

Counterfeit and fraudulent parts: Improving prevention and detection

By Marc Tannenbaum

The threat of counterfeit and fraudulent items (CFI) finding their way into nuclear plants is not new, but it has gained increased attention due to recent high-profile events such as those experienced by the nuclear industry in South Korea. Concern originally emerged in the late 1980s because of several incidents involving fraudulent commodity items such as piping components and refurbished molded-case circuit breakers being sold as new. These concerns prompted efforts by both the U.S. Nuclear Regulatory Commission and the U.S. commercial nuclear industry to improve the ability to detect fraudulent items.

In the late 1980s, the NRC published Information Notice 89-70, *Possible Indications of Misrepresented Vendor Products* [1], and Generic Letter 89-02, *Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products*. [2] Information Notice 89-70 discussed factors that could be used by licensees to detect procurements involving fraudulent items, such as unusually low cost, unusually short delivery times, signs of refurbished parts, and other indications. Generic Letter 89-02 discussed elements of procurement programs that licensees should consider to enhance the ability to detect fraudulent items, such as engineering involvement in the procurement process, effective inspection and testing, and engineering-based dedication of commercial-grade items used in safety-related applications.

Marc Tannenbaum (<mtannenbaum@epri.com>) is a Principal Technical Leader at the Electric Power Research Institute, where he leads research in the areas of procurement engineering and supply chain management.

The U.S. NRC and commercial nuclear industry are making efforts to keep counterfeit and fraudulent parts out of the nuclear industry's supply chain, especially where safety-related parts and components are concerned.

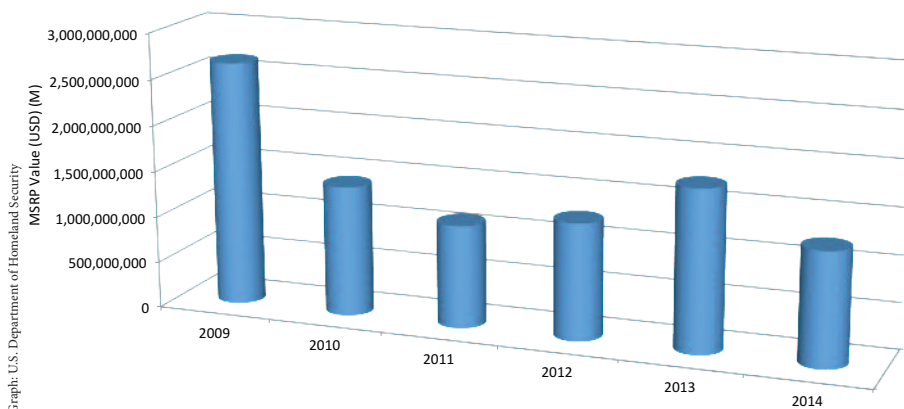


Fig. 1. Value of goods seized at manufacturer's suggested retail price

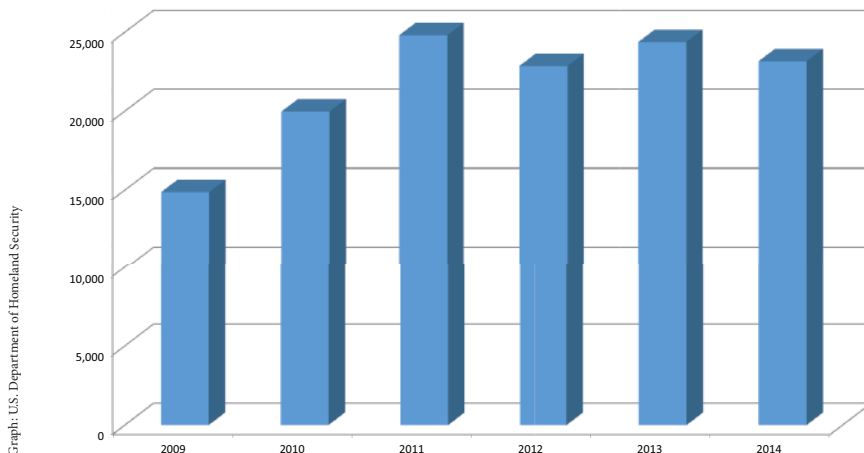


Fig. 2. Number of seizures of suspected counterfeit goods

The NRC's Vendor Inspection Program

The use of commercial-grade parts—as well as other items not specifically intended for nuclear use—in new reactor projects and in operating reactors is regulated through the Nuclear Regulatory Commission's Vendor Inspection Program (VIP). The program is carried out through the Division of Construction Inspection and Operational Programs in the Office of New Reactors (NRO).

The VIP verifies that reactor applicants and licensees are fulfilling their regulatory obligations with respect to providing effective oversight of the nuclear supply chain. The program accomplishes this through a number of activities, including the performance of limited-scope targeted inspections of the vendor's quality assurance program; the establishment of a strategy for the identification and selection of vendors to sample the effectiveness of the domestic and international supply chains for the current fleet of reactors and new reactor construction; and ensuring that vendor inspectors obtain the necessary knowledge and skills to perform inspections. The VIP also addresses interactions with nuclear consensus standards organizations, industry and external stakeholders, and international constituents.

The program's staff conducts inspections at vendors' facilities to verify that their quality assurance programs are effectively implemented and comply with applicable regulatory requirements, including 10 CFR Part 21 (which covers counterfeit, fraudulent, and suspect items), and the licensee-imposed requirements of Appendix B to 10 CFR Part 50, as well as with other codes and standards. The goal is to ensure that plants are properly overseeing their supply chain and reporting defects

and noncompliance issues.

The Center of Expertise, formed within NRO and the Office of Nuclear Reactor Regulation (NRR) and now operating out of NRO, conducts both routine and reactive inspections. Reactive inspections are conducted in response to allegations, previous inspection findings, and reports submitted under 10 CFR Part 21 or 10 CFR 50.55(e), or based on information that indicates that a vendor may not be meeting NRC requirements. In particular, the center aims to confirm that effective controls are in place to prevent counterfeit or fraudulent parts from entering the U.S. safety system supply chain. The efforts have so far been successful, as the NRC notes that it has not seen any instances of such parts in U.S. nuclear plant safety systems.

The staff communicates with other divisions within NRO and with NRR, as well as with numerous organizations outside the NRC, including ANS, the American Society of Mechanical Engineers, the Institute of Electrical and Electronics Engineers, the Electric Power Research Institute, the International Laboratory Accreditation Cooperation, the Multinational Design Evaluation Program, the Nuclear Energy Institute, and the Nuclear Procurement Issues Committee. Interaction with other stakeholders related to counterfeit, fraudulent, and suspect items issues—the U.S. Departments of Energy, Homeland Security, Labor, Justice, and Transportation, and the National Aeronautics and Space Administration and the Food and Drug Administration—keeps NRO informed of vulnerabilities in the procurement processes and allows for sharing best practices for preventing counterfeit and fraudulent parts from making their way into the supply chain.

Generic Letter 89-02 also conditionally endorsed EPRI NP-5652, *Guidance for the Utilization of Commercial Grade Items in Safety-Related Applications*. [3] Another EPRI document, *Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants* (EPRI NP-6629), provided specific inspection criteria for identifying fraudulent items upon receipt. Licensees institutionalized this guidance in their inspection procedures, providing U.S. nuclear plants with an enhanced ability to identify and reject items exhibiting signs of being fraudulent or counterfeit during receipt inspection.

Globalization of the supply chain and the resulting ease with which manufacturing technologies can be acquired has contributed to increased manufacturing of counterfeit items. For example, in the United States there were 23,140 seizures of counterfeit goods in 2014, representing a value of \$1.23 billion at manufacturers' suggested retail prices. [4] Figures 1 and 2 illustrate the magnitude of the problem and the trend in seizures over the past few years.

While about 70 percent of the seizures in 2014 involved items such as watches, jewelry, handbags, wallets, and apparel, 30 percent involved consumer electronics and parts used in industrial applications and equipment. Considering that the U.S. Immigration and Customs Enforcement data

represent only the fraction of CFIs actually discovered and seized by U.S. enforcement authorities, it is clear that the business of counterfeiting is thriving.

Obsolescence also plays a role in the growth of counterfeiting. Buyers are willing to—and in some cases must—consider suppliers other than the original manufacturer when sourcing difficult-to-find replacement parts. Counterfeiters often find high-volume, low-cost items such as component-level electronics attractive, since a broad market exists and the controls in place to purchase and inspect such commodity items may not be as rigorous as the controls in place for higher-cost items.

EPRI renewed its attention to counterfeit items in 2007 and 2008 in response to an increasing number of counterfeit electronics identified by the U.S. Department of Defense, comments by the NRC indicating concern about counterfeit items, and specific concerns expressed by commercial nuclear plant operators.

In April 2008, the NRC discussed a counterfeit valve installed in a non-safety-related application in a nuclear power plant in Information Notice 2008-04, *Counterfeit Parts Supplied to Nuclear Power Plants*. [5] Figure 3 shows the original and counterfeit valves. The notice also discussed a recall by the U.S. Consumer Products Safety Commission of counterfeit molded-case circuit breakers.

In 2009, EPRI published *Counterfeit, Fraudulent, and Substandard Items: Mitigating the Increasing Risk* [6], which confirmed that large-scale counterfeiting posed an ongoing threat to the supply chain. The report highlighted the proliferation of counterfeit electronic components, including the re-marking and resale of used integrated circuits that may be difficult to detect.

The industry took the following steps to increase awareness about counterfeiting and provide training to nuclear plant personnel and suppliers:

- In 2011, the CFI Task Force was formed to assess the potential impact of CFIs and identify mitigation strategies.
- In 2011, EPRI completed a database for sharing information on CFI incidents.
- In 2012, the Institute of Nuclear Power Operations (INPO) issued an industry event report summarizing operating experience and resources related to CFIs. INPO also expanded plant evaluations to include the consideration of measures to preclude the use of CFIs.

Growing awareness, concern

During this time, global awareness and concern in the nuclear power industry grew as well. The Nuclear Energy Agency's Committee on Nuclear Regulatory Affairs (an organization composed of representatives from international nuclear regulatory agencies) published NEA/CNRA/R(2011)9, *Op-*

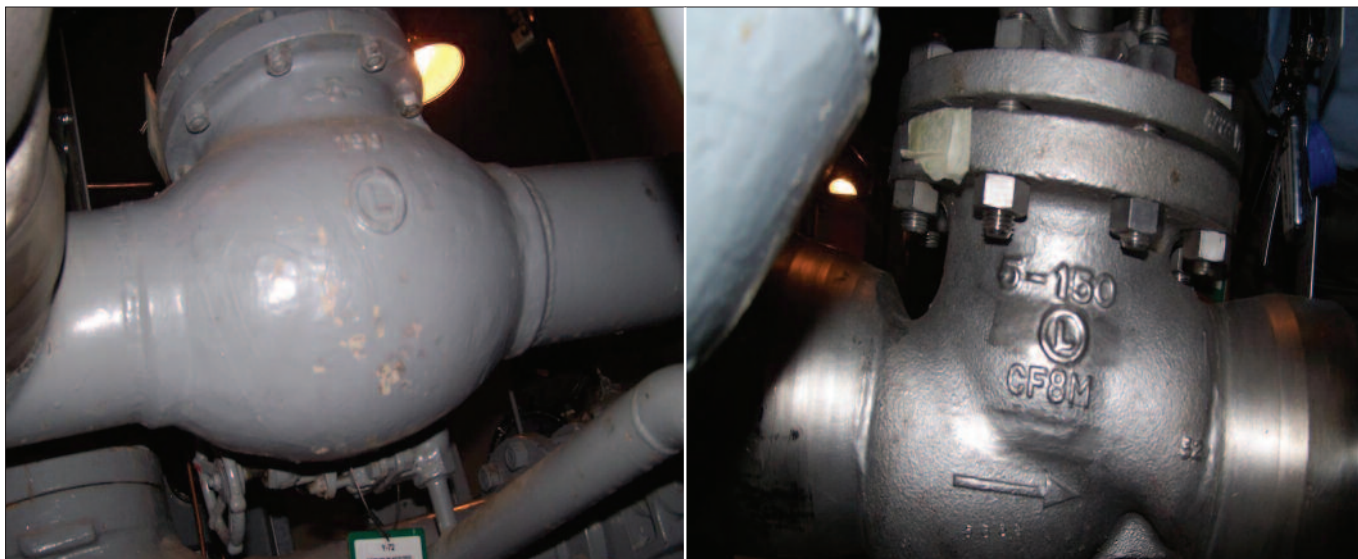


Fig. 3. Authentic valve (left); counterfeit valve (right)

erating Experience Report: Counterfeit, Suspect and Fraudulent Items [7] in October 2011. In February 2013, the same committee published NEA/CNRA/R(2012)7, *Regulatory Oversight of Non-conforming, Counterfeit, Fraudulent and Suspect Items*. [8]

U.S. nuclear plant licensees and the NRC reported several CFI incidents during this period. In 2010, the owner of a circuit board repair supplier directed an employee to replace a broken display unit on a steam leak detector monitor that had been received from one nuclear plant with a working display that had been received from a different nuclear plant, without informing either plant of the exchange. In addition, the employee was instructed to obscure the identity of the working unit by filing down the serial number before shipment. In March 2011, the owner made false statements to NRC investigators, and the U.S. Department

of Justice prosecuted the case in federal district court in Phoenix, Ariz. In February 2013, the owner pleaded guilty to felony charges of making false statements to NRC investigators, and in a plea deal was banned from making safety-related decisions for one year and from making quality assurance oversight decisions indefinitely, and was sentenced to five years of probation that includes special monitoring by the NRC. [9]

In March 2013, a U.S. nuclear plant identified suspect capacitors during receipt inspection. Specifically, the plant noticed that the electrolytic capacitors were not marked with a date code. The utility followed up with the original equipment manufacturer (OEM) and the OEM-approved supplier, which confirmed that the capacitors were counterfeit. The utility had been careful to purchase the capacitors from an OEM-approved supplier, but the supplier had not been able to source

the components from the OEM in time to meet the desired delivery date, and instead had obtained replacements from a broker. Figure 4 shows one of the “suspect counterfeit/fraudulent” capacitors and the corresponding authentic capacitor.

Perhaps the most significant counterfeiting incident in the nuclear industry occurred in South Korea in late 2012, when thousands of parts supplied with fraudulent certification were reportedly installed in two nuclear units that were shut down for extended outages. The discovery of the fraudulent certification prompted an investigation of items procured over the preceding 10 years. This investigation revealed that about 8,000 commercial-grade items supplied with fraudulent certification had been successfully dedicated for use in safety-related applications. The majority of these items were fuses, switches, and cooling fans.

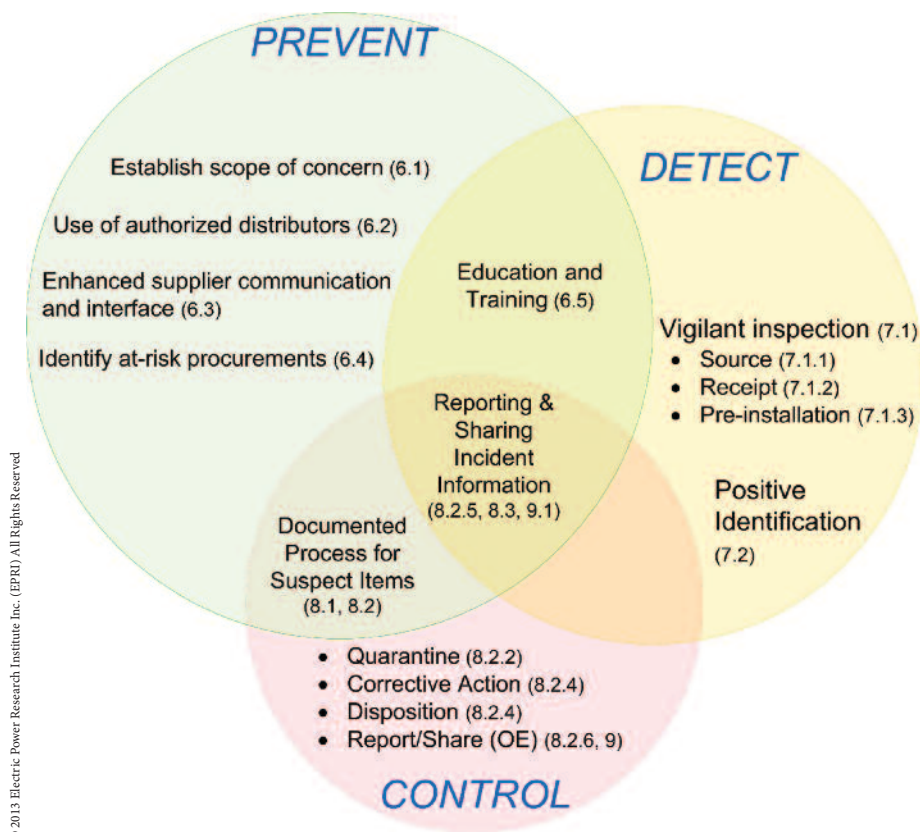
Although none of these items failed or experienced other performance problems that affected plant safety, the operating company decided to shut down the two reactors so that all of the installed fraudulent items could be replaced as quickly as possible. Note that the South Korea-based suppliers involved in the incidents did not provide items to U.S. nuclear facilities. [10]

Mitigating the use of CFIs

In the United States, nuclear plant owners bear primary responsibility for keeping CFIs out of their facilities, and nuclear suppliers are responsible for keeping CFIs out of the products they provide. In 2014, EPRI published a revision to *Counterfeit, Fraudulent, and Substandard Items: Mitigating the Increasing Risk* (3002002276) [10]. This revision, developed by a team that included U.S. and international nuclear operators and suppliers, presents a structured approach for mitigating the use of CFIs. The approach goes beyond reliance on careful examination at receipt, as



Fig. 4. Comparison of an authentic electrolytic capacitor (top) and a suspected counterfeit/fraudulent capacitor (bottom).



© 2013 Electric Power Research Institute Inc. (EPRI) All Rights Reserved

Fig. 5. Key measures for mitigating CFIs included in EPRI Report No. 3002002276.

it involves measures to prevent, detect, and control CFIs (Fig. 5).

As illustrated in Fig. 5, *prevention* begins before an item is purchased. A scope of concern should be established to identify items known to be susceptible to counterfeiting. Buyers should be trained to purchase only from original manufacturers or distributors authorized by the original manufacturer whenever possible. Purchase orders should communicate expectations regarding the authenticity of items provided. Protocols should be established for identifying at-risk procurements such as purchases involving items known to be counterfeited or purchases involving brokers or distributors not authorized by the OEM. At-risk procurements should be subject to enhanced detection measures.

In addition to inspection upon receipt, *detection* measures can include source inspection, and should include inspection immediately prior to installation. Craftpeople and mechanics involved in installation are typically very familiar with the equipment and may be the only individuals with an opportunity to compare the item they are installing with the one that is being replaced. Verifying the authenticity of certification received should also be considered when the certification is not issued by the supplier that provided the items. Individuals involved in detection should have access to information on CFI incidents and should know how to control items suspected of being counterfeit or fraudulent.

Measures to *control* suspected CFIs include identification as nonconforming items and physical quarantine to prevent them from being used. Careful consideration is called for when deciding how to disposition suspected CFIs. It may be appropriate to destroy the items to ensure that they cannot be resold. In some cases, the items might be returned to the original manufacturer for further investigation. Incidences of suspect items should be documented in the corrective action system, which should include guidance on how to report the incident as operating experience and when to notify the appropriate enforcement authorities. In the United States, the NRC's allegation process can be used to directly report a suspected CFI incident.

The NRC includes CFI considerations in its Vendor Inspection Plan (see sidebar, page 47). [11] Susceptibility to counterfeit devices and materials is one factor the NRC uses when selecting and prioritizing which vendors to inspect, and the plan includes provisions to conduct reactive inspections of suppliers when information is received that a supplier has provided a counterfeit or fraudulent item that could have resulted in the failure of a safety-related system.

NRC SECY-15-0003, *Staff Activities Related to Counterfeit, Fraudulent, and Suspect Items* (January 2015), summarizes actions the U.S. nuclear industry has taken to assess the potential impact of CFIs on activities regulated by the NRC. In the SECY, the NRC advises that "the EPRI guidance

document (3002002276) provides the necessary fundamental elements for detecting and preventing CFSI [counterfeit, fraudulent, and substandard items] from affecting NRC-regulated activities." [12] EPRI Report 1021493, *Counterfeit and Fraudulent Items: A Self-Assessment Checklist* [13], is another resource that can be used to identify areas where defenses against CFIs can be improved. This report and EPRI Report 3002002276 are available to the public free of charge at <www.epri.com>.

References

1. NRC Information Notice No. 89-70, *Possible Indications of Misrepresented Vendor Products*, ADAMS accession numbers ML031180470 and ML031190077, U.S. Nuclear Regulatory Commission, Washington, D.C. (Oct. 1989).
2. NRC Generic Letter 89-02, *Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products*, ADAMS accession number ML031140060, U.S. Nuclear Regulatory Commission, Washington, D.C. (Mar. 1989).
3. *Guideline for the Utilization of Commercial-Grade Items in Nuclear Safety-Related Applications*, NP-5652, EPRI, Palo Alto, Calif. (1988).
4. *Intellectual Property Rights Seizure Statistics Fiscal Year 2014*, U.S. Department of Homeland Security, Washington, D.C. (2015).
5. NRC Information Notice 2008-04, *Counterfeit Parts Supplied to Nuclear Power Plants*, ADAMS accession number ML093620098, U.S. Nuclear Regulatory Commission, Washington, D.C. (2008).
6. *Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items—Mitigating the Increasing Risk*, Report No. 1019163, EPRI, Palo Alto, Calif. (2009).
7. NEA/CNRA/R(2011)9, *Operating Experience Report: Counterfeit, Suspect, and Fraudulent Items*, Organization of Economic Cooperation and Development—Nuclear Energy Agency, Paris, France (2011).
8. NEA/CNRA/R(2012)7, *Regulatory Oversight of Non-Conforming, Counterfeit, Fraudulent, and Suspect Items*, Organization of Economic Cooperation and Development—Nuclear Energy Agency, Paris, France (2012).
9. NRC Information Notice 2013-15, *Willful Misconduct/Record Falsification and Nuclear Safety Culture*, ADAMS accession number ML131421437, U.S. Nuclear Regulatory Commission, Washington, D.C. (Aug. 2013).
10. *Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items—Mitigating the Increasing Risk*, Revision 1 of 1019163, Report No. 3002002276, EPRI, Palo Alto, Calif. (2014).
11. *Vendor Inspection Program Plan*, Revision 10, ADAMS accession number ML14329B345, U.S. Nuclear Regulatory Commission, Washington, D.C. (Nov. 2014).
12. NRC SECY-15-0003, *Staff Activities Related to Counterfeit, Fraudulent, and Suspect Items*, ADAMS accession number ML14240A629, U.S. Nuclear Regulatory Commission, Washington, D.C. (2015).
13. *Counterfeit and Fraudulent Items: A Self-Assessment Checklist*, Report No. 1021493, EPRI, Palo Alto, Calif. (2010). **EN**