NUCLEAR SECURITY IMPLICATIONS OF COUNTERFEIT, FRAUDULENT AND SUSPECT ITEMS ENTERING THE NUCLEAR SUPPLY CHAIN

C. HOBBS
King's College London
London, United Kingdom
Email: christopher.hobbs@kcl.ac.uk

Z. NASER
King's College London
London, United Kingdom

D. B. SALISBURY
King's College London
London, United Kingdom

S. TZINIERIS
King's College London
London, United Kingdom

Abstract

The paper presents the preliminary findings of research conducted by King's academics as part of an IAEA Coordinated Research Project (CRP) on counterfeit, fraudulent and suspect items (CFSIs). It explores how and why CFSIs have entered supply chains in the nuclear industry and other critical sectors, through examining the role of key actors and real-life incidents. The research discusses emerging trends and their relevance for the nuclear industry and illustrates how networks supplying counterfeit items operate in certain geographic hotspots and exploit legitimate channels of international trade to facilitate their operations. The research also reveals the potentially significant and wide-ranging impact of counterfeit and fraudulent items (CFIs) in critical sectors, which include financial, reputational and physical consequences such as the severe degradation of operational, safety and security systems. At present there is relatively little information available publicly on incidents involving CFIs and one of the major goals of this research is to unearth cases that improve international understanding of both the threat and how systems can be strengthened to prevent, detect and respond to this relatively unexplored aspect of nuclear security and safety.

1. INTRODUCTION

According to a 2021 study by the Organisation for Economic Co-operation and Development (OECD), trade in CFIs accounts for an estimated 2.5% of world trade [1]. This is exacerbated by supply chain interruptions, caused by factors like the Covid-19 pandemic, which can serve to increase the vulnerability of industrial actors to these products. CFIs do not undergo the rigorous quality assurance procedures that legitimate items do and may also deviate from prescribed specifications. These items can be found in a range of industries and commercial sectors, including fashion, electronics, pharmaceuticals and the aerospace industry. This paper focuses in particular on CFSIs in the nuclear sector, primarily in civil nuclear facilities.

The inadvertent or malicious insertion of CFIs into the nuclear supply chain can diminish the integrity of equipment, systems, structures, components or devices, posing a significant risk to nuclear operations, and associated security and safety systems. These items

can enter at various stages of the supply chain, be it in the form of raw materials and parts in the early manufacturing phase, or as whole components and items at later stages [2]. Once inserted, CFIs can leave crucial aspects of a nuclear facility vulnerable to deliberate interference or the misfunctioning or failure of specific equipment or systems, creating the potential for security incidents or accidents. For example, fasteners for securing heavy items are widely used in a range of industrial settings; however, those employed in nuclear installations need to meet specific high stress, heat and other quality requirements for safe and proper use. If standard industrial fasteners, sold with falsified certification, were to be installed at a nuclear facility without passing quality assurance testing, these bolts may not be as robust as they appear. This could pose a significant risk of an accident or even deliberate manipulation by an adversarial actor.

The paper presents preliminary findings of research presented by King's academics as part of an IAEA CRP on the 'Nuclear Security Implications of Counterfeit, Fraudulent, and Suspect Items (CFSI)', focused on furthering understanding of risks in this area through analysing cases of CFIs in nuclear and other critical sectors [3]. The culmination of this research will be a handbook of comprehensive case studies and lessons on CFSIs in the nuclear industry, with the aim of helping IAEA member states and organisations conceptualise and address the risk that CFSIs pose to nuclear and radiological facilities.

The article begins by providing a brief overview of CFSIs in the nuclear supply chain, including the parts vulnerable to counterfeiting. It then discusses the primary threat actors involved in counterfeiting operations in this sector. The paper then goes on to discuss the dissemination of CFSIs in the supply chain, including the target markets for these goods and the innovative methods that nefarious actors use to deliver the items to customers. Finally, it provides some short cases studies where CFIs have been inserted into nuclear and non-nuclear industries, with analysis of the impact this can have. To conclude, the paper discusses how the international community can take steps to mitigate the risks posed by CFIs.

2. OVERVIEW OF CFSIs

CFSIs can potentially manifest in a variety of ways at a nuclear facility, from their installation on key primary systems, like reactors, to subsidiary supporting systems, such as fire safety equipment or physical protection technology. Counterfeit and fraudulent objects can also range from raw materials and parts, to more complex electrical items or generators. A simple taxonomy of parts to be at risk of counterfeiting, as identified by the United States Department of Energy, includes [4]:

- **General items** – Lubricants, adhesives, flanges, etc.
- **Electrical items** – Starting coils, fuses, AC inverters, etc.
- **Mechanical items** – Rods, wires, valves, etc.
- **Diesel generator items** – diesel speed governors, diesel injection pumps, and diesel fuel transfer pumps
- **Lifting materials** – Slings, cables, hooks, etc.

Despite the term 'counterfeit and fraudulent *items*', definitions of CFIs typically also include fraudulent services and paperwork. This typically involves individuals engaging in dishonest conduct and claiming to have offered a particular service or completed a certain action when they have not done so. Examples of this could include entering false data into

records, cheating on an examination, and forging signatures on certificates [5]. The range of items and services included under the banner of CFSIs means that vigilance is required across the supply chain, and not just at certain critical procurement stages. Individuals could unknowingly install a CFI from a legitimate trusted supplier, unaware that the item has been counterfeited or fraudulently manufactured at an earlier stage of production. CFI infiltration into the nuclear supply chain has been documented by a range of organisations and government agencies since the 1980s. For example, a United States Nuclear Regulation Commission (NRC) bulletin in June 1987 outlines how substandard and potentially counterfeit fasteners had been installed at nuclear power plants (NPPs) across the country [6]. The NRC continues to release bulletins and information notices following significant CFI incidents and is just one of the many national authorities releasing information like this [7].

The authors of the paper emphasise the importance of an integrated approach to nuclear safety and security and discuss how CFIs can have a critical impact on safety and security at NPPs. As with any nuclear incident, safety risks can create security shortcomings and vice versa. This poses a significant threat as even if the installer does not have harmful intentions, an ensuing security crisis could be generated if a more malicious actor exploits the weakness created by the CFI. For example, an electronic component that does not meet quality assurance specifications and is installed in a NPP surveillance system could render the system ineffective. If adversarial actors were to become aware of this, they could exploit this weakness and create a security breach. Similarly, an insider adversary could deliberately install a CFI to create a weakness at the NPP, and this could impact safety equipment. If safety systems fail during an accident, this could create a huge radiological risk to people and the wider environment.

3. CFI THREAT ACTORS

There are a variety of actors in the nuclear supply chain, illustrated in Figure 1, who could serve as facilitators to the installation of CFIs in nuclear facilities. These actors could be present at earlier manufacturing stages sourcing fraudulent materials and parts or could be the end customer knowingly procuring counterfeit items from an illegitimate firm. Furthermore, deception could be simple and occur in one stage, or could be more complex network operation, and involve several individuals using various methods at different levels of the production and procurement process.

FIG. 1. Notional supply chain for tangible CFIs.

3.1 Manufacturers

The manufacturing stage is where objects are knowingly produced as counterfeits of genuine articles, and the actors and their networks can range significantly in methods and size of operation. Smaller, more localised networks may consist of a single person or small group

manufacturing these products. Larger operations can be transnational, involving factories mass-manufacturing CFSIs and generating larger profits than smaller operations.

3.2 Intermediaries

Intermediary actors are individuals and firms that may perform a variety of counterfeiting roles, from manipulating genuine items produced by legitimate suppliers to make them appear of higher specification, to peddling, distributing and brokering already counterfeited products to customers. These actors help disseminate CFSIs into the supply chain and embed them into critical industrial installations. Whereas it can be difficult to trace manufacturers, intermediary actors are major players in supply chain networks and are often easier to trace in investigations. A significant group in this category are E-waste harvesters, who use crude methods to 'recycle' old or faulty chips and sell them on as legitimate semiconductors. These chips are already difficult to manufacture and even legitimate parts can be prone to failure, so counterfeited and poorly recycled semiconductors produced by unqualified individuals pose a great risk of malfunctioning. This challenge is illustrated in the 2011 testimony by the President of the Semiconductor Industry Association, which claimed that counterfeiting operations cost American semiconductor companies over US$7.5 billion a year and that at the time of the testimony, up to 15% of all spare and replacement chips purchased by the Department of Defense were counterfeit [8]. The recent semiconductor shortage that came about during the Covid-19 pandemic heightened the risk of these counterfeit chips entering critical industrial supply chains as the disruption caused customers to seek out recycled and resold chips, buying from a wider range of sellers, some of which were not legitimate [9].

3.3 Customers

Finally, customers also have a crucial role to play in the infiltration of CFSIs in the supply chain. It is often the duty of customers, especially in critical industries like nuclear, to ensure that parts sourced meet quality assurance requirements and that any parts that are identified as counterfeit are immediately flagged for further investigation [10]. Customers can be unintentional or intentional participants when it comes to embedding CFSIs. Sometimes customers purchase items from legitimate suppliers, unaware that these have been counterfeited earlier in the supply chain, or they can be duped into believing that their supplier is providing them with a genuine item. Other times however, elements of customer organisations – posing a form of 'insider threat' – may intentionally seek out cheaper routes for sourcing items, purchasing them from illegitimate or unverified suppliers with the knowledge that they could be counterfeit or substandard.

4. MARKETS AND GEOGRAPHIES OF CFSIs

CFI networks operate across the globe, although they often target particular jurisdictions or marketplaces where there exists a lax regulatory environment. For example, the growth of online marketplaces has helped bolster the transfer and sale of CFIs. In particular online shopping grew in popularity during the Covid-19 pandemic, when supply chain shortages drove many organisations to utilise E-commerce platforms like eBay and Amazon to procure products. These sites are key markets for counterfeiters as it is easy to distribute parts to customers around the world with minimal checks and balances. A 2020 investigation by *Which?*, a British consumer advisory organisation, found that some sellers were abusing the

ratings system to market counterfeit electronic device chargers to customers and that this was going largely undetected by eBay [11]. A wide variety of products are available on these online market places, including safety-critical devices fire alarms, manufacturing parts and electronic items. If a nuclear organisation were to purchase goods via an online marketplace, they could be at risk of sourcing parts that do not come from legitimate sellers. Evidence to support this includes a 2021 report by the OECD and European Union Intellectual Property Office (EUIPO) that found 7% of counterfeit electrical equipment and machinery seized in the European Union (EU) was sourced from E-commerce platforms [12]. Given the number of key industrial and dual-use items sourced from online marketplaces, both large and public like Amazon or more specialist online platforms for industries such as aerospace, nefarious actors could potentially make use of these to disseminate CFI products on a global scale.

In disseminating CFIs, nefarious actors frequently use complex routings and operate in particular types of jurisdictions. For example, multiple transhipment hubs are often utilised by actors involved in CFIs, to mask their origin and to establish distribution hubs for the objects close to some of the largest international container ports in the world [13]. By establishing complex routes with multiple ports of call in between, the movement of these items becomes harder for authorities to track and monitor. The point of origin of the items also become more difficult to uncover, and transhipping items in multiple jurisdictions means authorities need to collaborate to monitor transnational supply chains, which ultimately makes interdiction of shipments more difficult. CFIs are also regularly moved through, and manipulated in, loosely regulated free trade zones (FTZs). FTZs are designed to operate with limited regulation to help facilitate international trade; however, while this supports legitimate business, it can also be exploited by CFI actors, who use the lax oversight of FTZs to their advantage [14]. Transhipment hubs and FTZs frequently used by those moving CFSIs are found on major shipping routes, and particularly in jurisdictions such as China, the United Arab Emirates and Singapore [15].

The handbook, to be released once the research has been completed, explores these issues in further depth, with a detailed discussion of the geographic hotspots for the dissemination of certain CFSIs, such as electronic items, and jurisdictions that may pose a future risk. For example, the handbook touches on North Korean counterfeit networks and how these could potentially be an area of concern to consider in the future considering the history of illicit trade stemming from the country.

5. CASE STUDIES

While information on CFIs remains relatively scarce, there exists a number of previous cases of CFI incidents. Analysing these provides insights into both their impact and how they were able to successfully defeat supply chain security measures, serving useful lessons for CFI prevention, detection and response programmes. To this end, three case studies from both nuclear and non-nuclear industries are explored in this section.

5.1 Counterfeit Square-D circuit breakers

In 2006, the US Consumer Product Safety Commission (CPSC) announced three separate recalls of circuit breakers with the label ‘Square-D’, believing them to be counterfeit. An estimated 144,000 units of circuit breakers were believed to have been distributed to customers nationwide [16]. This particular brand of consumer-grade circuit breakers were also

installed in a number of NPPs across the United States, creating fears that the counterfeit parts could be present at any one of these power plants. Although the NRC was able to rule out the presence of the parts at most of the plants, they could not confirm that the circuit breakers at one plant were genuine and so replaced them to be safe. There was no incident associated with these breakers reported but the potential risk that they posed was very serious and necessitated their recall. Shortly after the incident, the Los Alamos National Laboratory estimated that approximately half-a-million counterfeit Square-D circuit breakers had entered the US domestic market between 2005 and 2008 [17]. Electronics counterfeiting is a major issue in a number of industries, not just nuclear, with the vast majority of parts coming from China [18]. This case highlighted the need for operators to be vigilant about parts, no matter how small and insignificant they may appear, and to be aware of the risk of counterfeiting in a globalised market.

5.2 Falsified quality assurance certificates at a French forge

The Creusot Forge is a facility in France that specialises in manufacturing heavy components, including the large steel forgings and castings used in nuclear installations like reactor vessels and coolant pumps. The plant supplies parts to a number of NPPs in France and around the world; it also supplied the vessel head at Flamanville NPP. Routine testing on reactor heads spurred French firm Areva to test reactor vessel heads at a number of its NPPs, and tests at Flamanville revealed inconsistencies in the metallurgical composition of the vessel head and end at the plant. This posed a risk as it could mean that the structural integrity of critical safety and security-related equipment at the plant was compromised. Areva began a wider internal investigation into manufacturing work, focusing closely on the Creusot forge. They found inconsistencies and evidence of record tampering dating back decades, suggesting that hundreds of parts manufactured at the plant could be fraudulent [19]. In addition to this, regulatory bodies like the French Nuclear Safety Authority (ASN) had contacted Le Creusot about potentially fraudulent activity and substandard items in the early 2000s, but little had been done to address concerns. The impact on the French nuclear industry was significant, with up to 22 reactors shut down for investigation and parts replacement initiated in June 2016 [20]. In addition, Le Creusot had supplied parts to NPPs in other countries, including the United Kingdom, the United States and China, creating concern that the fraudulent activity could impact power plants abroad. The forge remained shut until all plants were cleared to restart and it resumed operation in April 2017.

5.3 Aeroplane crash caused by counterfeit bolts

On 8 September 1989, Norwegian charter airline Partnair flight 394 departed Oslo on a flight bound for Hamburg, Germany. As the aircraft neared the Danish coast, Danish air traffic control noticed that the plane was veering off course and falling at a rapid rate. Flight 394 subsequently crashed in the ocean off the Danish coastal town of Hirtshals, with all 55 people on board being killed [21]. Theories explored by an international aviation investigation team contained a range of possibilities, including a potential terror attack as the accident occurred less than a year after the bombing of Pan Am Flight 103 in December 1988. However, further investigation revealed that counterfeit bolts were to blame for the deadliest accident in Danish aviation history [22]. Investigators had discovered a range of issues with the aircraft, including a broken auxiliary power unit (APU) mount. The APU was not typically utilised and was there as a back-up but had been deployed by the pilots due to issues with the main power generators. The three bolts installed in the fin of the plane impacted the structural integrity of the tail causing it to vibrate; when combined with vibrations from the broken APU mount, resonance

occurred, amplifying vibration in the tail until it fell off, leading to the crash [23]. The case brought much needed attention to the issue of counterfeits in the global aviation industry, prompting stricter oversight and regulation of parts. Despite this, counterfeits are once more in the public consciousness as a high-profile case currently in the British judicial system explores the possibility that a British firm may have allegedly sold thousands of counterfeit parts to major airlines across the world [24]. This demonstrates that while some lessons have been learnt and some action taken, the risk that CFSIs pose still needs to be addressed. As well as this, it demonstrates the financial risk that can be created through CFSI infiltration. Partnair, the airline responsible for the flight, was already dealing with a host of financial issues, which could have led to the implementation of the counterfeit bolts. The crash was the final straw for the airline and the company filed for bankruptcy shortly after the accident [25]. The potential consequences of a CFSI entering the system and creating an accident of this dimension serves to highlight not only the risk to life and infrastructure, but the risk to business that can come from negative press and costly repairs.

7. CONCLUDING REMARKS

This paper has presented ongoing research by King's College London on the issue of CFIs in nuclear supply chains, as part of a CRP for the IAEA. Initial findings demonstrate how CFIs have already infiltrated certain areas of the nuclear supply chain. Through careful analysis of the goods, actors and geographies involved, the authors have identified a number of insights that could be helpful in better understanding how CFSIs go undetected. This includes the use of complex shipping routes and transhipment through FTZs to help evade monitoring, targeting of certain parts like electronic components that are a vulnerable market due to supply chain shortages, and exploiting lack of industry knowledge on CFSIs, to name a few. The team also identified a series of weaknesses that counterfeiting networks exploit to help peddle counterfeits in the supply chain. Examples of the factors identified include weak organisational culture and ethics, lax procurement functions, and poor quality assurance, quality control, audit, and inspection mechanisms. The case studies employed in the research provide crucial evidence to support these points and help pinpoint key areas and lessons that need to be addressed by policy and industry actors in future discussions on CFSIs.

ACKNOWLEDGEMENTS

The authors would like to thank the other participants of the IAEA Coordinated Research Project (CRP) for their feedback and insight on this research. The CRP brings together research institutes in both developing and developed IAEA Members States to collaborate on research topics of common interest.

REFERENCES

[1] Organisation for Economic Co-operation and Development and European Union Intellectual Property Office, 'Global Trade in Fakes: A Worrying Threat', OECD Publishing, Paris, 22 June 2021. https://doi.org/10.1787/74c81154-en

[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] International Atomic Energy Association, 'Nuclear Security Implications of Counterfeit, Fraudulent, and Suspect Items (CFSI)', December 2022. https://www.iaea.org/projects/crp/j02019

[4] Office of Corporate Safety Analysis, 'Suspect/Counterfeit Items Awareness Training', United States Department of Energy Office of Health, Safety and Security, Washington D.C., June 2007. https://www.energy.gov/sites/prod/files/2014/06/f16/SCI_Training_Manual.pdf

[5] 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

[6] United States Nuclear Regulatory Commission Office of Nuclear Reactor Regulation, 'NRC Compliance Bulletin No.87-02: Fastener Testing to Determine Conformance with Applicable Material Specifications', 6 November 1987. https://www.nrc.gov/docs/ML0312/ML031210865.pdf

[7] United States Nuclear Regulatory Commission, 'Guidance Documents and Background Information for Counterfeit, Fraudulent, and Suspect Items (CFSI)', undated. https://www.nrc.gov/about-nrc/cfsi/guidance.html

[8] Semiconductor Industry Association, 'Detecting and Removing Counterfeit Semiconductors in the U.S. Supply Chain', ACTF Whitepaper, June 2018. https://www.semiconductors.org/wp-content/uploads/2018/06/ACTF-Whitepaper-Counterfeit-One-Pager-Final.pdf

[9] Aaron Aboagye, Ondrej Burkacky, Abhijit Mahindroo, Bill Wiseman, 'When the chips are down: How the semiconductor industry is dealing with a worldwide shortage', World Economic Forum, 9 February 2022. https://www.weforum.org/agenda/2022/02/semiconductor-chip-shortage-supply-chain/

[10] United States Department of Energy, 'Suspect/Counterfeit Items Resource Handbook', Washington DC, January 2017. https://www.standards.doe.gov/standards-documents/1200/1221-BHdbk-2016-CN1-2017/@@images/file

[11] Hannah Walsh, 'How eBay's review system is promoting fake, counterfeit and even dangerous products', *Which?*, 13 March 2020. https://www.which.co.uk/news/article/ebay-customer-reviews-aDd0j0g9ewIk

[12] OECD 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

[13] OECD and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

[14] Andrea Viski and Quentin Michel, 'Free Zones and Strategic Trade Controls', Strategic Trade Review, Vol. 2, No. 3, Autumn 2016. http://www.str.ulg.ac.be/wp-content/uploads/2016/10/Free-Zones-and-Strategic-Trade-Controls.pdf

[15] OECD and EU Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods', 18 March 2019. https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en

[16] United States 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; United States 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; United States 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

[17] 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

[18] Organisation for Economic Co-operation and Development and European Union Intellectual Property Office, 'Global Trade in Fakes: A Worrying Threat', OECD Publishing, Paris, 22 June 2021. https://doi.org/10.1787/74c81154-en

[19] Nuclear Safety Authority of France, '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

[20] Nuclear Safety Authority of France, '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

[21] 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

[22] Aviation Safety Network, 'ASN aircraft Convair CV-580 LN-PAA Hirtshals [Skagerrak]', accessed 19 February 2024. https://aviation-safety.net/database/record.php?id=19890908-0

[23] 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

[24] 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/

[25] 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