[39]

The parts involved were primarily commercial grade items, such as fuses, diodes and relays, and the Korean authorities maintained that they did not pose a risk of causing a safety incident at the plants where they were present.[40] However, the scope and frequency of these parts within multiple plants raised serious concern about potential further risks.

KHNP was able to determine that most parts were installed at the Hanbit NPP, at units 5 and 6, with the rest at Hanbit units 3 and 4, and at unit 3 of Hanul NPP.[41] The reactor units at Hanbit were taken offline while the parts were replaced. After a thorough investigation, all the affected plants were allowed to restart in January 2013.

However, in May 2013, the Korean Nuclear Safety and Security Commission (NSSC) identified further falsifications in six different reactor units. This time, the equipment qualification certificates of control cables at units 1-4 of the Shin-Kori NPP and units 1 and 2 of the Shin-Wolsong NPP were falsified. These incidents raised further concern as they were safety-related components that were crucial in the event of a severe incident. Control cables provide control for important aspects of the plant like primary pumps, ventilation, safety valves, waste treatment, and various other functions. The potential failure of these items was therefore incredibly dangerous and required immediate attention and investigation.

Perpetrator Spotlight:

JS Cable, Saehan TEP and Falsified Cables (2013)

JS Cable, headquartered in the South Korean city of Cheonan, was the supplier of the cable installed in the four Korean NPPs identified in May 2013. They had won a contract with the KHNP in 2004 and were the first domestic firm to supply this part to a Korean NPP. JS Cable was awarded the contract on the condition that they would meet certain standards requirements, but they reportedly did not actually possess the capability to manufacture the part to these required specifications.[42]

JS Cable was also required to have the cables tested, obtain an official test report, and to have this report verified by the Korean Electric Power Company (KEPCO) before it was sent to the KHNP. JS Cable decided to outsource testing to a private testing firm, Saehan Total Engineering Provider (TEP), and sent the samples for tests, including loss of coolant accident (LOCA) testing. Saehan reportedly did not have the means to conduct LOCA testing, so it passed on the samples to Canadian company TCMT. Of the six samples tested, only one passed – which, according to Korean quality standards, meant the cable could not be used at the plants. During a second round of testing, JS Cable and Saehan TEP allegedly sent TCMT two illegitimate samples, but these still did not pass testing standards.[43]

After multiple failed tests, the companies sent their findings to KEPCO, the country's largest electric utility company, which notified the KHNP. Instead of revoking the contact, managers at KHNP reportedly worked with KEPCO engineers and management at JS Cable and Saehan TEP to allegedly falsify testing reports and claim that all samples had passed testing. JS Cable supplied the first shipment of the reportedly fraudulent cable in February 2008, and continued to sell the cable for several years, earning roughly US$18 million in income.[44]

In response, KHNP immediately shut down the relevant plants to replace the affected parts. The investigation was expansive, with all safety related items purchased within the past six years in 23 operating reactor units and eight under construction investigated. Additionally, all Korean NPP equipment qualifications certificates were investigated to check for further inconsistencies. Following the completion of the investigation, six nuclear engineers and equipment suppliers were arrested and 100 people indicted on corruption charges.[45] The NSSC gave permission for plants to restart operations from January 2014, and began implementing measures to ensure an oversight of this nature would be avoided in the future.[46]

Preventative and Mitigation Measures

Given that these incidents occurred in the aftermath of the 2011 Fukushima Daiichi accident in Japan, Korean officials ensured these findings were given the utmost attention and dealt with swiftly. Fukushima had demonstrated to the global nuclear community the dangers of safety features being inoperable at a NPP, and how the inability to sufficiently cool and shut a reactor can have devastating consequences. The KHNP was incredibly thorough in its investigations, and keen to ensure that no part went unchecked in the effort to uncover CFSIs. In its 2013 investigation, all safety-related items were tested for falsified certificates.[47] Those with certificates that could be proven to be forged were immediately replaced or retested for integrity and any items with untraceable certificates were assumed to be falsified.

Throughout the investigation and in its aftermath, the Korean NSSC has been maintained transparency about CFSIs and inconsistencies it has identified, regularly releasing press statements and reports via its website.

The NSSC also initiated independent and specialised reviews into the matter to identify problems and solutions around forged documents and the wider presence of CFSIs in the Korean nuclear supply chain. In addition, the NSSC established a nuclear safety ombudsman to whom anyone witnessing misconduct can anonymously report an incident.[48] These public efforts towards a strong and transparent safety culture in quality and procurement activities display commitment to combatting challenges in the nuclear supply chain.

Broader Implications

This case raised several important points relevant to nuclear security. The immediate impact on the Republic of Korea's energy industry was immense. The country's 23 nuclear power reactors provide roughly one-third of its energy supply, making it heavily reliant on the continued operation of these plants.[49] Yet, in fact, the incidents were indicative of a wider problem with safety culture at the time identified by both the IAEA and NSSC. On 9 February 2012, two months before the anonymous tip-off, Shin Kori reactor unit 1 experienced a station blackout. A subsequent IAEA mission found wider issues with safety culture and internal oversight powers that contributed to the event.[50]

The revelations also shed light on the presence of corruption, clientelism and nepotism in the Korean nuclear industry at the time. The indictments of 100 people revealed schemes including allegations against KHNP executives for taking bribes in exchange for awarding key contracts to various firms.[51] Clearly this is an issue that is not limited to the Republic of Korea and has been identified by academics as a global issue affecting the nuclear industry in numerous countries. Richard Tanter, for example, reports that between 2012 and mid-2013, every major nuclear power seeking to export rector technology experienced a major corruption incident in their respective nuclear power sectors, including Canada, Russia and the US.[52] The World Nuclear Industry Status Report 2021 also highlighted a concerning trend between corruption and collusion, and the introduction of counterfeit parts in the nuclear supply chain.[53] The Republic of Korea took steps in the wake of the incident to address this misconduct, but the widening of the investigation in 2014 demonstrated that this issue would take time to address.[54]

The incidents also highlighted why testing is crucial for nuclear components, and why forgery of test results and CFSIs should be addressed in a timely manner. The NSSC found several instances of fraudulent seismic qualification reports for parts installed at Shin Kori units 1-4 and Shin Wolsong units 1 and 2.[55] The company responsible had allegedly modified the results of seismic testing of six items, including an air cleaning unit and electronic duct heater. Seismic testing is used to ensure equipment can withstand an earthquake and other seismic events and is thus a crucial test to conduct in a system as critical as an NPP. With the recent 2011 Fukushima Daiichi accident demonstrating just how dangerous earthquakes can be to plant operations, this is a prime example of the danger that CFSIs pose to both nuclear safety and security.

Case Study 5:
Falsified Parts at the Creusot Forge Impacts Multiple Nuclear Power Plants, France

Background Context

Nuclear is a key component of France's energy sector, with roughly 70% of the country's electricity coming from 56 nuclear reactors.[56] The country is highly active in developing nuclear technology and French firms Électricité de France (EDF) and Framatome (formerly Areva NP) are the leading national firms in this endeavour. France is also a global leader in heavy engineering expertise, and firms like Framatome design and assemble nuclear system equipment for plants all over the world, having produced over 10,000 components since 1970.[57] France is also very active in nuclear technology exports and has supplied reactor technology to nations like China and the Republic of Korea.

Incident Summary

In March 2015, the French Nuclear Safety Authority (ASN) revealed that they had been informed by Areva (now Framatome) of an anomaly detected in the steel composition of parts in certain zones of the reactor vessel head and reactor vessel bottom head of the new European pressurised reactor (EPR) under construction at the Flamanville Nuclear Power Plant.[58] ASN also disclosed that, a few months earlier, Areva had carried out chemical and mechanical tests on a vessel head similar to that at Flamanville, as per regulation requirements. The results of the tests indicated that there was a zone in the vessel head where a high carbon concentration was detected, leading to lower-than-expected mechanical toughness readings. When cross-checked with the reactor vessel head and bottom head at the EPR unit, Areva discovered a similar anomaly. Areva thus petitioned ASN in 2015 for a detailed testing campaign to investigate further.

As part of the wider investigation, Areva began a series of quality reviews on its manufacturing work, particularly at the Creusot Forge, where the EPR vessel head had been manufactured and welded. It was during these reviews that Areva uncovered irregularities in manufacturing checks at the forge.[59]

Areva's initial investigation reviewed practices dating back to 2010, but ASN thought this insufficient and asked the firm to investigate back to 2004, when the first parts for Flamanville EPR were manufactured. The checks revealed inconsistencies in manufacturing check records on roughly 400 parts produced at the forge since 1965.

By 20 June 2016, 22 reactors across France had been impacted by the irregularities, with Fessenheim NPP reactor 2 shut down because of investigation and following confirmation of fraudulent forging process concerning its steam generator.[60] Areva was ordered to halt operations at the Creusot Forge while the investigation into the anomalies continued. By December 2016, 20 French rectors were offline, and investigators suspected that over half of France's NPPs were impacted by the anomalous carbon reading.[61] Concerns were heightened by the fact that Areva and Creusot Forge supply parts to NPPs outside of France, and therefore plants in other countries with French components were potentially also at risk.

In March 2017, crucial information associated with the case was uncovered by French radio channel France Inter. The station published a series of letters between ASN, EDF and Areva which suggested that ASN had allegedly been voicing concerns about potential misconduct at Creusot Forge since 2005.[62] This was highly consequential as it could demonstrate that EDF and Areva were reportedly aware that the forge could be producing defective or substandard parts but allegedly took little action to address this. A few weeks later, in the interest of transparency around the case, ASN published a series of its correspondence with EDF and Areva regarding the forge, as well as dates and details of previous inspections by ASN at the forge.[63] The letters showed that previous inspections had noted a range of issues at the plant, including outdated metallurgical knowledge, numerous deficiencies detected in products, and continuing issues despite EDF and Areva allegedly implementing recommendations from ASN.[64]

After almost two years of thorough investigating, Areva NP informed ASN that they intended to resume operations at Creusot Forge on nuclear pressure equipment components for French basis nuclear installations (BNI) sites.[65] After negotiations with ASN, operations resumed and following a comprehensive investigation by ASN, all reactors were cleared to operate online once more.

Preventative and Mitigation Measures

The ASN launched a detailed investigation into Creusot Forge and the wider French nuclear industry, while also taking several important and proactive measures to ensure the safety of the plants, plant workers, the French public and the environment. The French nuclear authority also prompted firms like Areva NP to take additional measures when they deemed that not enough work had been done to address a particular issue. For example, upon discovery that the problem may be more widespread that initially feared, the ASN widened the scope of the inquiry and requested that Areva expand its records search back to 2004. The ASN also published frequent press releases and reports on it work, demonstrating a commitment to transparency and keeping the public informed of the ongoing work being done to ensure French NPPs were safe. Other measures included a public inquiry at the end of the investigation to determine local responses to the ASN, Areva and EDF's actions, and what could be done to improve the nuclear industry's service to the public.[66]

ASN also highlighted that the feasibility of certain checks could not be confirmed, and therefore additional action needed to take place in the interest of nuclear safety. The organisation ruled that due to the difficulty in conducting checks, the current closure head at Flamanville EPR should be replaced by the end of 2024.[67] After a request by EDF to extend this lifecycle and the authorisation of the commissioning of the EPR, the ASN conceded that the vessel head be replaced after the end of the first operating cycle, extending this timeframe by up to 18 months and making replacement more likely to be carried out in 2026-2027 based on the current timeline.[68]

Due to the fact that the forge also produced parts for a number of plants around the world, a multinational inspection took place between 28th November and 2nd December 2016.[69] This was carried out by the UK, US, China, Canada and Finland. The report revealed some alarming findings, including cases of alleged certificate falsification by employees as recent as September 2016, when the forge was already being scrutinised and under investigation. This particular incident was also reportedly missed by onsite inspectors from Areva and EDF, and only discovered during the multilateral investigation.[70] The group issued a series of recommendations to improve safety culture, oversight and quality management at the plant, with these aspects to be monitored at future inspections by ASN, EDF and Areva.

Broader Implications

This case highlights the need for better oversight of CFSIs at the manufacturing level, not just of items counterfeited later in the supply chain. As seen with other case studies in this handbook, CFSIs can be introduced early in the procurement process and, although procured from legitimate firms and actors, they may still potentially be deficient. The situation is made more complicated in instances where parts are also supplied to plants in different countries. As such, the various countries affected may need to launch their own investigations in their respective nuclear sectors. Adequate information sharing, transparency and communication between nuclear stakeholders is key to help eliminate the uncertainty created in these situations.

This incident also highlights the importance of through industry-wide testing and communication about CFSIs between stakeholders. The initial report into anomalies concerned one type of component in a plant, the reactor vessel, but wider investigation into CFSIs revealed problems with a range of other items including steam generators.

Case Study 6:
Falsified Data of Mixed Oxide (MOX) Fuel Pellets from Sellafield Has International Repercussions, United Kingdom

Background Context

The UK has a well-established domestic civil nuclear system that dates back to the mid-1950s and oversaw the establishment of the world's first civil nuclear programme.[71] The first NPPs in the UK were Magnox reactors, which began operation in 1956 (Calder Hall) and 1959 (Chapelcross). All 26 Magnox reactors established in the mid-20th century have now been decommissioned and many of the UK's reactors have been permanently shut down.[72] Today, nine reactors remain in operation with two under construction in partnership with French firm EDF, with the British government looking to expand domestic nuclear generation fourfold by 2050.[73]

Some of these reactors, such as the now decommissioned Calder Hall reactors and Windscale Piles, were located at larger multi-function nuclear sites, like Sellafield. Though power generation no longer occurs at Sellafield, the plant's primary function is now the processing, storage and disposal of spent fuel.[74] Several parties however, including the Office for Nuclear Regulation (ONR), have expressed concerns about the plant's operations. In 2022, the ONR allegedly classified the plant's Magnox Swarf Storage Silo as 'an intolerable risk',[75] and published a strategy in 2020 for managing risk at the site.[76]

Incident Summary

One of the industrial processes that took place at the Sellafield site was nuclear fuel production, with British Nuclear Fuels plc (BNFL) producing mixed oxide (MOX) fuel onsite. MOX is a mixture of uranium and plutonium oxides that is used in nuclear reactors; in contrast, conventional nuclear fuel typically contains just uranium oxide. MOX is produced by milling the oxide powders together and pressing them into cylindrical pellets. These pellets are fired to make them hard and then loaded into zirconium alloy tubes which are sealed to make fuel rods.

Although produced in the UK, MOX was primarily aimed to be used at non-British NPPs, and exported to plants in Germany, Belgium, France, Japan, Switzerland, and Russia, to name a few destinations.[77]

In August 1999, a member of the quality control team at the Sellafield MOX plant noticed that multiple batches of MOX fuel pellets had similar quality control data readings.[78] This observation was raised with plant management and, a few days later, a process worker at the plant admitted falsifying data, while a second worker admitted being aware that falsification was taking place. This final stage of manually inputting quality assurance data had occurred after the first two stages of checking: first, pellets were measured with an automatic laser micrometre to ensure they were the correct size; and second, those that passed this check then underwent visual inspection.[79] Roughly 5% of pellets that pass these first two stages were then randomly picked for manual measurement by plant workers, who then logged the readings onto a spreadsheet – and this is where the falsification allegedly occurred.

Shortly after the testimonies by the workers, BNFL suspended operations at the plant, and agreed with the Nuclear Installations Inspectorate (NII) that it would not re-open the plant without prior notification to the NII. The NII was an early precursor to the present-day ONR and formed part of the Health and Safety Executive's Nuclear Directorate, which was later merged with the Department of Transport's Radioactive Materials Transport Team to form the ONR. The NII conducted a thorough investigation and on 18 February 2000 published a series of reports about wider safety culture issues at Sellafield, which included the report on the MOX falsification issue. The NII report confirmed that some of the data had been copied from previous spreadsheets and the majority of those on shift for this task were allegedly involved. The NII found 22 lots of falsified data, with one lot relating to approximately 200 pellets, as well as four more lots of suspected incidents.[80]

Although the NII eventually determined that the falsifications had no impact on safety of the fuel, the incident impacted the perception of BNFL's MOX operations. BNFL MOX was shipped to a number of plants across the globe, including a batch of MOX that had been shipped to Japan around a month before the discrepancies were first flagged.

Measures taken by other countries as a result of the disclosure included the German Unterweser Nuclear Power Plant shutting down so that its fuel rods could be replaced, Japanese customers halting business with BNFL, and the German government banning supplies of MOX from BNFL.[81]

Preventative and Mitigation Measures

In addition to the alleged malpractice at the company, the incident highlighted shortcomings in the UK's industry regulations, as the NII gave did not prioritise quality assurance for MOX fuel and rather viewed it as an issue between the BNFL and its customers. The NII did get involved in investigating, however, when it became clear that the incident could have implications for the safe operation of the plant, being a breach of Nuclear Site License requirements. The NII's report was part of a wider investigation by the inspectorate concerning safety culture at Sellafield.

In response to the report, BNFL introduced a series of measures to try and improve operations. The firm's chief executive stepped down shortly after the report was released to the public, and an action plan was implemented for the company. A new Sellafield MOX fuel plant was completed in 2001 but ceased operations in 2011 following a loss of orders from its Japanese customer base as a result of the Fukushima Daiichi disaster.[82]

Broader Implications

This case highlights the criticality of safety culture in nuclear systems, and how a variety of human factors, such as complacency, can have serious impacts. Human factors were highly significant in this case. As was revealed by the investigation, the motivation for falsification was due in part to poor workstation design, the monotony of the job, and disjointedness of the process; these factors all impacted the workers who allegedly falsified the data. In addition, management appeared not to exercise sufficient oversight of the process and were allegedly more concerned with productivity than accuracy.[83] In this sense, the fault was not with a malicious actor, but instead a wider organisational culture of complacency and lack of oversight.

Case Study 7: Company Head Sells Counterfeit Turbine Vibrometers Bound for Multiple Nuclear Power Plants, Russian Federation

Background Context

The Russian Federation has a long history of nuclear power production, with the then-Soviet Union's Obninsk NPP being the first in the world to produce electricity when it came online in 1954.[84] The building of further nuclear reactors and NPPs meant that by my mid-1980s, the Soviet Union had 25 reactors in operation. The Soviet nuclear industry faced a significant drawback shortly after this however with the accident at Chernobyl Nuclear Power Plant in 1986, prompting a reorganisation of the Ministry of Atomic Energy and restructuring of the country's civil nuclear regulatory bodies.[85]

Today, the State Atomic Energy Corporation (Rosatom) oversees the Russian nuclear industry and the operation of 36 reactor units at 11 different NPPs across the country.[86] In addition, Rosatom oversees the exportation of reactor units and civil nuclear energy technology to various nations including Iran, China, India and Bangladesh.[87]

Incident Summary

The perpetrator of the incident was Alexander Murach, the former deputy head of the testing department at the Research Institute for Complex Testing of Optoelectronic Devices and Systems (NIIKI OEP) in St. Petersburg, Russia.[88] Murach also created his own company, Informtech, through which he supplied NPPs and other energy power stations with various parts and devices.[89] In May 2007, Murach entered into a contract with the Leningrad Metal Plant,[90] a flagship turbine producer in Russia. The agreement stated that Murach would supply the metal plant with three vibrometers, at a total cost of 1.48 million rubles.[91] The vibrometers are crucial pieces of equipment used to measure the vibration in NPP turbines, which helps ensure that they are not at risk of breaking and potentially damaging other equipment.

However, Informtech did not have the facilities nor license to manufacture such equipment, so Murach reportedly created false quality assurance certificates and test results to create the illusion that the vibrometers were legitimate items.[92] The profit generated by Informtech from the counterfeiting was worth approximately US$49,000.[93]

When the falsification was discovered, a court in the Leningrad region sentenced Murach to three years of prison time for knowingly selling fraudulent parts bound for NPPs.[94] Leningrad Metal Plant's parent company Power Machines reportedly suffered damages of over 1.4 million rubles as a result of the incident, and the vibrometers involved were decommissioned before being seized by law enforcement.[95]

Preventative and Mitigating Measures

Alexander Murach and Informtech were sentenced in a criminal case due to the severity of the crime and made to pay for the damages by supplying Power Machines with new, legitimate measuring equipment that had undergone testing and had the appropriate certification.[96]

Broader Implications

This case highlights the danger of CFSIs entering the nuclear supply chain at an early stage. Power Machines is a legitimate firm that provides genuine equipment for NPPs; it is Russia's largest producer of electrical equipment for the energy industry and has supplied parts to 57 countries around the world.[97] Informtech was a supplier that was able to impact the procurement chain early on; had the fraudulent parts not been noticed, they could have been installed in NPPs across Russia, and perhaps the world.

The consequences of this incident for plant safety are potentially very serious, as turbine malfunctions can cause significant accidents. An example of this was the 1993 fire at Narora Atomic Power Plant in Uttar Pradesh state, India. The fire began when two blades in the turbine generator of Unit 1 snapped due to accumulated stress, cutting through the remaining blades in the generator. The rotor system began to vibrate excessively, and a fire broke out in the plant's turbine room, cutting off electric supply to the reactors cooling system, as well as burning the cables for the backup power supply.[98]

Without adequate cooling, the temperature in the core would have overheated, leading to potential meltdown. Fortunately, a group of plant engineers were able to pour boron solution into the reactor before this could occur.[99] If a fraudulent vibrometer is installed in an NPP, it may fail to record any irregular vibrations that could be a sign of the turbine being on the verge of a malfunction. The potential for such a serious accident highlights the importance of ensuring that equipment meets quality controls.

Case Study 8: Misconduct and Certificate Falsification Causes Fire Detection Equipment Approval to be Revoked, Japan

Background Context

Japan's nuclear industry is well established, with the country's commitment to the peaceful development of atomic energy inaugurated in 1955 with the Atomic Energy Basic Law.[100] Japan has 33 nuclear reactors that are classed as 'operational', but only 10 are online, with 23 in suspended operation due to changes to plant regulatory requirements by the Nuclear Regulation Authority (NRA) in 2013.[101] Regulations and laws surrounding equipment and quality assurance at Japanese NPPs are incredibly strict, as a result of the 2011 Fukushima Daiichi accident. The accident caused a sharp downturn in nuclear power production as all plants across the country shut down, and the first to reopen after the disaster did so in 2015.[102]

Incident Summary

On 31 March 2022, a statement by Tokyo Electric Power Company (TEPCO) revealed that Fenwal Controls of Japan, a company that primarily produces fire protection technology, had been providing customers with fraudulent equipment.[103] Fenwal produces a series of fire safety equipment, including waterproof sensors that monitor temperatures to look for signs of fire outbreak. An internal investigation revealed that 9,633 units of such equipment supplied to customers between September 2013 and October 2020 did not pass conformity and quality assurance tests.[104] The equipment in question was created using parts that did not meet regulations set by the Japan Fire Protection Certification Association, and it was allegedly that test results had fraudulently been reported by the company.[105] The specific products impacted included fixed temperature spot type sensors (both waterproof and non-waterproof) and repeaters used for fire detection and contact monitoring.[106]

Many of the parts had been installed at nuclear power stations across Japan, with reportedly approximately 60% of the products (6,055 parts) installed at NPPs under the operation of TEPCO and Kyushu Electric Power Company. It is believed that 3,595 of the products were at the Kashiwazaki-Kariwa Nuclear Power Plant, 2,030 at the Genkai Nuclear Power Plant, and 430 at Fukushima's No. 1 unit.[107]

A source reported to *The Asahi Shimbun*, a Japanese newspaper, that the misconduct came in the wake of the Fukushima Daiichi accident, which had reduced confidence in the nuclear industry and led to the strengthening of measures at nuclear facilities across Japan, including fire prevention measures.[108] This allegedly impacted Fenwall's business, leading them to take these measures in an attempt to drive sales.[109] Internal investigation at Fenwal instead attributed the misconduct to inadequate understanding of the Fire Services Act and lack of internal checking.[110]

Preventative and Mitigating Measures

The Japan Fire Equipment Inspection Institute and Ministry of Internal Affairs both acted swiftly following the discovery of the misconduct. The institute, for the first time in its history, revoked its approval of a fire detection product and removed the passing grades it had given to the Fenwal products.[111] In addition, the Japanese Ministry of Internal Affairs' fire and disaster management agency ordered Fenwal Controls to recall all products and replace them. TEPCO took similar measures, announcing on 27 April 2022 that it would replace all affected parts.[112]

In an internal report, Fenwal committed to a number of changes to ensure that such an incident would not occur again. These included better training on legal compliance to ensure all personnel understand the Fire Services Act and other legal instruments, strengthening opportunities for information sharing between departments, and improved internal regulations.[113]

Broader Implications

The issues of misconduct and fraudulent certifications reflect a wider problem of collusion and corruption that can occur within the nuclear or other industries.[114] This is most vividly illustrated by the report of the National Diet of Japan (Japan's parliament) following the accident at Fukushima, which highlighted the organisational and institutional issues that exacerbated the accident.[115]

This report was unprecedented in its criticism of the Japanese nuclear industry,[116] noting the reluctance of regulators, operators and the government to proactively consider updating regulations and policy around nuclear safety.[117] Although the report is not linked to this case, it highlights how underlying weaknesses in culture can lead to the degradation of nuclear safety.

The potential safety and security implications of this case are significant. Faulty fire detection equipment could mean that crew at the station are unaware of a fire somewhere in the plant, and fraudulent transmitters could mean that even if a fire is detected by equipment in the building, it would not be able to relay that information to the relevant personnel. In relation to nuclear security, this could be exploited by malicious actors to set fires and damage plant facilities with operators being unaware. The safety implications of this case are especially salient due to Japan's experience of the 2011 Fukushima disaster, and the subsequent nuclear scepticism that emerged among the Japanese public. CFSI incidents like this could serve to heighten concern about NPPs and potential accidents.

Cases from Other Critical National Infrastructure Sectors

The following section discusses case studies of CFSI infiltration in other critical national infrastructure.[118] These are industries that provide necessary services for a country to function and, consequently, like nuclear, place high importance on safety and security. The cases have been picked to illuminate how other industries are dealing with the issue of CFSIs and if lessons can be applied to the nuclear sector.

Case Study 9: False Quality Assurance and Misconduct at Kobe Steel, Japan

Background Context

Kobe Steel is one of Japan's oldest industrial firms. It was established in 1905 in the Japanese port city of Kobe. Kobe Steel manufactures, produces and sells iron and steel to a range of multinational companies in various industries including, aviation, automotive, and nuclear. The firm also sells a wider range of products including materials like titanium, copper and aluminium, as well as welding and machinery,[119] making it a key firm in many industrial supply chains. The wider Kobe Steel Group is made up of various companies in Japan, Asia, Europe and the Americas, with 251 subsidiaries and 49 companies affiliated with the firm as of March 2023.[120]

Incident Summary

In June 2016, a company affiliated with the Kobe Steel Group, Shinko Wire Stainless Company Ltd, detected a quality issue with its products following self-inspection, triggering an investigation by Kobe Steel into this discrepancy.[121] The investigation revealed its findings in October 2017, which uncovered misconduct at the company dating back to the 1970s, alleging that several executives over the years were reportedly aware of misconduct happening at companies associated with Kobe Steel but took little action to address the issue.[122]

In a public announcement on 8 October 2017, Kobe Steel disclosed that it had falsified quality assurance data about the strength and durability of some of its aluminium and copper products. Investigation into products shipped by the company between September 2017 and August 2016 had revealed a number of instances of misconduct. This included falsified data for materials like aluminium sheets, copper tubes, and steel powder.[123]

These components were used in a range of parts that were sold to prominent firms both in Japan and abroad, including Hitachi, Ford, General Motors of America, Toyota, Mitsubishi, and Boeing. Following the announcement, Kobe Steel Group established an independent investigation committee to further explore the inconsistencies and determine the true scope of the issue. These investigations culminated in a report released to the public by the Board of Directors of Kobe Steel Group on 6 March 2018.[124]

The investigation revealed that a total of over 600 customers were impacted by the data falsification, including 222 overseas customers.[125] Furthermore, the company revealed that the misconduct was not a recent phenomenon, and falsifications dated back as far as the 1970s, a period during which the company experienced significant overseas activities and the establishment of Kobelco as an international conglomerate (with Kobe Steel made a subsidiary).[126] Misconduct was not limited to just falsifying recorded inspection data, but also fabricating data for tests that were never actually completed to falsely indicate that they had met quality assurance measures.[127]

The report also revealed that in some cases, executives at the companies were allegedly aware of wrongdoing, and reportedly even sometimes involved.[128] For example, some executives were allegedly aware of falsification but failed to report it to their superiors. Others were reportedly involved in misconduct before taking positions in higher office, and allegedly did little to address continuing falsifications when they became executives.[129]

Preventative and Mitigating Measures

Following the publication of the report, the CEO and Chair of Kobe Steel resigned. The Executive Vice President also resigned, and a temporary pay cut for up to 80% of all internal executives was announced.[130] Kobe Steel installed a series of measures, as discussed in the report, to ensure such an incident would not occur again. This included the adoption of a 'quality charter' and general improvements to the company's quality assurance and quality control systems, as well as a change in managerial and executive culture.[131] Although there was an eventual investigation into the falsification of records, the fact that these practices were able to continue for five decades raised serious concerns about the safety and transparency culture at Kobe Steel.

Broader Implications

The Kobe Steel incident was notable as the products sold by the company were present in a range of critical infrastructure including aviation, the automotive industry, and nuclear, where faulty parts can have significant safety implications. Detection of CFSIs higher in the supply chain, such as at the material level, can make them harder to detect as they may be supplied to legitimate distributors that are unaware of their fraudulent nature.

A report by the US NRC found that Kobe Steel parts were installed in safety-related features at American nuclear facilities, but the parts found to be counterfeited were not present at American NPPs.[132] If these parts had been present, however, they would have presented a major risk in that parts could potentially be less durable or more susceptible to damage.

Case Study 10: Counterfeit Integrated Circuits Sold for Military Use, United States

Background Context

Electronics counterfeiting is a serious issue as fraudulent parts are becoming increasingly common, likely due to the increasing obsolescence of parts and the need to constantly update electronic components.[133] In addition, the globalised supply chain creates conditions that mean parts can be manufactured in environments without stringent quality oversight and by manufacturers which do not meet industry standards.[134] This is a particularly problematic issue when it comes to electronics counterfeiting, as electronics counterfeiting is one of the most profitable counterfeiting markets in the world.[135]

Fraudulent electronics are a prevalent issue in the defence supply chain. A US Senate Armed Services Committee investigation in 2012 found that in one part of the supply chain, over one million counterfeit electronic components were used in 1,800 instances between 2009 and 2010, affecting key defence infrastructure.[136] A Public Law was established following the report to tackle the issue of counterfeiting in the military supply chain.[137]

Incident Summary

The perpetrator in this case was Rogelio Vasquez, pseudonym 'James Harrison', a resident of Orange County, California. Vasquez served as the owner of PRB Logics Corporation for several years and knowingly counterfeited electric components bound for key military systems.[138] PRB Logics Corporation advertised itself as a legitimate firm selling name-brand and trademarked integrated circuits to a range of customers.[139]

Vasquez primarily supplied integrated circuits, an electronic circuit used on semiconductor chips, and used in a variety of applications, including in military aircraft and equipment.

He began his business in July 2009, obtaining old and used integrated circuits from Chinese suppliers. He would then instruct his partners to take measures to remark the products with altered lot codes, date codes, and origin information to trick customers into believing the circuits were legitimate.[140] Vasquez's indictment records his communications with his suppliers in China where he details the counterfeiting measures at length. It includes emails of him urging his partners to ensure fraudulent parts 'look good' and pass visual inspections, as well as asking suppliers to use specific counterfeiting techniques such as remarking.[141] It also reports that he instructed a testing lab in China to provide him with two copies of the parts' test report, one legitimate to Vasquez and one for his customers that omitted all details of remarking and other counterfeiting measures used on the product.[142]

In 2012, Vasquez sold some of these counterfeited integrated circuits to a US defence subcontractor, and the parts ended up in a classified US Air Force weapons system.[143] Three years later, a federal undercover investigation was launched against Vasquez, and undercover agents purchased multiple counterfeit parts from Vasquez between November 2015 and May 2016. Vasquez sold the agents eight counterfeit circuits that he was led to believe would be installed by the US military in B-1 Lancer Bomber aircraft.[144]

Preventative and Mitigating Measures

The federal investigation against Rogelio Vasquez resulted in his arrest and charges being brought against him in 2018.[145] He surrendered over US$97,000 in cash and 169,148 counterfeit integrated circuits that were in his possession.[146]

Vasquez was charged in a 30-count indictment with charges including wire fraud, trafficking in counterfeit goods, and trafficking in counterfeit military goods.[147] Evidence included the undercover investigation, as well as a record of wire communications between Vasquez and his Chinese partners in the form of emails.[148] He pleaded guilty to four counts, was sentenced to 46 months in federal prison, and ordered to pay US$144,000 in restitution.[149] During the case, Vasquez helped federal officials identify where and how the counterfeit parts entered the defence supply chain, aiding government officials in their investigations and helping mitigate any further risk from the products.[150]

Following Vasquez's sentencing, Special Agent in Charge Michael Mentavlos emphasised the continued dedication of federal bodies in the United States to fighting cases of counterfeiting in military technology, and that pursuing such cases was crucial to protecting national security.[151] A number of investigations by these agencies in subsequent years have aided in halting further infiltration of counterfeit parts into the defence supply chain. A recent example includes a case against an individual from California who pled guilty to defrauding the Department of Defense's Defense Logistics Agency of over $3.5 million in the sale of counterfeit and fraudulent fan assemblies, some of which were bound for nuclear submarines.[152]

Broader Implications

Counterfeits in the defence supply chain is a highly significant challenge that a number of countries are facing. In the US, much action has been taken to combat the risk that this poses to military equipment and personnel.

The US Senate Armed Services Committee report in 2012 shed a light on just how pervasive the issue was, reporting some staggering findings. For example, the investigation found that 84,000 suspect counterfeit electronic parts had infiltrated the Department of Defense supply chain, allegedly via a single electronic parts supplier: Hong Dark Electronic Trade, of Shenzhen, China.[153] These parts made it into the Traffic Alert and Collision Avoidance Systems (TCAS) of the widely used C-5AMP airlifter, the C-12 Operational Support Aircraft, and the RQ-4 Global Hawk unmanned aircraft system. Parts also infiltrated assemblies intended for the P-3 Anti-Submarine Warfare (ASW) aircraft, the Special Operations Force A/MH-6M helicopter, and other naval, air force and military equipment.[154]

As mentioned earlier in the handbook, the majority of the counterfeit electronics bound for industrial systems originate from China, according to research by the OECD-EUIPO and the US Department for Homeland Security (DHS). The DHS has reported that the region is a hotbed for counterfeit microelectronics production, likely due to the already thriving and legitimate electronics trade existing in the area.[155] The networks that disseminate these are complex, with some remarking chips in China while others ship genuine chips abroad and remark them once they have reached their market destination.[156]

This case demonstrated how individuals in target markets like the US can form global partnerships and connections, facilitating the entry of counterfeit parts into key industrial systems.

Case Study 11: Counterfeit Parts Cause Aeroplane Crash, Norway

Background Context

Counterfeit and fraudulent parts are a major concern in the aviation industry, with an estimated 10% of aircraft parts in the legal market estimated to be CFSIs.[157] The scale of the problem is highly significant, with the European Union Aviation Safety Agency records a staggering 7,721 separate incidents of CFSI, unapproved, or stolen parts between 2008 and the time of writing on its online database.[158]

Incident Summary

On 9 September 1989, Partnair Flight 394 departed Oslo on a chartered flight to Hamburg. Partnair was a Norwegian chartered airline that had a fleet of aircraft, including the Convair 340/580 involved in the crash.[159] On board were 50 passengers and five crew members, including the pilot and first officer, who were very experienced with a total flight time of over 32,000 hours between them. Other members of the crew included two flight attendants and a mechanic, who was to accompany the flight to check the aircraft during its stop in Hamburg.[160] The passengers of the flight were a group of employees of the Norwegian shipping company Wilhelmsen Lines, and roughly half of the employees were from the company's head office.[161]

Partnair had reportedly been experiencing financial difficulty around the time of the crash, and take-off of Flight 394 had been delayed due to an unsettled catering bill that the pilots paid for with its own funds.[162] The aircraft had also previously experienced technical difficulty, specifically with the alternating current (AC) generators, but also with closing the main door/stairway and operating the right-hand engine. AC generators convert the mechanical energy created by the rotation of the aeroplane's engine into electrical energy, powering the aircraft's electrical system and making it a critical component in the vehicle's operation.

The left-hand AC generator of the aircraft was replaced days before Flight 394, but malfunctions persisted. Fred. Olson Air Transport Ltd. (FOF), another chartered airline which oversaw the preparation of the aircraft for flight, advised temporarily flying the plane with the auxiliary power unit (APU) as well as grounding the aircraft for further inspection. This method of the APU running during flight-time was only used once on the plane before it was deployed for Flight 394.[163]

Shortly before take-off, the flight mechanic reported to flight crew that the left AC system was still faulty, and so the pilots made the decision to employ APU power for the duration of the flight.[164] The flight took off shortly before 1600 hrs and proceeded to the planned cruise levels, before making a slight course adjustment after being informed of strong westerly winds by air traffic control at Oslo. After leaving Norwegian airspace, Flight 394 made contact with air traffic control in Copenhagen as it crossed into Danish airspace; this was the last radio communication made with Flight 394.[165] The flight subsequently disappeared from Danish radar, and despite numerous attempts to make contact, there was no trace of the aircraft. After almost 30 minutes of no response, air traffic control informed rescue authorities in Norway and Denmark, then upgraded the search to an accident investigation.

A range of theories were investigated including human error by the flight crew, bad weather, and the demolition of an explosive, with the latter theory being explored due to the recent bombing of a Pan-Am flight over Lockerbie, Scotland several months earlier.[166]

After multiple tests, the investigation team discovered that the plane's flight data recorder (FDR) had been recording abnormal vibrations for months, but this problem had briefly stopped after a repair, before continuing some weeks later. It was revealed that the pause in abnormal readings came after a mechanic noticed wear on one of four bolts used in the empennage, or tail assembly, of the aircraft and replaced it.[167] Further investigation of this bolt in comparison to the other three revealed that the three old bolts were counterfeit and did not meet quality assurance standards.

The team concluded that the weak bolts, combined with the already broken APU mount, created violent vibrations that led to a catastrophic failure of the plane's tail structure, with the tail breaking off the aircraft, leading to the crash.[168]

Preventative and Mitigating Measures

The investigative team at the Aircraft Accident Investigation Board (AIB-Norway) conducted an in-depth study of the accident and had a team of experts from the National Transportation Safety Board, the original manufacturer of the plane General Dynamics, and academic partners from institutions like Cranfield Institute of Technology.[169] Flight 394 spurred air safety organisations to take the risk of counterfeit and fraudulent parts more seriously. In the aftermath of the accident, Mary Schiavo, Inspector General at the US Department of Transportation began a tough campaign against counterfeit and unapproved parts on aeroplanes.[170] Schiavo's investigations led to roughly 120 criminal convictions from 1990 to 1996.[171] In a Senate hearing in 1995, Schiavo testified that a study on domestic and foreign repair stations found that of the parts used by these stations that were obtained from brokers, 95% were suspected unapproved parts.[172]

Broader Implications

Like the nuclear sector, the aviation industry is one where fraudulent parts can undermine safety-critical components and put many lives at risk. The case of Partnair 394 revealed how counterfeit parts, even on a relatively small-scale, can have devastating consequences. Given that nuclear installations are also complex in nature – relying on multiple components working in integrated ways – this case demonstrates the importance of identifying and addressing CFSIs, no matter how small or insignificant they may appear.

Recently, counterfeit aircraft parts are once again at the forefront of discussion as an ongoing case as the London High Court investigates the possibility of a British firm allegedly selling thousands of counterfeit parts for use in engines used by companies like Airbus and Boeing.[173] Additionally, recent cases of aviation safety breaches, like the mid-air blowout of a Boeing 737 Max aircraft, have once again shed a light in the shortcomings of safety and quality assurance in the aviation industry, and how prioritising profit over safety can have significant consequences.[174]

Case Study 12: Counterfeit Parts Cause Catastrophic Engine Failure at a Western Australian Mine, Australia

Background Context

The Australian mining industry is one of the largest in the world, amounting to roughly 75% of the country's exports and a total net worth of AUSD$160bn in resource exports.[175] Materials exported include uranium, copper, iron ore and lithium, the latter of which Australia is the world's largest producer.[176] The majority of mines are located in Western Australia, placing it at the centre of the country's mining industry.[177]

Incident Summary

In October 2023, a mining operation was put at risk when a high-power engine inside a mining excavator went into catastrophic failure. The engine had been running for just 6,000 hours, despite being able to run for up to 16,000 hours with correct maintenance.[178] Excavators perform crucial roles at mines, including digging up ground, moving material and helping ensure excess material is stacked and stored in a safe manner. The engine in question was a Cummins K50, frequently used in industrial settings across the world and known for its durability and reliability.[179]

Technicians from Cummins checked the engine and discovered that a number of counterfeit parts had been used by a third-party supplier to rebuild the engine.[180] Parts appeared cheap and flimsy, and some were poorly etched with the Cummins logo to make them appear legitimate. These were likely sourced from outside Cummins' official channels, with an unauthorised repairer hired to avoid higher costs.[181]

Preventative and Mitigating Measures

Cummins have been fighting counterfeits for years, and in 2021 made a seizure of 440,000 parts in roughly 30 cities in China with the support of Chinese law enforcement.[182] In an interview following the 2023 incident, a Cummins' manager stated that the company is developing further measures to help combat counterfeiting of Cummins' products.[183]

Wider steps being taken by the mining sector include issuing bulletins to industry actors when cases are uncovered and encouraging better procurement and quality assurance practices across the sector.[184] In Kenya, where 23% of illicit trade directly impacts the mining and construction sector, measures like an intellectual property rights recordation programme for all imports have helped better identify counterfeit and fraudulent parts bound for industries like mining.[185]

Broader Implications

The Australian mining industry has been dealing with the risk of counterfeit and fraudulent parts for many years. In the same month as the Western Australia mine incident, a Queensland mining operation found that heavy-duty bearings being used in its mine were counterfeit.[186] A month earlier, in September 2023, counterfeit heavy-duty bearings were also discovered in a Queensland mine.[187] Counterfeits present significant risks for mines and mine workers as the faulty components could malfunction, potentially creating life-threatening events such as a fire or electric failure.

References

1 International Atomic Energy Agency, 'Country Nuclear Power Profiles: Mexico', 2022. https://www-pub.iaea.org/MTCD/Publications/PDF/cnpp2022/countryprofiles/Mexico/Mexico.htm

2 World Nuclear Association, 'Nuclear Power in Mexico', March 2024. https://world-nuclear.org/information-library/country-profiles/countries-g-n/mexico.aspx

3 International Atomic Energy Agency, 'Mexico: Preamble and summary', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/MX/profile/preview

4 United States Nuclear Regulatory Commission, 'Emergency Diesel Generators: Diesel Generators as Emergency Power Sources', August 2011. https://www.nrc.gov/docs/ML1122/ML11229A062.pdf

5 José Francisco López Jiménez, 'Electrical Systems at Laguna Verde Nuclear Power Plant (LVNPP) after the Fukushima accident', Nuclear Energy Agency (NEA) of the OECD, 2015. https://inis.iaea.org/collection/NCLCollectionStore/_Public/46/066/46066610.pdf

6 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

7 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

8 Secretaria de Energia, 'National Report Presented by the United Mexican States to Meet the Requirements of the Convention on Nuclear Safety 2016-2018', 2019. https://www.gob.mx/cms/uploads/attachment/file/486785/National_Report-_Mexico_2019.pdf

9 International Atomic Energy Agency, 'IAEA Concludes Long Term Operational Safety Review at Mexico's Laguna Verde Nuclear Power Plant', 27 June 2022. https://www.iaea.org/newscenter/pressreleases/iaea-concludes-long-term-operational-safety-review-at-mexicos-laguna-verde-nuclear-power-plant-0

10 The identity of this particular NPP is not available in the open-source documentation.

11 World Nuclear Association, 'Nuclear Power in Canada', September 2023. https://world-nuclear.org/information-library/country-profiles/countries-a-f/canada-nuclear-power.aspx

12 International Atomic Energy Agency, 'Canada', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/CA/profile/highlights

13 Sasha Istvan, 'Strong domestic supply chain an advantage as Canada moves ahead with new nuclear: Sasha Istvan for Insider Policy', Macdonald-Laurier Institute, 5 February 2024. https://macdonaldlaurier.ca/strong-domestic-supply-chain-an-advantage-as-canada-moves-ahead-with-new-nuclear-sasha-istvan-for-inside-policy/#:~:text=While%20the%20bulk%20of%20the,provider%20of%20BWRX%2D300%20components.

14 P. Wong, 'Canadian Nuclear Safety Commission Supply Chain Oversight', USNRC Regulatory Information Conference 2017, North Bethesda, MD, delivered 15 March 2017. https://www.nrc.gov/docs/ML1708/ML17086A506.pdf

15 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

16 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

17 World Nuclear Association, 'Nuclear Power in the USA', March 2024. https://world-nuclear.org/information-library/country-profiles/countries-t-z/usa-nuclear-power.aspx

18 United States Nuclear Regulatory Commission, 'Counterfeit Parts Supplied to Nuclear Power Plants', NRC Information Notice 2008-04, 7 April 2008. https://www.nrc.gov/docs/ML0807/ML080790266.pdf

19 Consumer Product Safety Commission, 'Scott Electric Co. Inc. Recalls Counterfeit Circuit Breakers Due to Fire Hazard', Recalls Release no.07-036, 16 November 2006. https://www.cpsc.gov/Recalls/2007/Scott-Electric-Co-Inc-Recalls-Counterfeit-Circuit-Breakers-Due-To-Fire-Hazard

20 Consumer Product Safety Commission, 'Connecticut Electric Recalls Counterfeit Square D Circuit Breakers Due to Fire Hazard', Recalls Release no.08-054, 30 October 2007. https://www.cpsc.gov/Recalls/2007/connecticut-electric-recalls-counterfeit-square-d-circuit-breakers-due-to-fire-hazard

21 Consumer Product Safety Commission, 'North American Breaker Co. Recalls Counterfeit Circuit Breakers Due to Fire Hazard', Recalls Release no.08-151, 27 December 2007. https://www.cpsc.gov/Recalls/2007/north-american-breaker-co-recalls-counterfeit-circuit-breakers-due-to-fire-hazard

22 United States Nuclear Regulatory Commission, 'Counterfeit Parts Supplied to Nuclear Power Plants', NRC Information Notice 2008-04, 7 April 2008. https://www.nrc.gov/docs/ML0807/ML080790266.pdf

23 United States Nuclear Regulatory Commission, 'Counterfeit Parts Supplied to Nuclear Power Plants', NRC Information Notice 2008-04, 7 April 2008. https://www.nrc.gov/docs/ML0807/ML080790266.pdf

24 Los Alamos National Laboratory Office of Health, Safety and Security, 'Identifying Counterfeit Square D Circuit Breakers', Safety Bulletin 2008-01, January 2008. https://www.lanl.gov/safety/electrical/docs/counterfeit_squared_circuit_breakers.pdf

25 Consumer Product Safety Commission, 'Connecticut Electric Recalls Counterfeit Square D Circuit Breakers Due to Fire Hazard', Recalls Release no.08-054, 30 October 2007. https://www.cpsc.gov/Recalls/2007/connecticut-electric-recalls-counterfeit-square-d-circuit-breakers-due-to-fire-hazard

26 Los Alamos National Laboratory Office of Health, Safety and Security, 'Identifying Counterfeit Square D Circuit Breakers', Safety Bulletin 2008-01, January 2008. https://www.lanl.gov/safety/electrical/docs/counterfeit_squared_circuit_breakers.pdf

27 United States District Court of the Western District of Pennsylvania, 'Square D Company v. Scott Electric Company', Civil Action No. 06-00459, W.D. Pa., 30 September 2008. https://casetext.com/case/square-d-company-v-scott-electric-company-7/

28 Schneider Electric, 'Awareness and actions against counterfeiting', 2024. https://www.se.com/us/en/work/support/counterfeit/

29 Consumer Product Safety Commission, 'Connecticut Electric Recalls Counterfeit Square D Circuit Breakers Due to Fire Hazard', Recalls Release no.08-054, 30 October 2007. https://www.cpsc.gov/Recalls/2007/connecticut-electric-recalls-counterfeit-square-d-circuit-breakers-due-to-fire-hazard; Consumer Product Safety Commission, 'North American Breaker Co. Recalls Counterfeit Circuit Breakers Due to Fire Hazard', Recalls Release no.08-151, 27 December 2007. https://www.cpsc.gov/Recalls/2007/north-american-breaker-co-recalls-counterfeit-circuit-breakers-due-to-fire-hazard; Consumer Product Safety Commission, 'Scott Electric Co. Inc. Recalls Counterfeit Circuit Breakers Due to Fire Hazard', Recalls Release no.07-036, 16 November 2006. https://www.cpsc.gov/Recalls/2007/Scott-Electric-Co-Inc-Recalls-Counterfeit-Circuit-Breakers-Due-To-Fire-Hazard

30 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

31 Jordan Robertson and Michael Riley, 'The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies', Businessweek Feature, *Bloomsberg*, 4 October 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies#xj4y7vzkg

32 Kate Fazzini, 'Chinese Spy chips are found in hardware used by Apple, Amazon, Blomberg says; Apple, AWS say no way', *CNBC*, 4 October 2018. https://www.cnbc.com/2018/10/04/chinese-spy-chips-are-said-to-be-found-in-hardware-used-by-apple-amazon-apple-denies-the-bloomberg-businessweek-report.html

33 Jim Finkle, 'Apple, Amazon deny Bloomberg report on Chinese hardware attack', *Reuters*, 5 October 2018. https://www.reuters.com/article/us-china-cyber-idUSKCN1ME19J/

34 U.S. Energy Information Administration, 'South Korea is one of the World's Largest Nuclear Power Producers', 27 August 2020. https://www.eia.gov/todayinenergy/detail.php?id=44916#:~:text=South%20Korea%2C%20which%20is%20about,square%20mile)%20in%20the%20world.

35 World Nuclear Association, 'Nuclear Power in South Korea', May 2024. https://world-nuclear.org/information-library/country-profiles/countries-o-s/south-korea.aspx

36 International Atomic Energy Agency, 'Republic of Korea: Preamble and summary', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/KR/profile/preview

37 Choe Sang-Hun, 'Scandal in South Korea Over Nuclear Revelations', *New York Times*, 3 August 2013. https://www.nytimes.com/2013/08/04/world/asia/scandal-in-south-korea-over-nuclear-revelations.html?pagewanted=1

38 K.J. Kwon, 'South Korea shuts down 2 nuclear reactors after parts scandal', *CNN*, 5 November 2012. https://edition.cnn.com/2012/11/05/world/asia/south-korea-nuclear-reactors/

39 Philip Andrews-Speed, 'South Korea's nuclear power industry: recovering from scandal', *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010

40 Philip Andrews-Speed, 'South Korea's nuclear power industry: recovering from scandal', *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010

41 World Nuclear Association, 'Nuclear Power in South Korea', September 2023. https://world-nuclear.org/information-library/country-profiles/countries-o-s/south-korea.aspx

42 Ilchong Nam (Ed.) and Geoffrey Rothwell (Ed.), 'New Nuclear Power Industry Procurement Markets: International Experiences', *KDI Research Monograph 2014*, vol.1, December 2014. https://www.econstor.eu/bitstream/10419/200944/1/kdi-res-monograph-2014-01.pdf

43 Philip Andrews-Speed, 'South Korea's nuclear power industry: recovering from scandal', *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010; Kim Da-ye, 'Endless scandals hit nuclear power supplier', *The Korea Times*, 01 September 2013. https://www.koreatimes.co.kr/www/news/biz/2013/09/335_142036.html

44 Philip Andrews-Speed, 'South Korea's nuclear power industry: recovering from scandal', *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010; Ilchong Nam (Ed.) and Geoffrey Rothwell (Ed.), 'New Nuclear Power Industry Procurement Markets: International Experiences', *KDI Research Monograph 2014*, vol.1, December 2014. https://www.econstor.eu/bitstream/10419/200944/1/kdi-res-monograph-2014-01.pdf; Nuclear Safety and Security Commission, 'Investigation result regarding the test record forgery of Shin-kori No. 1 and No. 2 reactors/Shin-wolsong No. 1 and No. 2 reactors', 28 May 2013. https://www.nssc.go.kr/en/cms/FR_BBS_CON/BoardView.do?pageNo=93&pagePerCnt=10&MENU_ID=90&CONTENTS_NO=&SITE_NO=3&BOARD_SEQ=1&BBS_SEQ=11954&USER_NAME=&TEL_NO=&WRITER_DI=&_csrf=&SEARCH_FLD=&SEARCH=; Will Davis, 'South Korea nuclear power: are the dark times over?', *Nuclear Newswire*, 6 February 2014. https://www.ans.org/news/article-1510/south-korea-nuclear-power-are-the-dark-times-over/

45 Ju-Min Park, 'South Korea charges 100 with corruption over nuclear scandal', *Reuters*, 10 October 2013. https://www.reuters.com/article/us-korea-nuclear-idUSBRE99905O20131010

46 World Nuclear News, 'Korean reactors cleared for restart', *World Nuclear News*, 2 January 2014. https://www.world-nuclear-news.org/RS-Korean-reactors-cleared-for-restart-0201144.html

47 Sang-Jong Lee, 'Korean Industry Perspective on CFSI', NRC Workshop on Vendor Oversight Portland, OR, delivered 12 June 2014, https://www.nrc.gov/docs/ML1415/ML14153A200.pdf; Ilchong Nam (Ed.) and Geoffrey Rothwell (Ed.), 'New Nuclear Power Industry Procurement Markets: International Experiences', *KDI Research Monograph 2014*, vol.1, December 2014. https://www.econstor.eu/bitstream/10419/200944/1/kdi-res-monograph-2014-01.pdf

48 Nuclear Safety and Security Commission, 'NSSC To Operate 'Nuclear Safety Ombudsman' To Root Out Corruptive Actions', 4 June 2013. https://www.nssc.go.kr/en/cms/FR_BBS_CON/BoardView.do?pageNo=93&pagePerCnt=10&MENU_ID=90&CONTENTS_NO=&SITE_NO=3&BOARD_SEQ=1&BBS_SEQ=11959&USER_NAME=&TEL_NO=&WRITER_DI=&_csrf=&SEARCH_FLD=&SEARCH=

49 Meeyoung Cho, 'South Korea Widens Investigation into Forged Nuclear Safety Certificates', *Business Insider*, 7 February 2014. https://www.businessinsider.com/south-korea-widens-nuclear-investigation-2014-2?r=US&IR=T

50 International Atomic Energy Agency, 'IAEA Completes Expert Mission to Kori 1 Nuclear Power Plant in the Republic of Korea', 11 June 2012. https://www.iaea.org/newscenter/pressreleases/iaea-completes-expert-mission-kori-1-nuclear-power-plant-republic-korea

51 Kim Da-ye, 'Endless scandals hit nuclear supplier', *The Korean Times*, 1 September 2013. https://www.koreatimes.co.kr/www/biz/2023/12/602_142036.html

52 Richard Tanter, 'After Fukushima: A Survey of Corruption in the Global Nuclear Power Industry', *Asian Perspective*, Vol. 37, No. 4, 2013, pp. 475-500. https://doi.org/10.1353/apr.2013.0020

53 Mycle Schneider et al., 'The World Nuclear Industry Status Report 2021', Paris, France, September 2021. https://www.worldnuclearreport.org/IMG/pdf/wnisr2021-hr.pdf

54 Meeyoung Cho, 'South Korea Widens Investigation into Forged Nuclear Safety Certificates', *Business Insider*, 7 February 2014. https://www.businessinsider.com/south-korea-widens-nuclear-investigation-2014-2?r=US&IR=T

55 Nuclear Safety and Security Commission, 'NSSC Found More Cases of Counterfeit Seismic Qualification Reports Submitted by Saehan TEP', 3 July 2013. https://www.nssc.go.kr/en/cms/FR_BBS_CON/BoardView.do?pageNo=89&pagePerCnt=10&MENU_ID=90&CONTENTS_NO=&SITE_NO=3&BOARD_SEQ=1&BBS_SEQ=11967&USER_NAME=&TEL_NO=&WRITER_DI=&_csrf=&SEARCH_FLD=&SEARCH=

56 World Nuclear Association, 'Nuclear Power in France', May 2024. https://world-nuclear.org/information-library/country-profiles/countries-a-f/france.aspx

57 Framatome, 'Manufacture components of the primary loop for nuclear facilities under construction or in operation', undated. https://www.framatome.com/en/expertise/component-manufacturing/

58 Autorité de Sûreté Nucléaire, 'Flamanville EPR reactor vessel manufacturing anomalies', 7 April 2015. https://www.french-nuclear-safety.fr/asn-informs/news-releases/flamanville-epr-reactor-vessel-manufacturing-anomalies

59 Autorité de Sûreté Nucléaire, 'AREVA has informed ASN of irregularities concerning components manufactured in its Creusot Forge plant', 4 May 2016. https://www.french-nuclear-safety.fr/asn-informs/news-releases/irregularities-concerning-components-manufactured-in-its-creusot-forge-plant

60 Autorité de Sûreté Nucléaire, 'ASN suspends the test certificate for a steam generator in the Fessenheim NPP affected by one of the irregularities detected in Areva's Creusot Forge plant', 20 July 2016. https://www.french-nuclear-safety.fr/asn-informs/news-releases/fessenheim-npp-affected-by-one-of-the-irregularities-detected-in-areva-s-creusot-forge-plant

61 Lee Buchsbaum, 'France's Nuclear Storm: Many Power Plants Down Due to Quality Concerns', *POWER Magazine*, 1 December 2016. https://www.powermag.com/frances-nuclear-storm-many-power-plants-down-due-to-quality-concerns/?printmode=1

62 Sylvain Tronchet, 'Cuve de l'EPR de Flamanville : l'incroyable légèreté d'Areva et EDF', *Radio France Inter*, 31 March 2017. https://www.radiofrance.fr/franceinter/cuve-de-l-epr-de-flamanville-l-incroyable-legerete-d-areva-et-edf-4103446

63 Autorité de Sûreté Nucléaire, 'Manufacturing quality at Creusot Forge: ASN publishes the record of its correspondence with EDF and Areva NP on this subject since 2005', 5 April 2017. https://www.french-nuclear-safety.fr/asn-informs/news-releases/manufacturing-quality-at-creusot-forge

64 Autorité de Sûreté Nucléaire, 'Manufacturing quality at Creusot Forge: ASN publishes the record of its correspondence with EDF and Areva NP on this subject since 2005', 5 April 2017. https://www.french-nuclear-safety.fr/asn-informs/news-releases/manufacturing-quality-at-creusot-forge

65 Autorité de Sûreté Nucléaire, 'ASN defines the preconditions for the resumption of manufacturing in AREVA NP's Creusot Forge plant', 12 April 2017. https://www.french-nuclear-safety.fr/asn-informs/news-releases/resumption-of-manufacturing-in-areva-np-s-creusot-forge-plant

66 Autorité de Sûreté Nucléaire, 'ASN issues its opinion on the anomaly in the composition of the steel used for the Flamanville EPR rector pressure vessel lower head and closure head', 11 October 2017. https://www.french-nuclear-safety.fr/asn-informs/news-releases/flamanville-epr-reactor-asn-issues-its-opinion

67 Autorité de Sûreté Nucléaire, 'ASN issues its opinion on the anomaly in the composition of the steel used for the Flamanville EPR rector pressure vessel lower head and closure head', 11 October 2017. https://www.french-nuclear-safety.fr/asn-informs/news-releases/flamanville-epr-reactor-asn-issues-its-opinion; Autorité de Sûreté Nucléaire, 'ASN authorises use of the Flamanville EPR reactor vessel closure head until the first refuelling outage of the reactor', 31 May 2023. https://www.french-nuclear-safety.fr/asn-informs/news-releases/asn-authorises-use-of-the-flamanville-epr-reactor-vessel-closure-head#:~:text=Delivery%20of%20the%20replacement%20closure%20head%20is%20planned,scheduled%20between%2015%20and%2018%20months%20after%20commissioning

68 World Nuclear News, 'ASN allows longer use of Flamanville EPR vessel head', 15 March 2023. https://world-nuclear-news.org/Articles/ASN-allows-longer-use-of-Flamanville-EPR-vessel-he ; Reuters, 'EDF's Framatome seeks more time for Flamanville vessel head replacement', 23 January 2023. https://www.reuters.com/business/energy/edfs-framatome-asks-watchdog-more-time-change-nuclear-vessel-head-flamanville-2023-01-23/; Autorité de Sûreté Nucléaire, 'ASN authorise commissioning of the Flamanville EPR reactor', 8 May 2024. https://www.french-nuclear-safety.fr/asn-informs/news-releases/asn-authorise-commissioning-of-the-flamanville-epr-reactor

69 Autorité de Sûreté Nucléaire, 'Multinational inspection of AREVA NP in its Creusot Forge plant in Le Creusot (France)', 27 February 2017. https://www.french-nuclear-safety.fr/asn-inspects/supervision-of-the-epr-reactor/anomaly-affecting-the-flamanville-epr-reactor-vessel/multinational-inspection-of-areva-np-in-its-creusot-forge-plant-in-le-creusot-france

70 Adam Vaughan, 'Inspectors find safety irregularities at Creusot nuclear forge in France', *The Guardian*, 24 March 2017. https://www.theguardian.com/environment/2017/mar/24/areva-creusot-nuclear-forge-france-hinkley-point.

71 World Nuclear Association, 'Nuclear Development in the United Kingdom', 12 October 2016. https://world-nuclear.org/information-library/appendices/nuclear-development-in-the-united-kingdom

72 World Nuclear Association, 'Nuclear Development in the United Kingdom', 12 October 2016. https://world-nuclear.org/information-library/appendices/nuclear-development-in-the-united-kingdom; Ian Curwen, 'Decommissioning the world's first commercial nuclear power station', *Cleaning up our nuclear past: faster, safer and sooner*, Nuclear Decommissioning Authority Blog, 3 September 2019. https://nda.blog.gov.uk/decommissioning-the-worlds-first-commercial-nuclear-power-station/

73 UK Department for Energy Security and Net Zero, 'Biggest expansion of nuclear power for 70 years to create jobs, reduce bills and strengthen Britain's energy security', 11 January 2024. https://www.gov.uk/government/news/biggest-expansion-of-nuclear-power-for-70-years-to-create-jobs-reduce-bills-and-strengthen-britains-energy-security

74 Sellafield Ltd., 'About us', undated. https://www.gov.uk/government/organisations/sellafield-ltd/about

75 Tom Clarke, 'Sellafield: An inside look at the most hazardous building in Western Europe as work to remove radioactive sludge begins', *Sky News*, 9 June 2022. https://news.sky.com/story/sellafield-an-inside-look-at-the-most-hazardous-building-in-western-europe-as-work-to-remove-radioactive-sludge-begins-12630798

76 Office for Nuclear Regulation, 'ONR's strategy for regulating Sellafield', 9 April 2024. https://www.onr.org.uk/our-work/what-we-regulate/sellafield-decommissioning-fuel-and-waste/sellafield/onrs-strategy-for-regulating-sellafield/

77 The Parliamentary Office of Science and Technology, 'Mixed Oxide Nuclear Fuel (MOX)', Post 137, April 2000. https://www.parliament.uk/globalassets/documents/post/pn137.pdf; International Atomic Energy Agency, 'Status and Advances in MOX Fuel Technology', IAEA Technical Reports Series no.415, May 2003. https://www-pub.iaea.org/MTCD/Publications/PDF/TRS415_web.pdf?trk=public_post_comment-text

78 The Parliamentary Office of Science and Technology, 'Mixed Oxide Nuclear Fuel (MOX)', Post 137, April 2000. https://www.parliament.uk/globalassets/documents/post/pn137.pdf

79 Simon Thorne, 'The Misuse of Spreadsheets in the Nuclear Fuel Industry: The Falsification of Safety Critical Nuclear Fuel Data Using Spreadsheets at British Nuclear Fuels Limited (BNFL)', *45th Hawaii International Conference on System Sciences*, Maui, HI, 2012. https://ieeexplore.ieee.org/document/6149454

80 Simon Thorne, 'The Misuse of Spreadsheets in the Nuclear Fuel Industry: The Falsification of Safety Critical Nuclear Fuel Data Using Spreadsheets at British Nuclear Fuels Limited (BNFL)', *45th Hawaii International Conference on System Sciences*, Maui, HI, 2012. https://ieeexplore.ieee.org/document/6149454

81 BBC News, 'German ban on Sellafield fuel stays', 8 March 2000. http://news.bbc.co.uk/1/hi/uk/670740.stm

82 Nuclear Decommissioning Authority and Sellafield Ltd, 'NDA Statement on future of the Sellafield Mox Plant', 3 August 2011. https://www.gov.uk/government/news/nda-statement-on-future-of-the-sellafield-mox-plant

83 Simon Thorne, 'The Misuse of Spreadsheets in the Nuclear Fuel Industry: The Falsification of Safety Critical Nuclear Fuel Data Using Spreadsheets at British Nuclear Fuels Limited (BNFL)', *45th Hawaii International Conference on System Sciences*, Maui, HI, 2012. https://ieeexplore.ieee.org/document/6149454

84 World Nuclear Association, 'Country Profiles: Nuclear Power in Russia', April 2024. https://world-nuclear.org/information-library/country-profiles/countries-o-s/russia-nuclear-power.aspx; A. M. Petros'yants, 'A pioneer of nuclear power', *IAEA Bulletin*, Vol. 26, No. 4, December 1984. https://www.iaea.org/sites/default/files/26404794246.pdf

85 International Atomic Energy Agency, 'Russian Federation', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/RU/profile/preview

86 World Nuclear Association, 'Country Profiles: Nuclear Power in Russia', April 2024. https://world-nuclear.org/information-library/country-profiles/countries-o-s/russia-nuclear-power.aspx

87 World Nuclear Association, 'Country Profiles: Nuclear Power in Russia', April 2024. https://world-nuclear.org/information-library/country-profiles/countries-o-s/russia-nuclear-power.aspx; International Atomic Energy Agency, 'Russian Federation', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/RU/profile/preview

88 Mycle Schneider et al., 'The World Nuclear Industry Status Report 2021', Paris, France, September 2021. https://www.worldnuclearreport.org/IMG/pdf/wnisr2021-hr.pdf

89 Richard Tanter, 'After Fukushima: A Survey of Corruption in the Global Nuclear Power Industry', *Asian Perspective*, Vol. 37, No. 4, 2013, pp. 475-500. https://doi.org/10.1353/apr.2013.0020

90 Nuclear.Ru, 'A verdict has been issued in the case of supplying counterfeit devices for nuclear power plant turbines', 11 May 2012. http://www.nuclear.ru/news/77756/

91 Nuclear.Ru, 'A verdict has been issued in the case of supplying counterfeit devices for nuclear power plant turbines', 11 May 2012. http://www.nuclear.ru/news/77756/

92 Richard Tanter, 'After Fukushima: A Survey of Corruption in the Global Nuclear Power Industry', *Asian Perspective*, Vol. 37, No. 4, 2013, pp. 475-500. https://doi.org/10.1353/apr.2013.0020; Mycle Schneider et al., 'The World Nuclear Industry Status Report 2021', Paris, France, September 2021. https://www.worldnuclearreport.org/IMG/pdf/wnisr2021-hr.pdf

93 Richard Tanter, 'After Fukushima: A Survey of Corruption in the Global Nuclear Power Industry', *Asian Perspective*, Vol. 37, No. 4, 2013, pp. 475-500. https://doi.org/10.1353/apr.2013.0020

94 Nuclear.Ru, 'A verdict has been issued in the case of supplying counterfeit devices for nuclear power plant turbines', 11 May 2012. http://www.nuclear.ru/news/77756/

95 Nuclear.Ru, 'A verdict has been issued in the case of supplying counterfeit devices for nuclear power plant turbines', 11 May 2012. http://www.nuclear.ru/news/77756/

96 Nuclear.Ru, 'A verdict has been issued in the case of supplying counterfeit devices for nuclear power plant turbines', 11 May 2012. http://www.nuclear.ru/news/77756/

97 Power Machines, 'Sales Geography: References', 2024. https://power-m.ru/en/customers/references

98 T.S. Gopi Rethinaraj, 'In the Comfort of Secrecy', *Bulletin of Atomic Scientists*, Vol. 55, No. 6, November 1999. https://doi.org/10.2968/055006015

99 T.S. Gopi Rethinaraj, 'In the Comfort of Secrecy', *Bulletin of Atomic Scientists*, Vol. 55, No. 6, November 1999. https://doi.org/10.2968/055006015

100 International Atomic Energy Agency, 'Japan', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/JP/profile/preview

101 International Atomic Energy Agency, 'Japan', Country Nuclear Power Profiles, 2023. https://cnpp.iaea.org/public/countries/JP/profile/preview, World Nuclear Association, 'Nuclear Power in Japan', Country Profiles, March 2024. https://world-nuclear.org/information-library/country-profiles/countries-g-n/japan-nuclear-power#:~:text=Nuclear%20power%20industry,from%20the%20regulator%20to%20restart

102 World Nuclear Association, 'Nuclear Power in Japan', Country Profiles, March 2024, https://world-nuclear.org/information-library/country-profiles/countries-g-n/japan-nuclear-power#electricity-sector.

103 Tokyo Electric Power Company, 'Regarding fraudulent acts related to fire detectors and repeaters by Nippon Fenol Co., Ltd. (impact on our equipment)', 31 March 2022. https://www.tepco.co.jp/press/news/2022/hd11123_8973.htm

104 Fenwal Controls of Japan, 'Regarding Fraudulent Acts Related to Some of our Products', 31 March 2022. https://www.fenwal.co.jp/wp/wp-content/uploads/2022/03/当社の一部製品に関する不正行為について-3.pdf

105 Tokyo Electric Power Company, 'Regarding fraudulent acts related to fire detectors and repeaters by Nippon Fenol Co., Ltd. (impact on our equipment)', 31 March 2022. https://www.tepco.co.jp/press/news/2022/hd11123_8973.htm

106 Fenwal Controls of Japan, 'Regarding Fraudulent Acts Related to Some of our Products', 31 March 2022. https://www.fenwal.co.jp/wp/wp-content/uploads/2022/03/当社の一部製品に関する不正行為について-3.pdf

107 Kenji Izawa and Shimpei Doi, 'Approval yanked for certain fire detectors used at nuclear plants', *The Asahi Shimbun*, 27 April 2022. https://www.asahi.com/ajw/articles/14608924

108 Kenji Izawa and Shimpei Doi, 'Approval yanked for certain fire detectors used at nuclear plants', *The Asahi Shimbun*, 27 April 2022. https://www.asahi.com/ajw/articles/14608924

109 Kenji Izawa and Shimpei Doi, 'Approval yanked for certain fire detectors used at nuclear plants', *The Asahi Shimbun*, 27 April 2022. https://www.asahi.com/ajw/articles/14608924

110 Fenwal Controls of Japan, 'Regarding Fraudulent Acts Related to Some of our Products', 31 March 2022. https://www.fenwal.co.jp/wp/wp-content/uploads/2022/03/当社の一部製品に関する不正行為について-3.pdf

111 Kenji Izawa and Shimpei Doi, 'Approval yanked for certain fire detectors used at nuclear plants', *The Asahi Shimbun*, 27 April 2022. https://www.asahi.com/ajw/articles/14608924

112 Kenji Izawa and Shimpei Doi, 'Approval yanked for certain fire detectors used at nuclear plants', *The Asahi Shimbun*, 27 April 2022. https://www.asahi.com/ajw/articles/14608924

113 Fenwal Controls of Japan, 'Regarding Fraudulent Acts Related to Some of our Products', 31 March 2022. https://www.fenwal.co.jp/wp/wp-content/uploads/2022/03/当社の一部製品に関する不正行為について-3.pdf

114 Richard Tanter, 'After Fukushima: A Survey of Corruption in the Global Nuclear Power Industry', *Asian Perspective*, Vol. 37, No. 4, 2013, pp. 475-500. https://doi.org/10.1353/apr.2013.0020

115 National Diet of Japan, 'Report of the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission', 5 July 2012.

116 Geoffrey Chapman, Rebecca Earnhardt, Christopher Hobbs, Nickolas Roth, Daniel Salisbury, Amelie Stoetzel and Sarah Tzinieris, 'Nuclear Security in Times of Crisis', King's College London and Stimson Center, 2021. https://www.kcl.ac.uk/csss/assets/nuclear-security-in-times-of-crisis-handbook.pdf

117 National Diet of Japan, 'Report of the National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission', 5 July 2012.

118 National Protective Security Authority, 'Critical National Infrastructure', 25 April 2023. https://www.npsa.gov.uk/critical-national-infrastructure-0

119 Kobelco Group, 'History', 2024. https://www.kobelco.co.jp/english/about_kobelco/outline/history/index.html

120 Kobelco Group, 'Integrated Report 2023', March 2023. https://www.kobelco.co.jp/english/about_kobelco/outline/integrated-reports/index.html#integrated-report

121 United States Nuclear Regulatory Commission, 'Kobe Steel Quality Assurance Falsification', NRC Information Notice 2018-11, 24 September 2018. https://www.nrc.gov/docs/ML1819/ML18190A466.pdf

122 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

123 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

124 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

125 Yuka Obayashi, 'Kobe Steel admits data fraud went on nearly five decades, CEO to quit', *Reuters*, 5 March 2018. https://www.reuters.com/article/us-kobe-steel-scandal-ceo-idUSKBN1GH2SM

126 Kobelco Group, 'History', 2024. https://www.kobelco.co.jp/english/about_kobelco/outline/history/index.html

127 United States Nuclear Regulatory Commission, 'Kobe Steel Quality Assurance Falsification', NRC Information Notice 2018-11, 24 September 2018. https://www.nrc.gov/docs/ML1819/ML18190A466.pdf

128 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

129 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

130 Yuka Obayashi, 'Kobe Steel admits data fraud went on nearly five decades, CEO to quit', Reuters, 5 March 2018. https://www.reuters.com/article/us-kobe-steel-scandal-ceo-idUSKBN1GH2SM

131 Kobe Steel Ltd., 'Report on the Kobe Steel Group's Misconduct', 6 March 2018. https://www.kobelco.co.jp/english/progress/files/20180306_en.pdf

132 United States Nuclear Regulatory Commission, 'Kobe Steel Quality Assurance Falsification', NRC Information Notice 2018-11, 24 September 2018. https://www.nrc.gov/docs/ML1819/ML18190A466.pdf

133 World Nuclear Association Supply Chain Working Group, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', 27 August 2019. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

134 Electric Power Research Institute, 'Plant Support Engineering: Counterfeit and Fraudulent Items – Mitigating the Increasing Risk', 2014 Technical Report, July 2014. https://www.epri.com/research/products/3002002276

135 Organisation for Economic Co-operation and Development and European Union Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p.3. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

136 United States Senate Committee on Armed Services, 'Inquiry into Counterfeit Electronic Parts in the Department of Defence Supply Chain', 112th Congress, 2nd Session, Report 112-167, 21 May 2012. https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

137 Electric Power Research Institute, 'Plant Support Engineering: Counterfeit and Fraudulent Items', Technical report, California: Electric Power Research Institute, July 2014. https://www.epri.com/research/products/3002002276

138 United States Attorney's Office Central District of California, 'Orange County Electronics Distributor Charged with Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 1 May 2018. https://www.justice.gov/usao-cdca/pr/orange-county-electronics-distributor-charged-selling-counterfeit-integrated-circuits

139 Julia Sclafani, 'Owner of Costa Mesa company sentenced to prison for selling counterfeit electronic parts', *The Los Angeles Times*, 4 June 2019. https://www.latimes.com/socal/daily-pilot/news/tn-dpt-me-cm-counterfeit-electronics-20190604-story.html

140 United States Attorney's Office Central District of California, 'O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 30 May 2019. https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

141 United States District Court for the Central District of California, 'Indictment: United States of America, Plaintiff v. Rogelio Vasquez, Defendant', February 2018.

142 United States District Court for the Central District of California, 'Indictment: United States of America, Plaintiff v. Rogelio Vasquez, Defendant', February 2018.

143 Julia Sclafani, 'Owner of Costa Mesa company sentenced to prison for selling counterfeit electronic parts', The Los Angeles Times, 4 June 2019. https://www.latimes.com/socal/daily-pilot/news/tn-dpt-me-cm-counterfeit-electronics-20190604-story.html

144 United States Attorney's Office Central District of California, 'O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 30 May 2019. https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

145 United States Attorney's Office Central District of California, 'Orange County Electronics Distributor Charged with Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 1 May 2018. https://www.justice.gov/usao-cdca/pr/orange-county-electronics-distributor-charged-selling-counterfeit-integrated-circuits

146 United States Attorney's Office Central District of California, 'O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 30 May 2019. https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

147 United States Attorney's Office Central District of California, 'O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 30 May 2019. https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

148 United States District Court for the Central District of California, 'Indictment: United States of America, Plaintiff v. Rogelio Vasquez, Defendant', February 2018.

149 Julia Sclafani, 'Owner of Costa Mesa company sentenced to prison for selling counterfeit electronic parts', T*he Los Angeles Times*, 4 June 2019. https://www.latimes.com/socal/daily-pilot/news/tn-dpt-me-cm-counterfeit-electronics-20190604-story.html

150 Julia Sclafani, 'Owner of Costa Mesa company sentenced to prison for selling counterfeit electronic parts', *The Los Angeles Times*, 4 June 2019. https://www.latimes.com/socal/daily-pilot/news/tn-dpt-me-cm-counterfeit-electronics-20190604-story.html

151 United States Attorney's Office Central District of California, 'O.C. Businessman Sentenced to 46 Months in Prison for Selling Counterfeit Integrated Circuits with Military and Commercial Uses', Press Release, 30 May 2019. https://www.justice.gov/usao-cdca/pr/oc-businessman-sentenced-46-months-prison-selling-counterfeit-integrated-circuits

152 United States Department of Justice Office of Public Affairs, 'Man Pleads Guilty to Selling $3.5M in Counterfeit and Deficient Electronics for Use in Military Systems', Press Release, 28 March 2024. https://www.justice.gov/opa/pr/man-pleads-guilty-selling-35m-counterfeit-and-deficient-electronics-use-military-systems

153 United States Senate Committee on Armed Services, 'Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain', 112th Congress, 2nd Session, Report 112-167, 21 May 2012. https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

154 United States Senate Committee on Armed Services, 'Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain', 112th Congress, 2nd Session, Report 112-167, 21 May 2012. https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

155 US Department of Homeland Security, 'Dangerous Chinese Microelectronics don't always come with Balloons', 2023. https://www.dhs.gov/sites/default/files/2023-09/23_0915_oia_CCM_White_Paper_508_final.pdf

156 US Department of Homeland Security, 'Dangerous Chinese Microelectronics don't always come with Balloons', 2023. https://www.dhs.gov/sites/default/files/2023-09/23_0915_oia_CCM_White_Paper_508_final.pdf

157 Justin Kotzé and Georgios A. Antonopoulos, 'Con Air: exploring the trade in counterfeit and unapproved aircraft parts', *The British Journal of Criminology*, Vol. 63, 2023, pp. 1293-1308. https://doi.org/10.1093/bjc/azac089

158 European Union Aviation Safety Agency, 'Suspected Unapproved Parts (SUP)', 2024. https://www.easa.europa.eu/en/domains/aircraft-products/suspected-unapproved-parts?populate=&field_easa_case_type_tid%5B0%5D=2474&page=0

159 Robert W. Luedeman, 'Flying Underground: The Trade in Bootleg Aircraft', *Journal of Air Law and Commerce*, Vol. 62, No. 1, 1996. https://scholar.smu.edu/jalc/vol62/iss1/6; Markil Gregersen, Peter J.T. Knudsen, and Steen Jensen, 'The Crash of the Partnair Convair 340/580 in the Skagerrak: Traumatological Aspects', *Aviation, Space, and Environmental Medicine*, Vol.66, February 1995, pp.158-63.

160 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

161 Mayday (T.V. Documentary), Episode: 'Blown Apart'; Robert W. Luedeman, 'Flying Underground: The Trade in Bootleg Aircraft', *Journal of Air Law and Commerce*, Vol. 62, No. 1, 1996. https://scholar.smu.edu/jalc/vol62/iss1/6

162 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

163 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

164 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

165 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

166 Central Intelligence Agency, 'Exhibits: Terrorist Bombing of Pan Am Flight 103', undated. https://www.cia.gov/legacy/museum/exhibit/terrorist-bombing-of-pan-am-flight-103/; Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

167 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

168 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993, pg.58-61; pg.66-69. https://www.nsia.no/Aviation/Published-reports/1993-02-eng.

169 Norwegian Aircraft Accident Investigation Board, 'Report on the Convair 340/580 LN-PAA Aircraft Accident North of Hirtshals, Denmark, on September 8, 1989', February 1993. https://www.nsia.no/Aviation/Published-reports/1993-02-eng

170 Howard Mustoe, 'The airline parts scandal sparking panic and introspection in aerospace', *The Telegraph*, 14 October 2023. https://www.telegraph.co.uk/business/2023/10/14/fake-airline-parts-sparks-panic-aerospace-cfm56/

171 Julie Johnsson, Ryan Beene, Siddharth Vikram Philip, Sabah Meddings, 'Ghost in the Machine: How Fake Parts Infiltrated Airline Fleets', *Bloomberg*, 12 October 2023. https://www.bloomberg.com/news/features/2023-10-11/fake-parts-found-on-boeing-airbus-jets-plague-airlines?leadSource=uverify%20wall

172 Subcommittee on Oversight of Government Management and the District of Columbia, 'Aviation Safety: Do Unapproved Parts Pose a Safety Risk?: Hearing Before the Subcommittee on Oversight of Government Management and the District of Columbia of the Committee on Governmental Affairs, United States Senate, One Hundred Fourth Congress, First Session, May 24, 1995', US Government Printing Office, 1996.

173 Sam Tobin and Tim Hepher, 'UK firm sold thousands of unverified jet engine parts, CFM says', *Reuters*, 20 September 2023. https://www.reuters.com/business/aerospace-defense/engine-maker-cfm-says-up-96-planes-affected-by-fake-parts-probe-2023-09-20/

174 Sylvia Pfeifer and Claire Bushey, 'Boeing's Alaska Airline mid-air blowout puts focus on Spirit AeroSystems', *The Financial Times*, 8 January 2024. https://www.ft.com/content/8edfe845-99f1-431a-9bfd-073309d9ebf0

175 Australasian Institute of Mining and Metallurgy, 'Australia's mining industry', https://www.ausimm.com/insights-and-resources/mining-industry/australian-mining-industry/

176 International Trade Administration, 'Australia – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/australia-mining

177 Australasian Institute of Mining and Metallurgy, 'Australia's mining industry', https://www.ausimm.com/insights-and-resources/mining-industry/australian-mining-industry/

178 Alexandra Eastwood, 'Counterfeit parts destroy 50L Cummins engine at WA mine', *Australian Mining*, 27 October 2023. https://www.australianmining.com.au/counterfeit-parts-destroy-50l-cummins-engine-at-wa-mine/

179 Alexandra Eastwood, 'Counterfeit parts destroy 50L Cummins engine at WA mine', *Australian Mining*, 27 October 2023. https://www.australianmining.com.au/counterfeit-parts-destroy-50l-cummins-engine-at-wa-mine/

180 Alexandra Eastwood, 'Counterfeit parts destroy 50L Cummins engine at WA mine', *Australian Mining*, 27 October 2023. https://www.australianmining.com.au/counterfeit-parts-destroy-50l-cummins-engine-at-wa-mine/

181 Alexandra Eastwood, 'Counterfeit parts destroy 50L Cummins engine at WA mine', *Australian Mining*, 27 October 2023. https://www.australianmining.com.au/counterfeit-parts-destroy-50l-cummins-engine-at-wa-mine/

182 Cummins Inc., 'Cummins in the fight against counterfeiting', Cummins newsroom, 12 December 2022. https://www.cummins.com/news/2022/12/12/cummins-fight-against-counterfeiting

183 Alexandra Eastwood, 'Counterfeit parts destroy 50L Cummins engine at WA mine', *Australian Minin* , 27 October 2023. https://www.australianmining.com.au/counterfeit-parts-destroy-50l-cummins-engine-at-wa-mine/

184 Timothy Bond, 'Counterfeit machine parts found on a Queensland mine', Australian Mining Safe to Work, 27 September 2023. https://safetowork.com.au/counterfeit-machine-parts-found-on-a-queensland-mine/

185 Tobias Alando, 'What the Intellectual Property Recordation Program means for manufacturers', Anti-counterfeit Newsletter, Eleventh Edition, Anti-counterfeit authority, 2022. https://www.aca.go.ke/images/downloads/newsletters/Newsletter-11-Edition-Anti-Counterfeit-Authority-ACA.pdf

186 Victorian Trades Hall Council's Occupational Health and Safety Unit, 'Counterfeit Components Endanger Mine Workers', 3 October 2023. https://www.ohsrep.org.au/union_news_sn_690_counterfeit

187 Queensland Mine Inspectorate, 'Counterfeit Items', Bulletin No.215(1), Queensland Resources Safety and Health, 15 September 2023. https://www.rshq.qld.gov.au/safety-notices/mines/counterfeit-items

Part IV
Conclusion


IAEA
International Atomic Energy Agency
Atoms for Peace and Development

This handbook has aimed to demonstrate how CFSIs can infiltrate the nuclear supply chain and their potential impact, by examining the threat landscape and the goods and actors involved, and through an analysis of relevant case studies.

There has been an increase in attention to CFSIs by the global nuclear community in recent years, driven by a series of high-profile cases, like the 2012-14 Republic of Korea nuclear CFSI scandal and the allegations against the Creusot Forge, as well as a heightened focus on nuclear safety following the devastating accident at Japan's Fukushima Daiichi Power Plant in 2011. Attempts to address the issue have included adjustments to quality assurance procedures, awareness-raising at international fora like the IAEA, and industry-specific guidance from organisations like the US-based Electric Power Research Institute (EPRI). Despite this, there have been some alarming developments concerning CFSIs in recent years, including a 2022 US investigation that found a downwards trend in reporting, lack of inspection on violations, and over 100 CFSI instances at American NPPs in the 2021 financial year alone.[1] Alongside supply chain shortages following the Covid-19 pandemic and use of newer technologies and distribution methods by counterfeiting networks, the threat of CFSIs remains clear and present.

What has become apparent from the research conducted for this handbook is that although there have been some efforts made on the issue of CFSIs already, there are still lessons to be learned and steps to be taken for more effective and coordinated action against counterfeit and fraudulent items. This chapter seeks to bring together the findings of the handbook alongside recommendations offered in other publications to provide a succinct series of conclusions, as well as a prompt for further efforts on tackling CFSIs in the nuclear supply chain.

The chapter is split into four sub-sections: prevention, investigation, management, and reporting. These section titles are loosely based on IAEA guidance from a 2019 technical document and have been adapted for the purposes of this handbook.[2] These conclusions could be utilised in future policy considerations and aim to serve as thinking points for stakeholders involved in the nuclear sector for further discussion on CFSIs in the nuclear supply chain. All four practices discussed in this chapter must be used together to ensure adequate mitigation of and response to CFSIs, and weaknesses in one area can have consequences for the implementation of another.

1. Prevention

Prevention policies seek to limit CFSIs entering the facility through operational strategy that is proactive and involves actors at all levels. Recommendations from existing guidance includes:[3]

- Top management being adequately trained in the risk associated with CFSIs and understanding the responsibility of addressing CFSIs in their organisation.
- Training in a range of CFSI related areas, such as ethics, and training for individuals in roles like supply, procurement, and maintenance and construction.
- Engineers involved in the procurement process better understanding their role in mitigating CFSI infiltration.
- Improved supplier selection and oversight, including audits and oversight of audits conducted.
- Better management of the procurement system, including risk management and identifying requirements.

This strategy links strongly with the issue of organisational culture and attempts to make organisations more aware of the risk that CFSIs can pose to the supply chain, including through better procurement practices. These attempts are often the first line of defence against the infiltration of CFIs into a nuclear facility, and training professionals in prevention policies can have a positive on the overall organisational culture at a nuclear facility. Furthermore, there is evidence to suggest that earlier stages of the procurement chain are more likely to have information about CFSIs and are often more directly involved, meaning that mitigation and prevention at this early stage is particularly important.[4]

Targeting procurement as a strategy for CFSI prevention can be especially useful for applying sanctions and criminal charges to deter counterfeiting networks and businesses. Better procurement practices can help actors throughout the supply chain better identify companies who may be engaging in routine and deliberate sale of CFIs, leading to swifter apprehension and halting of the network's operations.

This applied in some cases explored in the handbook, for example, in the sale of counterfeit turbine vibrometers by the Russian firm Informtech and in the sale of counterfeit chips to the US military. In both cases, counterfeit parts were identified during the procurement process, and the perpetrators arrested and charged for their crimes. In many cases however, it is difficult to apprehend the perpetrators, likely due to the significant size of the supply chain and the complexity of the procurement network. Examples of this include the counterfeit electronics trade, which spans the globe and infiltrates supply chains at rates of millions of parts every year.[5] Supporting actors from across the industry identify CFIs in various parts of the procurement chain could lead to quicker identification and help target networks that evade prosecution.

This is a strategy that many states have made an effort to implement, through new regulations, laws, guidance and training on counterfeits and quality assurance. Examples include US workshops for individuals involved in procurement on spotting CFSIs and EPRI's range of guidance documents for those working in the nuclear field.

Despite such initiatives, efforts to prevent CFSIs can be undermined by weaknesses in organisational culture. As the handbook has highlighted, there exist cases where individuals have often 'looked the other way' when faced with a CFSI. For example, in the Sellafield MOX case, several individuals involved in a final quality check were allegedly aware of the fact that false test results were being put into records and reportedly failed to report it to senior management.[6]

In another more extreme example, systematic corruption in the Korean energy industry allegedly facilitated the insertion of multiple fraudulent parts into NPPs across the country.[7] Here, there was an arguable failure of procurement personnel to recognise or report false certification, as well as instances of executives allegedly giving preferential bids and ignoring instances of falsification, as allegedly seen in the case of JS Cable.[8] These cases demonstrate how culture and commitment to prevention and safety is something that needs to be an organisation-wide mission, and involves learning and change at all tiers of an organisation.

2. Investigation

Identifying and investigating CFSIs in good time is another crucial step in mitigating the risk posed by these items and ensuring that their impact is minimal, with the part removed, if necessary, in a timely manner. Recommendations for those in the nuclear field include:[9]

- CFSI identification by inspection personnel and disposition implementation by the relevant actors.
- Inspection and acceptance testing before the part is delivered from the factory, upon receipt by the nuclear installer, before installation, and periodically during installation at a nuclear facility.
- Thorough investigation once a CFSI is suspected to be implemented at a facility.
- Sensible and adequate decision making and disposition in relation to CFIs once they are discovered at a facility.

Research conducted in this handbook found that the investigation stage is often where CFSI incidents can go intentionally, or unintentionally, unnoticed. For example, a recent investigation by the US NRC found that there was a substantial lack of investigation into reported CFSI incidents being raised by individuals at nuclear facilities.[10] This is supported with case studies like the systemic certificate falsification at Creusot Forge, where senior management at EDF allegedly failed to investigate allegations of misconduct identified by the French nuclear authority ASN years before testing revealed inconsistencies.[11] Another example discussed in the handbook is the falsification of data of MOX pellets at Sellafield, where the British Nuclear Installations Inspectorate (NII) reportedly failed to oversee quality assurance on MOX and there was a lack of investigation and checks at various stages of the manufacturing and shipping process, leading to a fear that falsified pellets could have been shipped to NPPs in several other countries.[12] In a number of case studies discussed in this handbook, CFSIs are only identified following an incident or routine test reveals that the counterfeit part is present.

However, there are a number of cases where appropriate action upon discovery of CSFIs was taken. The aforementioned Creusot Forge example is an example of this, as although there had been a severe lack of checks historically, once the fraudulent certificates were uncovered, ASN took swift and decisive action to address the issue. As highlighted in the case study, this involved public consultations, transparency about the misconduct, the shutting of multiple reactors to replace parts, and an independent investigation into the plant by a host of foreign countries. The discovery of systematic integration of CFSIs into the Korean nuclear industry is another example where thorough investigation and rigorous action was taken upon discovery of falsified parts. This case study discussed how the Korean nuclear authority and KHNP took extensive measures, including checking quality assurance certificates of all safety-related items at Korean NPPs, to uncover CFIs at their facilities.

Here the challenge is a shortfall of investigations at every stage of the procurement chain. CFSIs are often only discovered once they have been implemented, and the majority of the cases discussed in this handbook show how counterfeits can go undetected in a nuclear installation for years without being noticed. Investigation after installation is still a positive step towards CFI elimination, but better inspection of factories or receipt inspection could be a useful tool for actors to ensure that CFSIs do not slip through the net and can be identified before installation.

3. Post-Incident Management

Creating a comprehensive risk management strategy is important for ensuring that when a CFI is identified at a facility, there is a full-proof and effective plan to address these items. A step-by-step guide is important to establish so that employees are aware of a routine that needs to be followed once a CFI has been discovered. The IAEA discusses a typical strategy in its guidance, including:[13]

1. Quarantining the item.
2. Recording the incident in the organisation's corrective action programme.
3. Assessing the immediate operational and safety implications and performing an extent of condition review.
4. Notifying the relevant internal authority.
5. Gathering further information.
6. Considering reporting preliminary findings to industry databases.
7. Contacting the appropriate actors in the supply chain for information about any related incidents or other cases of CFSI investigation.
    a. This needs to be done with some care as the information could invertedly reach the counterfeiting network, who may destroy all evidence.
8. Inspect, test, review or take other actions to determine whether the item is in fact counterfeit, or is simply non-conforming.
9. Once the CFI is confirmed, physically dispose of the item.

The steps outlined above are standard practice and reflect the CFSI post-incident risk management system of many organisations. While this is a useful methodology for risk management, there have been some insights uncovered through the research in this handbook which could be beneficial to consider alongside this template.

There was evidence found in the case studies that appropriate measures are being taken following the discovery of a CFSI. For example, there was swift action taken upon the discovery of CFIs, including the Republic of Korea case where all quality certificates for safety-related items were checked at all NPPs across the country after multiple fraudulent certificates were discovered.[14] Furthermore, in a Canadian case involving fraudulent operational amplifiers, the team at the plant made sure to document the presence of the 50 counterfeit items in their corrective action programme.[15] In an American case involving counterfeit circuit breakers, the relevant authority, here the Consumer Product Safety Commission, contacted relevant actors in the supply chain to ensure that there were no further incidents involving the fraudulent parts.[16] Generally, the case studies demonstrated that there was more issues with mitigation strategies than post-incident risk management, and most examples explored in the handbook indicated that appropriate steps were taken when operators were faced with a CFSI.

4. Reporting

Reporting is another crucial step in CFSI response, with information sharing and transparency being an important tool for addressing CFI incidents in a timely and efficient manner, and to help limit the potential for future events. Suggestions for the implementation of this include:[17]

- Internal communication within the organisation.
- External information sharing with other organisations and countries.
- Whistle-blowers being protected when they raise a CFSI incident.

There have been some significant improvements in this area that have actively helped reduce the risk of CFSIs in the nuclear supply chain. One relevant example is the UAE's transparent quality assurance programme, which regularly shares information it learns, such as knowledge of untrustworthy suppliers, with the international community.[18] Reporting databases are recommended by groups like the World Nuclear Association (WNA), which notes that although some national and supranational databases exist, there is opportunity to develop international information sharing initiatives, like the Nuclear Energy Agency's protocol to report and distribute information about CFSIs detected and their safety significance between regulatory bodies.[19]

On a more localised level, initiatives like the nuclear safety ombudsman established in the Republic of Korea after the certification falsification investigations help encourage anonymous reporting of CFSI incidents, protecting those who wish to raise a complaint but are worried about potential repercussions.[20]

However, there is still much work to be done on this issue. A 2022 report by the NRC found that there was a lack of communication between different NPPs in different regions when a CFSI incident was raised.[21] This could lead to differences in responses and solutions between different facilities, making nationwide coordination on CFSI response more difficult. The handbook has highlighted a number of cases when counterfeits infiltrated multiple NPPs across a country or region, including the US Square-D case, The French Creusot forge case, and fraudulent fire detection equipment in Japan.

In most of these instances, there was good communication between NPPs, usually due to the electric companies involved holding monopoly over most plants, but there could be instances where communication is subpar, having detrimental consequences. With the Creusot forge case, for example, there were reports of alleged misconduct raised in previous years but it appeared that this concern was not raised with the power plants and facilities that could be impacted.[22]

Furthermore, information sharing and reporting of incidents to industry databases is a promising potential tool for helping mitigate any further risk of CFIs, as well as identifying if the incident that occurs at a particular facility is the work of a wider campaign. There are currently few databases of this nature that exist, and few that share this information internationally.[23] Many of the cases identified in this handbook involve products that were likely shipped from abroad and crossed a number of jurisdictions to arrive at their end destination. Better international information sharing on CFSIs and counterfeiting networks in the industry could be useful in helping raise global awareness of CFSIs and how they can be disseminated across various countries, impacting several facilities. For example, some of the cases in this handbook involve counterfeit electronic parts, which tend to be transhipped through multiple FTZs and ports and often originate from China. This means that the parts could potentially be intercepted in multiple jurisdictions before they reach the customer. Better information sharing throughout the industry and supply chain could not only help customers be more vigilant of the parts they are sold, but also raise awareness of suppliers in other countries who may be selling fake parts, or help sellers identify if the parts they are sourcing come from a legitimate place of origin.

References

1 United States Office of the Inspector General and United States Nuclear Regulatory Commission, 'Special Inquiry into Counterfeit, Fraudulent, and Suspect Items in Operating Nuclear Power Plants', OIG Case No. 20-022, 9 February 2022. https://www.nrc.gov/docs/ML2204/ML22040A111.pdf

2 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

3 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

4 World Nuclear Association Supply Chain Working Group, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', World Nuclear Association, 2019-005, August 2019. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

5 Organisation for Economic Co-operation and Development and European Union Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019, p. 3. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en; United States Senate Committee on Armed Services, 'Inquiry into Counterfeit Electronic Parts in the Department of Defence Supply Chain', 112th Congress, 2nd Session, Report 112-167, 21 May 2012. https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf

6 The Parliamentary Office of Science and Technology, 'Mixed Oxide Nuclear Fuel (MOX)', Post 137, April 2000. https://www.parliament.uk/globalassets/documents/post/pn137.pdf

7 Philip Andrews-Speed, South Korea's nuclear power industry: recovering from scandal, *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010

8 Ilchong Nam and Geoffrey Rothwell (eds.), 'New Nuclear Power Industry Procurement Markets: International Experiences', KDI Research Monograph, Vol. 1, December 2014; Philip Andrews-Speed, 'South Korea's nuclear power industry: recovering from scandal', *The Journal of World Energy Law & Business*, Vol. 13, No. 1, March 2020, pp. 47–57. https://doi.org/10.1093/jwelb/jwaa010

9 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

10 United States Office of the Inspector General and United States Nuclear Regulatory Commission, 'Special Inquiry into Counterfeit, Fraudulent, and Suspect Items in Operating Nuclear Power Plants', OIG Case No. 20-022, 9 February 2022. https://www.nrc.gov/docs/ML2204/ML22040A111.pdf

11 Sylvain Tronchet, 'Cuve de l'EPR de Flamanville: l'incroyable légèreté d'Areva et EDF', Radio France Inter, 31 March 2017. https://www.radiofrance.fr/franceinter/cuve-de-l-epr-de-flamanville-l-incroyable-legerete-d-areva-et-edf-4103446

12 The Parliamentary Office of Science and Technology, 'Mixed Oxide Nuclear Fuel (MOX)', Post 137, April 2000. https://www.parliament.uk/globalassets/documents/post/pn137.pdf

13 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

14 Sang-Jong Lee, 'Korean Industry Perspective on CFSI', NRC Workshop on Vendor Oversight, Portland, Oregon, delivered 12 June 2014, https://www.nrc.gov/docs/ML1415/ML14153A200.pdf; Ilchong Nam and Geoffrey Rothwell (eds.), 'New Nuclear Power Industry Procurement Markets: International Experiences', *KDI Research Monograph*, Vol. 1, December 2014. https://www.econstor.eu/bitstream/10419/200944/1/kdi-res-monograph-2014-01.pdf

15 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

16 United States Nuclear Regulatory Commission, 'Counterfeit Parts Supplied to Nuclear Power Plants', NRC Information Notice 2008-04, 7 April 2008. https://www.nrc.gov/docs/ML0807/ML080790266.pdf

17 International Atomic Energy Agency, 'Managing Counterfeit and Fraudulent Items in the Nuclear Industry', IAEA Nuclear Energy Series, No. NP-T-3.26, 2019. https://www.iaea.org/publications/11182/managing-counterfeit-and-fraudulent-items-in-the-nuclear-industry

18 Emirates Nuclear Energy Corporation, 'Lessons Learned from the Nuclear Industry', 2022. https://www.enec.gov.ae/barakah-plant/lessons-learned-from-nuclear-industry

19 World Nuclear Association Supply Chain Working Group, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', World Nuclear Association, 2019-005, August 2019. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

20 Nuclear Safety and Security Commission, 'NSSC To Operate "Nuclear Safety Ombudsman" To Root Out Corruptive Actions', 4 June 2013. https://www.nssc.go.kr/en/cms/FR_BBS_CON/BoardView.do?pageNo=93&pagePerCnt=10&MENU_ID=90&CONTENTS_NO=&SITE_NO=3&BOARD_SEQ=1&BBS_SEQ=11959&USER_NAME=&TEL_NO=&WRITER_DI=&_csrf=&SEARCH_FLD=&SEARCH=

21 United States Office of the Inspector General and United States Nuclear Regulatory Commission, 'Special Inquiry into Counterfeit, Fraudulent, and Suspect Items in Operating Nuclear Power Plants', OIG Case No. 20-022, 9 February 2022. https://www.nrc.gov/docs/ML2204/ML22040A111.pdf

22 Sylvain Tronchet, 'Cuve de l'EPR de Flamanville: l'incroyable légèreté d'Areva et EDF', *Radio France Inter*, 31 March 2017. https://www.radiofrance.fr/franceinter/cuve-de-l-epr-de-flamanville-l-incroyable-legerete-d-areva-et-edf-4103446

23 World Nuclear Association Supply Chain Working Group, 'Countering Counterfeit, Fraudulent and Suspect Items in the Nuclear Supply Chain', World Nuclear Association, 2019-005, August 2019. https://world-nuclear.org/images/articles/REPORT-countering-counterfeit.pdf

Disclaimer

The authors of this report invite liberal use of the information provided in it for educational purposes, requiring only that the reproduced material clearly cite the source, with the following elements to be included (in any reasonable referencing format): *Securing the Nuclear Supply Chain: A Handbook of Case Studies on Counterfeit, Fraudulent and Suspect Items*, by Professor Christopher Hobbs, Zoha Naser, Dr Daniel Salisbury and Dr Sarah Tzinieris, Department of War Studies, King's College London, 2024.

The material in this document should not be used in other contexts without seeking explicit permission from the authors.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS

ISBN: 978-1-908951-52-6