Plant Support Engineering: Counterfeit and Fraudulent Items

Mitigating the Increasing Risk

3002002276

Draft Report, October 2013

EPRI Project Manager
M. Tannenbaum

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

ORGANIZATION(S) THAT PREPARED THIS DOCUMENT

Electric Power Research Institute (EPRI)

THE TECHNICAL CONTENTS OF THIS DOCUMENT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI NUCLEAR QUALITY ASSURANCE PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B AND 10 CFR PART 21, ANSI N45.2-1977 AND/OR THE INTENT OF ISO-9001 (1994). USE OF THE CONTENTS OF THIS DOCUMENT IN NUCLEAR SAFETY OR NUCLEAR QUALITY APPLICATIONS REQUIRES ADDITIONAL ACTIONS BY USER PURSUANT TO THEIR INTERNAL PROCEDURES.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGEMENTS

This report was prepared by

Electric Power Research Institute (EPRI)
1300 West W.T. Harris Boulevard
Charlotte, North Carolina, 28262

Principal Investigator
M. Tannenbaum

This report describes research sponsored by EPRI.

EPRI would like to thank the following individuals who participated in the technical advisory group and made significant contributions to the development of this report. Their valuable insight and experience were essential to the successful completion of this project.

Revision 1 Technical Advisory Group

Fran Starr	Areva
Tara Werner	Areva
Kim Smith	Bruce Power
Bhavesh Patel	Duke Energy Corporation
Carl Larsen	Institute of Nuclear Power Operations
Hee-seung (Daniel) Chang	Korea Hydro & Nuclear Power Company
Vann Mitchell	Mitsubishi Nuclear Energy Systems
Russell Bell	Nuclear Energy Institute
Marcus Nichol	Nuclear Energy Institute
Pat Scanga	Ontario Power Generation

Brian Mervak	SCANA
William Ware	Southern Nuclear Operating Company
Darryl Romashko	Tennessee Valley Authority
Tracy Wills	URS
Dale Harmon	Westinghouse Electric Corporation

In addition, EPRI would like to thank the following individuals and organizations who shared their valuable insights, recommendations, and lessons learned:

Tom Sharpe	SMT Corporation
Kristal Snider	Electronic Resellers Association International (ERAI)
Tom Snider	Electronic Resellers Association International (ERAI)

Original Technical Advisory Group

Paul Saksvig	Dominion
Jim Grant	Duke Energy Corporation
Marc Tannenbaum	Electric Power Research Institute
Roger Moerman	EnergySolutions
Bhavesh Patel	Progress Energy
William Ware	Southern Nuclear Operating Company
Scott Cameron	South Texas Nuclear Operating Company
Joe Hubbuch	Tennessee Valley Authority
Steve Lusk	Tennessee Valley Authority/NUPIC
Charles Busdosh	Xcel Energy

In addition, EPRI would like to thank the following individuals and organizations who participated in benchmarking activities and/or shared their valuable insights, recommendations, and lessons learned:

Kirsten Koepsel	Aerospace Industries Association
Scott Borland	Amidyne Group

Jim Fisicaro	Duke Energy / Nuclear Energy Institute
Richard Roessler	GE-Hitachi Nuclear Energy
Steve Litchfield	Square D Schneider Electric
Peter Sandborn	University of Maryland Center for Advanced Lifecycle Engineering
Marc Crawford	U.S. Department of Commerce
Ryan Mulholland	U.S. Department of Commerce
Brad Botwin	U.S. Department of Commerce, Bureau of Industry and Security
Jeannie Boyle	U.S. Department of Energy
Sharon Brown	U.S. Department of Energy
Robert Czincila	U.S. Department of Energy
Mark Petts	U.S. Department of Energy
Tom Rotella	U.S. Department of Energy
Skip Searfoss	U.S. Department of Energy
Tom Williams	U.S. Department of Energy
Greg Galletti	U.S. Nuclear Regulatory Commission
Richard McIntyre	U.S. Nuclear Regulatory Commission
Dan Pasquale	U.S. Nuclear Regulatory Commission
Paul Prescott	U.S. Nuclear Regulatory Commission

This publication is a corporate document that should be cited in the literature in the following manner:

Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items: Mitigating the Increasing Risk. EPRI, Palo Alto, CA: 2013. 3002002276.

ABSTRACT

The contents of this report summarize valuable insights gleaned by the Electric Power Research Institute (EPRI) technical advisory groups (TAGs) that researched the techniques being used by U.S. government agencies, licensees, similar industries, and manufacturers to combat the growing problem of counterfeit and fraudulent items. The report clearly indicates that commercial nuclear licensees and their suppliers need to implement measures to prevent counterfeit items from being introduced into their inventory and facilities to address concerns communicated in U.S. Nuclear Regulatory Commission (NRC) Information Notice IN 2008-04, "Counterfeit Parts Supplied to Nuclear Power Plants," [1] NRC SECY 2011-0154, "An Agency-wide Approach to Counterfeit, Fraudulent and Suspect Items," [2] and the NRC Staff Review of Counterfeit, Fraudulent, and Suspect Items [3].

This report presents a multi-tiered approach that includes measures to prevent, detect, and control counterfeit and fraudulent items.

Keywords

Counterfeit	Fraudulent	GIDEP
Receipt inspection	Suspect	

EXECUTIVE SUMMARY

Objective

The objectives of this report are to provide education on the issue of counterfeit and fraudulent items (CFIs) and to communicate measures that can be implemented to prevent CFIs from being introduced into our plants. This report is intended to:

- Communicate lessons learned from benchmarking
- Provide guidance on measures that should be taken to reduce exposure to CFIs
- Introduce appropriate protocols for reporting incidences of suspected CFIs.

Target Audience

This report should be read by staff involved in:

- Procurement
- Inspection (including quality assurance and quality control)
- Installation and maintenance of plant equipment
- Fabrication of products intended for use in nuclear power applications

Introduction

According to the U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE) agencies, the manufacturer suggested retail value of counterfeit and pirated goods seized in 2012 totaled more than $1.26 billion in 2012, representing more than a 21 percent increase in value over seizures made in 2011 [1].

From Major League baseball caps to integrated circuits for military fighter planes, counterfeit and fraudulent items are a growing problem in the United States and around the world. Counterfeit items that do not meet design requirements are finding their way into commercial nuclear power plant receiving areas as well as critical equipment in other industries that closely control procured items.

Counterfeits have made their way into aircraft carrier and fighter jet systems, commercial airliners, pharmaceuticals, petrochemical plants, Department of Energy facilities, and numerous commercial products and construction projects.

Even though significant resources are at work addressing the issue of counterfeits from legal and enforcement perspectives, the number of counterfeiters is rapidly increasing. The rapid spread of manufacturing technology enables quick and easy creation of counterfeit products that are difficult to distinguish from the genuine product. Counterfeiters' capabilities are improving. In fact, one manufacturer representative told the Technical Advisory Group (TAG) preparing this report that some counterfeiters are actually implementing quality assurance measures to ensure that their products *appear* to be genuine.

In light of the globalization of our supply chain and the resulting impact on the goods provided to our facilities, commercial nuclear power facilities face a unique challenge. We must continue to purchase the spare and replacement items required to support operations and maintenance, while at the same time recognizing that many of these items and the materials used to fabricate them may not originate from the original manufacturer. It is incumbent upon plant owners and suppliers to remain vigilant and implement appropriate measures to detect, prevent, and control CFIs.

The guidance provided in this report is intended to facilitate the industry's efforts to address concerns related to CFIs so as to assure the fidelity and reliability of nuclear plant systems, structures and components.

Regulatory Basis

Several reports published by the Nuclear Energy Agency Committee on Nuclear Regulatory Activities demonstrate that the international regulatory community is concerned about CFIs.

In the U.S., the NRC considers measures to prevent CFIs to be an important part of meeting 10CFR50, Appendix B [2] Criterion VII, Control of Purchased Material, Equipment, and Services; Criterion VIII, Identification and Control of Materials, Parts; and Components and Criterion X, Inspection. The NRC discusses specific concerns in "Staff Review of Counterfeit, Fraudulent, and Suspect Items" [3].

Actions to Reduce Risk

Although the measures implemented by the nuclear industry almost two decades ago have served the industry well, there are additional steps that can and should be taken to prevent counterfeit items from impacting safety and generation. These steps are discussed in this report and include:

- Improved communication with and qualification of suppliers including use of standard contractual terms and conditions that address CFI concerns
- Effective reporting, gathering, and sharing of information related to suspected CFIs to appropriate databases such as INPO operating experience, scfi.epri.com, and commercial databases that cater to specific industries

- Vigilant inspections and testing of procured items
  - Source
  - Receipt
  - Pre-installation
- Periodic training for staff, particularly inspectors, purchase agents, engineering personnel, mechanics, assembly and manufacturing personnel who have "hands-on" opportunities to prevent and detect counterfeits and keep them out of plants and manufactured products.
- Development of plans and instructions for addressing suspected CFIs including entering incident information into corrective action programs (or equivalent) and quarantine of suspect items
- Identification of "at-risk" procurements and enhanced inspection and testing when appropriate
- Safeguarding intellectual property
- Manufacturer's use of "positive identification" techniques

Incident Data Reporting and Sharing Protocols

The industry should continue to work together to effectively gather and share information about incidents of suspected CFIs. Sections 8 and 9 of this report outline current protocols to report and share information about suspected incidents of CFIs. These include reporting to INPO, WANO, EPRI, regulatory agencies and commercially available databases as appropriate.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1
INTRODUCTION

1.1 Genesis and Purpose of this Revision

This revision is primarily the product of industry meetings held to address industry operating experience and CFI concerns including those identified in NRC SECY 11-0154, "An Agency-wide Approach to Counterfeit, Fraudulent and Suspect Items" [4]. Meetings included NRC public meetings and meetings of the Nuclear Energy Institute's CFI Task Force which included representation from key suppliers to the U.S. commercial nuclear industry and licensees including members of EPRI's Joint Utility Task Group on Procurement Engineering (JUTG), and the Nuclear Procurement Issues Committee (NUPIC).

In addition, this revision draws upon the results gleaned through a ninety-six (96) question electronic self-assessment survey that was distributed to U.S. licensee and supplier members of the Nuclear Energy Institute in early 2013. The electronic self-assessment was based upon EPRI 1021493, Counterfeit and Fraudulent Items: A Self-Assessment Checklist [5].

The guidance included in this report is intended to assist nuclear facilities and their suppliers in addressing concerns related to CFIs so as to assure the fidelity and reliability of nuclear plant systems, structures, and components. Implementation of the guidance contained in this report can and will reduce exposure to CFIs.

1.2 Background

There are many contributors to the growing number of CFIs entering the marketplace. The situation is not temporary; CFIs are a permanent and growing concern. CFI concerns extend beyond the part or equipment level to raw materials. Even when the parts and equipment we buy are genuine, there is a possibility that the materials or certain parts used by the manufacturer may be counterfeit or fraudulent unless suppliers are aware of the issue and are implementing measures to detect and avoid the use of counterfeit and fraudulent raw materials and parts.

Owing in large measure to the industry's quality assurance and equipment reliability programs, no known incidents of counterfeit items being discovered in safety-related applications in operating U.S. commercial nuclear power plants have been reported. However, as shown in Section 4 of this report, there have been a small number of reports involving incidents where counterfeit items were found installed in non-safety-related systems.

Globalization of the supply chain and new manufacturing technologies are enabling an increase in the numbers of items being counterfeited. The growth of new manufacturing capabilities and

demand for low-cost items in rapidly developing regions has increased the number of CFIs that make their way into the global supply chain.

While we must continue to purchase the spare and replacement items required to support operations and maintenance, it is incumbent upon plant owners and suppliers to remain vigilant and implement appropriate measures to detect, prevent, and control CFIs. As discussed in NRC Information Notice 2008-04, it is the responsibility of each licensee to ensure that CFIs do not impact the safety of their plant(s). [6] There are clear precautions and measures licensees and their suppliers should implement to reduce the risk that counterfeit items will end up in inventory or, worse, installed in plants.

1.2.2 Regulatory Basis

The issue of CFIs is addressed, although not explicitly, in the requirements of 10CFR50, Appendix B [2], Enhanced guidance will ensure that nuclear power plants are protected against the increasingly significant factor of CFIs in assuring the quality of procured items. In the NRC's "Staff Review of Counterfeit, Fraudulent and Suspect Items," [3] the NRC states:

> "The integrity of the supply chain is a fundamental element of an effective quality assurance program for NRC licensee facilities and the suppliers of basic components to these facilities. For example, six of the 18 criteria presented in Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to Title 10 of the Code of Federal Regulations (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," are directly related to assuring that adequate procurement controls at these facilities have been appropriately established and effectively implemented."

For example, taking action to prevent CFIs can be considered an important part of meeting 10CFR50, Appendix B Criterion VII, Control of Purchased Material, Equipment, and Services; Criterion VIII, Identification and Control of Materials, Parts and Components, and Criterion X, Inspection [2].

Increasing concern about CFIs at all levels of government, compelled the NRC to issue Information Notice 2008-04, "Counterfeit Parts Supplied to Nuclear Power Plants" [6], which reminded licensees of their obligation to maintain effective procurement programs and controls and reiterated the importance of the actions contained in Generic Letters 89-02 [7] and 89-70 [8]. More recently, the NRC issued SECY-11-0154 [4] in response to troubling trends in CFI incidents. While precautions put in place in the early 1990s have proven to be effective barriers, additional actions should be considered to better address the resources and capabilities of today's counterfeiters.

The NRC is among a group of government agencies that are working to address the economic and safety implications associated with CFIs. Included are agencies that oversee or regulate "mission critical" equipment, such as the Naval Air Systems Command (NAVAIR), the National Aeronautics and Safety Administration (NASA), and agencies that oversee equipment or

programs related to infrastructure, such as the Departments of Energy (DOE) and Commerce (DOC). Some of the avenues being pursued by these agencies include heightening awareness, identifying threats to security, providing training, finding ways to impede the flow of CFIs into the country, and investigating and bringing appropriate action against entities providing CFIs. In addition, the NRC has engaged industry stakeholders on proactive initiatives to enhance protections against CFI.

The international regulatory community is also concerned about CFIs. In October of 2011, the Nuclear Energy Agency Committee on Nuclear Regulatory Activities published NEA/CNRA/R(2011)9 , Operating Experience Report: Counterfeit, Suspect and Fraudulent Items [9]. In February of 2013 the Committee followed-up with NEA/CNRA/R(2012)7 , Regulatory Oversight of Non-conforming, Counterfeit, Fraudulent and Suspect Items (NSFSI) [10].

1.2.3 Industry Focus

CFIs are generally a subset of nonconforming/substandard items. Simply put, the terms "counterfeit" and "fraudulent" imply intent to deceive.

The term "suspect items" is used to describe items that are suspected of being counterfeit or fraudulent. The phrase "suspect counterfeit or fraudulent items" is used to describe items that are suspected of being counterfeit or fraudulent when the results of a conclusive investigation into their authenticity are not available.

Ensuring that CFIs are not introduced into nuclear plants is of utmost importance. However, once CFIs are quarantined and controlled, it may not always be necessary or practical from a resources (or cost benefit) standpoint for a licensee to conduct a conclusive investigation to determine the origin of the items and establish into which category (counterfeit or fraudulent) the suspect items belong.

The licensee's focus is on keeping CFIs out of the plant, and the suppliers' focus is on keeping CFIs from being used in the manufacture of their products.

1.3 Historical Impact on U.S. Nuclear Facilities

Historically, existing U.S. nuclear facilities have been somewhat insulated from CFIs due to the age of their equipment and the low demand for nuclear-related components in the marketplace. This is consistent with the results of a survey performed by the U.S. Department of Commerce Bureau of Industry [11][12].

However, there have been incidents of CFI at U.S. nuclear plants. A number of incidents identified by the NRC in the 1980s and 1990s catalyzed the U.S. nuclear industry to adopt standard precautions to guard against counterfeit items. Those precautions were documented in 1989 in NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products," [7], NRC Generic Letter 89-70, "Possible Indications of

Misrepresented Vendor Products [8] and in Appendix C of a 1990 EPRI Report titled "Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants" (NP-6629) [13]. Similar guidance is contained in a 2000 International Atomic Energy Agency (IAEA) technical document, "Managing Suspect and Counterfeit Items in the Nuclear Industry" (TECDOC-1169) [14].

A few recent events in the U.S. nuclear power industry have drawn additional attention to the issue. In December of 2012, the owner of Pentas Controls, LLC pleaded guilty to making false statements about a safety-related circuit board repair [15]. In November 2007, the Plant Hatch nuclear facility in Georgia discovered a counterfeit stop check valve on the stator cooling water skid of Unit 2. Hatch personnel later determined that the plant contained two counterfeit valves, one in the warehouse and one installed on Unit 2. Duke Energy discovered that counterfeit circuit breakers manufactured in China and labeled as "Square D" products may have been purchased for its Oconee, McGuire, and Catawba nuclear plants in North and South Carolina sometime between 2003 and 2006.The counterfeit circuit breakers could fail to trip when overloaded, posing a fire hazard [6].

A historical perspective of CFIs in the commercial nuclear power industry and additional examples of incidents involving CFIs are provided in Section 4 of this report. Appendix A of this report contains a listing of various documents prepared by the NRC starting in the 1980s and 1990s to document incidents related to CFIs.

1.3.1 Recent CFI Impacts on Other Industries

Recent high-profile CFI examples in other industries including, pharmaceuticals, human food, pet food, and lead paint in toys highlight the extent of the issue and the growing level of concern. Further, with counterfeiters acquiring and using increasingly sophisticated methods and capabilities, CFIs could end up in the inventories and products of unknowing legitimate suppliers unless measures are taken to ensure otherwise.

In an extensive effort spanning several years, the Department of Commerce Bureau of Industry and Security conducted a survey of suppliers that provide electronics to the military industrial complex related to CFIs. The survey results were in draft form when the original version of this report was published in 2009 and the final survey results were published in 2010 [11]. Although several years old at the time this revision was prepared, the survey results referred to in this report are still meaningful and provide insight to the CFI problem.

In March 2009, the Department of Commerce study of counterfeit electronics indicated that 91% of the 498 organizations surveyed accept products returned by the customer, 40% place returned items into stock, and 14% have identified counterfeit items in returned merchandise [12]. Other cases have been documented where unknowing and well-intentioned manufacturers have sold products that turned out to be defective due to raw materials or parts purchased from sub-tier suppliers that did not meet applicable specifications.

Relevant examples of CFI incidents in other industries include:

- In July of 2013, the U.S. Department of Justice filed an indictment against an individual that sold counterfeit semiconductors purchased from sources in Hong Kong and China to the military under two companies he owned, Tytronix, Incorporated and Epic International Electronics [16].
- In April of 2009, the DOE Inspector General's Audit Report DOE/IG-0814 [17] alleged that 9,500 tons of substandard reinforcing materials were purchased to support construction of the Savanna River Site's Mixed Oxide Fuel Fabrication Facility.
- A Department of Energy (DOE) Category 2 nuclear facility discovered a fraudulent International Organization for Standardization (ISO) 9001 certificate prior to the award of a valve procurement.
- A company forged an American Welding Society (AWS) stamp and used a bogus Certified Weld Inspector (CWI) number in an effort to represent that its work was properly inspected.
- A main steam pipe provided with falsified documentation suffered catastrophic failure (burst) at the Datong Power Station Unit 2 in China, resulting in two fatalities and other injuries to personnel. The pipe was supplied and certified by a U.S. company in Houston, Texas.
- The Quality Assurance manager of Hunt Valve pleaded guilty to certifying tests on valves for nuclear steam systems where the tests were never conducted. The valves were sold to the U.S. Navy and DOE.
- The ICE branch of the Department of Homeland Security routinely prevents a variety of items from entering the marketplace, ranging from baseball caps to counterfeit blood sugar testing strips and pharmaceuticals

1.4 Scope of Concern for U.S. Nuclear Suppliers and Licensees

Robust quality assurance programs, safety-conscious work environments, and other controls that are routinely implemented extremely well at nuclear power plants have performed an invaluable function in keeping CFIs from being procured for, accepted into inventory for, and installed in safety-related applications.

However, CFIs can impact many types of items purchased to support operations and maintenance of a nuclear power plant. While the implications associated with failure of a counterfeit item installed in a safety-related application are obviously serious, a counterfeit item incident does not have to involve safety-related equipment to result in serious consequences.

In fact, an incident does not necessarily have to involve counterfeit plant equipment or parts for plant equipment. As an example, consider rigging hardware. What might be the possible outcomes if a counterfeit shackle failed while being used to lift plant equipment or barriers during routine maintenance in the plant? Such an incident could result in loss of life and limb, damage to plant systems and equipment, and loss of generation and system availability.

As another example, consider reloaded or substandard ammunition. What might be the possible outcomes if ammunition used by a plant security force did not function as it should during routine target practice or an actual security event? Such an incident could result in personal injury or compromise one aspect of plant security.

The Government Industry Data Exchange Program (GIDEP) and the Department of Energy's (DOE's) Suspect and Counterfeit Item database (S/CI), discussed in Appendix C of this report, include known incidents at DOE and other government facilities that involve discovery of counterfeit lifting and rigging equipment and reloaded ammunition being misrepresented and sold as new.

The U.S. Department of Commerce survey data indicated that while more than 50% of CFIs identified from 2005–2008 were out of production, counterfeiters are also targeting high-demand, moderately priced items. According to the survey, the majority of CFI incidents were associated with items priced between $0.11 and $500.00 [12].

Because counterfeit items can impact plant operations in many ways, the contents of this report may be applicable to many types of items purchased to support a nuclear facility, including safety and non-safety materials and components as well as some non-plant items such as security equipment, personnel protective equipment, lifting and rigging equipment, scaffolding, and other items.

1.5 Unintentional use of Counterfeit and Fraudulent Items

Items that counterfeiters produce are often manufactured with substandard or lower grade materials. Although substandard materials may appear to be the appropriate grade, they may not be able to withstand the design loads and demands of the application for which they are intended. Therefore, substandard counterfeit items can pose serious safety risks in some applications. In some cases, unethical suppliers are aware of the fact that they are providing a counterfeit or fraudulent item. In other cases, well-intended suppliers may be unaware that they are providing counterfeit or fraudulent items or that they are manufacturing items from counterfeit or substandard materials. The terms *knowingly* and *unknowingly* are used to describe the two situations:

- ***Unknowingly*** applies to a supplier who provides a counterfeit or fraudulent item, but who believed it to be genuine. The supplier may have purchased it from another supplier or distributor who also believed that they purchased a genuine part.
- ***Knowingly*** applies to a supplier who provides a counterfeit or fraudulent item that was acquired with full knowledge that the item was not genuine or who acquired it at a substantially lower price than genuine items and did not verify it as genuine before selling it. Suppliers who knowingly provide counterfeit or fraudulent items to commercial nuclear power facilities are subject to punitive action by the NRC in accordance with the provisions of 10CFR 50.5, Deliberate Misconduct [18].

1.6 Contributors to Counterfeiting and Fraud

Many factors contribute to the growing problem of CFIs. Perhaps the largest contributors are the profiteering and the rapidly evolving global supply chain. Other factors include obsolescence and short product lifecycles. Additional CFI prevention and detection measures may be necessary for procurements with known exposure to contributing factors. These factors are discussed in more depth in Sections 5 and 6.4 of this report.

1.7 How Counterfeit and Fraudulent Items are Introduced

CFIs can enter supply chains in many ways. A large number of counterfeit items are introduced by counterfeiters who intentionally reproduce and market hard-to-find or high-demand products for profit. It is more difficult for counterfeiters to penetrate approved distribution networks, so counterfeits are often introduced by brokers and distributors operating outside the original equipment manufacturer's approved distribution network. Although the chances of receiving a counterfeit are substantially reduced by purchasing directly from the original equipment manufacturer (OEM) or an approved distributor, risk still exists.

Rejected or excess inventory items that are not properly disposed of can also end up entering the supply chain misrepresented as new items. During research for this report, the TAG learned that an oil refinery worker receiving training on counterfeit items mentioned that several men drove up to people working in a lay-down (storage) yard and asked the workers to call them if they ever had any damaged or used items that they were going to throw away.

New technologies or standards introduced to the marketplace present yet another challenge, as inventory of items meeting new standards may become mixed with inventory of items meeting the old standards, even when they are not completely interchangeable.

It is important to recognize that although effective receiving inspection is important, inspection at receipt can not be solely relied upon to keep CFIs out of plants. For example, pre-installation inspection by craftspeople may be the last line of defense because they have a hands-on opportunity to identify suspicious items immediately prior to installation and, in some cases, have the opportunity to compare the replacement with the item being replaced.

1.8 Benchmarking and Collaboration

The guidance provided in this report was informed by benchmarking performed in support of the initial issuance of the report in 2009, as well as additional benchmarking completed more recently. These benchmarking activities are discussed in Section 10 of this report.

Benchmarking conducted subsequent to publishing the original version of this report included:

- Participation in NRC public meetings on the topic of counterfeiting and fraud
- An NEI/EPRI survey discussed in Section 10 of this report

- Participation in meetings held by the U.S. Department of Justice D.C. Counterfeit Microelectronics Working Group
- Discussions and information exchanges with the Construction Industries Institute
- Discussions with commercial organizations such as:
  - SMT Corporation who specializes in testing and inspecting electronic components and integrated circuits
  - ERAI who maintains a database of suspect item incidents involving electronic components
  - Eaton Controls and Square D Schneider Electric

Benchmarking activities completed during the development of the original revision of this report include the following:

- A survey was distributed to government agencies that procure or oversee procurement of "mission critical" equipment and supporting parts and materials.
- A "roundtable" benchmarking meeting was held at the Electric Power Research Institute's (EPRI's) offices in Washington, DC, with 26 participants representing 6 nuclear utilities and the following organizations.
  - Nuclear Regulatory Commission (NRC)
  - DOE
  - Department of Commerce (DOC)
  - DOC Bureau of Industry and Security (DOC BIS)
  - Square D Schneider Electric
  - Aerospace Industries Association (AIA)
  - University of Maryland Center for Advanced Lifecycle Engineering (CALCE)
- EPRI assisted the NRC in organizing an educational seminar on the issue of CFIs that followed the Nuclear Procurement Issues Committee (NUPIC) Auditor Training Conference in June 2009. The seminar included breakouts addressing perspectives and concerns of the NRC, EPRI, NUPIC, and several suppliers.
- EPRI participated in a Government Industry Data Exchange Program (GIDEP) Management Conference and presented an overview of this project and its results

Information gleaned from these benchmarking activities was used by the original EPRI technical advisor group to develop the recommended actions to reduce risk and formed the basis for development of scfi.epri.com, the database available to EPRI members to report and share operating experience on CFIs.

1.9 Guidance Approach

The approach presented in this report centers around measures intended to ***prevent*** CFIs from reaching our receiving docks, as well as measures to assure that we ***detect*** and effectively ***control*** counterfeit items that find their way into our facilities.

Although the problem of CFIs is extensive and is constantly evolving, there are actions that licensees and suppliers can and should take to minimize risk. In addition, the industry has developed the capability to gather and share data on CFI incidents in an effort to prevent recurrences. Methods for mitigating the risk associated with CFIs are discussed in Section 9 of this report.

Figure 1-1 captures a brief description of the measures for prevention, detection, and control of CFI along with the number of the Section in this report that discusses the measure. The size of the circles is intended to illustrate that significant emphasis is placed on proactive measures to prevent CFI from making their way into nuclear plants or manufactured components.

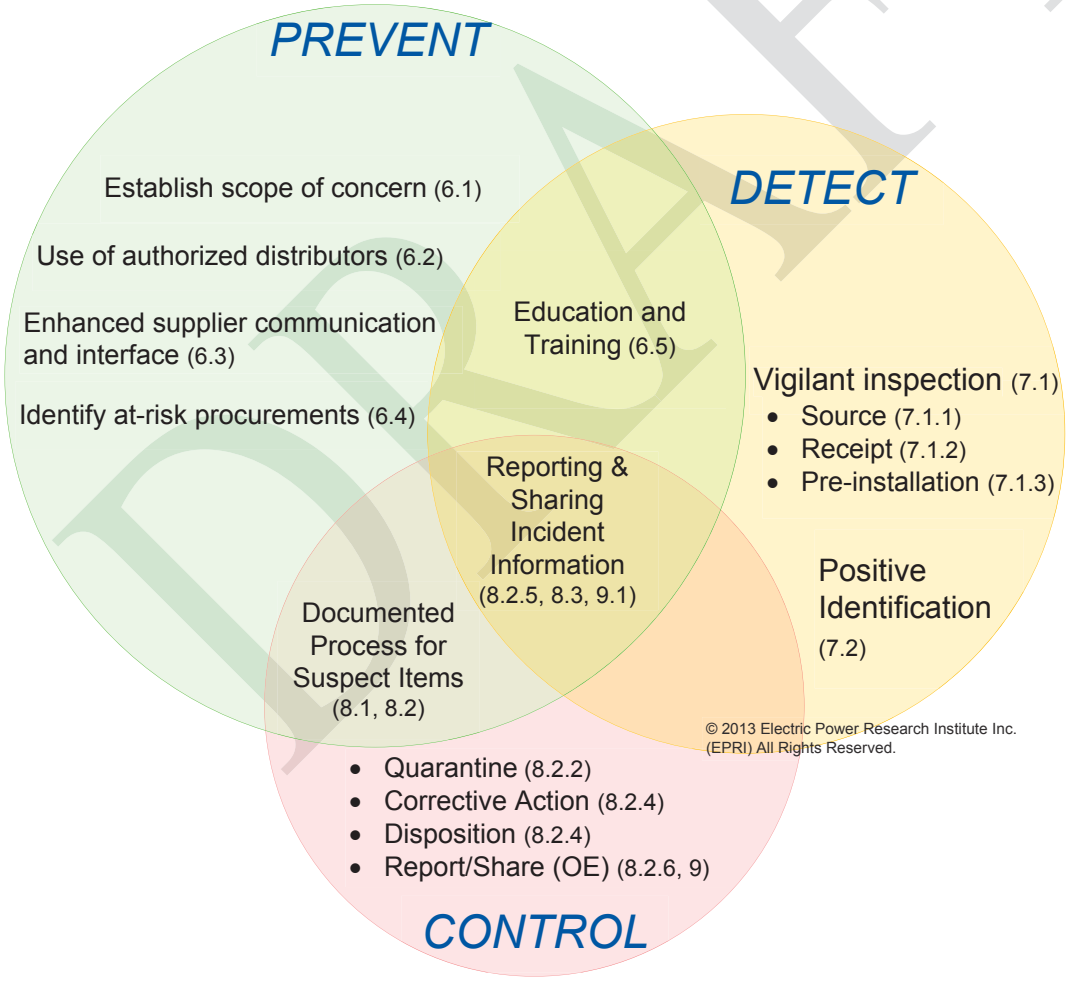


Figure 1-1
Key Measures for Preventing, Detecting, and Controlling Counterfeit and Fraudulent Items

2
DEFINITIONS AND ACRONYMS

2.1 Definitions of Key Terms in This Report

at-risk Exposed to one or more risk factors known to be associated with counterfeit and fraudulent items.

counterfeit Counterfeit items are items that are intentionally manufactured or altered to imitate a legitimate product without the legal right to do so.

A counterfeit item is one that has been fabricated in imitation of something else with purpose to defraud by passing the false copy for genuine or original or is an item copied without the legal right or authority to do so.

enhanced inspection/testing Inspection/testing performed in addition to the standard receiving inspection/testing process in order to reasonably assure that the items received are authentic.

fraudulent Fraudulent items are items that are intentionally misrepresented with intent to deceive. Fraudulent items include items provided with incorrect identification or falsified or inaccurate certification. Fraudulent items also include manufacturing overages sold by entities that have acquired the legal right to manufacture a specified quantity of an item (such as an integrated circuit), but produce a larger quantity than authorized and sell the overage as legitimate inventory.

incident An incident is a discrete event associated with the discovery of a suspected counterfeit or fraudulent item. An incident can involve one or many items discovered at once or over a period of time.

substandard Substandard items do not meet the intended product specification. It is possible for legitimate suppliers to unknowingly provide substandard items that were manufactured using raw materials or part-level items that were acquired from sub-tier suppliers and that, for some reason, did not meet the applicable specifications.

suspect	Suspect items are items that are suspected of being counterfeit or fraudulent.

2.2 Acronyms

AFOSI	Air Force Office of Special Investigations
AIA	Aerospace Industries Association
ANPR	Advanced Notice of Proposed Rulemaking (issued by U.S. NRC)
ANS	American Nuclear Society
ASD	Authorized Service Directory
AWS	American Welding Society
CACN	Canadian Anti-Counterfeiting Network
CACP	U.S. Chamber of Commerce Coalition against Counterfeiting and Piracy
CALCE	University of Maryland Center for Advanced Lifecycle Engineering
CBP	U.S. Customs and Border Protection
CFR	Code of Federal Regulations
CFI	Counterfeit and fraudulent item
CFSI	Counterfeit, fraudulent, and suspect items (used by U.S. NRC)
CIB	International Chamber of Commerce Counterfeiting Intelligence Bureau
CPSC	U.S. Consumer Products Safety Commission
CWI	Certified Weld Inspector
DCIS	Defense Criminal Investigative Service
DI	Defective Item (Department of Energy)
DLA	Defense Logistics Agency

DOC	United States Department of Commerce
DOC BIS	United States Department of Commerce, Bureau of Industry and Security
DOD	United States Department of Defense
DOE	United States Department of Energy
DOE HSS	United States Department of Energy, Office of Health, Safety, and Security
EPC	Engineering, procurement, and construction
EPRI	Electric Power Research Institute
ERAI	ERAI, Incorporated (aka Electronic Resellers Association International is a privately held global information services organization that monitors, investigates and reports issues affecting the global semiconductor supply chain
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FTP	File transfer protocol
GIDEP	Government Industry Data Exchange Program
IACC	International Anti-Counterfeiting Coalition
IAEA	International Atomic Energy Agency
ICE	U.S. Immigration and Customs Enforcement
IDEA	Independent Distributors of Electronics Association
JUTG	EPRI Joint Utility Task Group (on procurement engineering)
MMN	Manufacturer and model number
NAVAIR	Naval Air Systems Command
NCIS	Naval Criminal Investigative Service

NDAA	National Defense Authorization Act
NEC	National Electric Code
NEI	Nuclear Energy Institute
NEMA	National Electrical Manufacturers Association
NSFSI	Nonconforming, Counterfeit, Suspect and Fraudulent Items
NPEP	Nuclear Plant Equipment Procurement
NRC	U.S. Nuclear Regulatory Commission
NRTL	Nationally recognized testing laboratories
NSSS	Nuclear steam system supplier
NUMARC	Nuclear Management and Resources Council
NUPIC	Nuclear Procurement Issues Committee
OCM	Original component manufacturer
OE	Operating Experience
OEM	Original equipment manufacturer
OES	Original equipment supplier
O&M	Operations and maintenance
POMS	Rolls Royce's Proactive Obsolescence Management Systems
RAPID	Curtiss-Wright/Scientech's Rapidly Available Parts Information Database
RCMP	Royal Canadian Mounted Police
RoHS	Reduction of hazardous substances
SAE	Society of Automotive Engineers
SCFI	Suspected Counterfeit / Fraudulent Items

SC/I	Suspect and Counterfeit Item program and database (Department of Energy)
SECY	Secretary Letter (Issued by U.S. NRC to the NRC Commission)
SIA	Semiconductor Industry Association
SME	Subject matter expert
SMT	SMT Corporation, An electronics stocking distributor that maintains a database of counterfeit item data and is actively involved in counterfeit mitigation
SPOC	Single point of contact
STOP	Strategy targeting organized piracy
TAG	Technical advisory group
UL	Underwriters Laboratory, Incorporated
U.S.	United States
USACID	U.S. Army Criminal Investigative Division

3
HISTORICAL ISSUES AND THE INDUSTRY'S RESPONSE

3.1 Historical Perspective

Late in the 1980s, the NRC began to issue a number of communications alerting licensees to issues involving CFIs.

The communications addressed a variety of substandard and counterfeit items including valves, circuit breakers, fasteners, piping, tubing, flanges, sealants, structural steel, relays, gears, and fire-protection equipment. A list of these communications is included in Appendix A of this report.

Several of these communications specifically addressed actions that licensees should take to avoid CFIs. A few of the NRC's most notable communications from the 80s include:

- U.S. NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products" [7]
- U.S. NRC SECY 89-010, Advance Notice of Proposed Rulemaking (ANPR), "Acceptance of Products Purchased for Use in Nuclear Power Plant Structures, Systems, and Components" [19]
- U.S. NRC Information Notice No. 89-70, "Possible Indications of Misrepresented Vendor Products" [8]

3.1.1 The U.S. Commercial Nuclear Industry's Initial Response to the Issue of Counterfeiting and Fraud

The industry responded to the NRC's concerns in several ways. Realizing that both the NRC and licensees play active roles in protecting the health and safety of the public, EPRI formed task groups consisting of licensee subject matter experts who developed and published guidance on how to address NRC concerns that included:

- EPRI NP-5638, *Guidelines for Preparing Specifications for Nuclear Power Plants* [20], was published in April 1988.
- EPRI NP-5652, *Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications* [21], was published in June 1988.

- EPRI NP-6406, *Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants* [22], was published in December 1989.
- EPRI NP-6629, *Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants* [13], was published in May 1990 and included an appendix (Appendix C) titled "Identifying Substandard/Fraudulent Items" that contained guidance on how to identify CFIs .

EPRI also began delivering training to its members to assist them in implementing the concepts and processes included in the guidance.

In September of 1988, the Nuclear Management and Resources Council (NUMARC) (predecessor to the Nuclear Energy Institute [NEI]) formed the Nuclear Plant Equipment Procurement (NPEP) working group to address improvements in the industry's procurement processes and practices.

Recognizing that the requirements of 10CFR50, Appendix B [2] did not explicitly call-out intentional deception and fraudulent activities, the NPEP working group recommended several enhancements to be incorporated in licensees' procurement processes. These recommendations were published in October of 1990 in NUMARC 90-13, "Nuclear Procurement Program Improvements" [23].

A key element of these enhancements was placing more emphasis on the technical verification of product quality instead of relying upon documentation provided by the suppliers. Accordingly, NPEP recommended implementation of several measures that were identified in industry guidance including:

- Increase engineering involvement in the procurement process, including assessments (audits) of suppliers.
- Increase awareness of counterfeiting and fraud, and determine the best ways to detect fraudulent and counterfeit products by implementing the guidelines contained in NP-6629, Appendix C [13].
- Share objective information regarding procurement via established industry operational experience forums.
- Procure items from the original equipment manufacturer (OEM) or authorized distributor whenever possible. When not possible, establish product performance via traceability to the OEM or through testing and inspection.
- Establish acceptance criteria for items at the front end of the procurement process.

Licensees in the United States agreed to implement the improvements called for in NUMARC 90-13 no later than July 1, 1992. Licensees did, in fact, implement the improvements, including the guidance designed to counter fraudulent and counterfeit items contained in NRC Generic Letter 89-02 [7], NRC Information Notice 89-70 [8], and in Appendix C of EPRI NP-6629 [13], and these improvements have served the industry well.

Only a very small number of incidents involving counterfeit and substandard items have been identified in the commercial nuclear power industry. These incidents are among those captured by the NRC in their communications listed in Appendix A of this report.

3.1.2 Other Historical Responses to the Issue of Counterfeiting and Fraud

During the late 1980s, the commercial nuclear power industry was not alone in its concerns about fraudulent and counterfeit items. Many industries and government agencies instituted similar controls to address counterfeiting problems.

Enhancements and improvements were made in the ways components are designated in design documents, standard clauses were developed and added to procurement documents, and personnel were trained to detect counterfeits. Increased inspection and testing were applied to item types known to be counterfeited, such as fasteners, pipes, and pipe fittings manufactured outside the United States.

Investigation revealed that the problem included not only foreign manufacturers, but also distributors in the United States. In some instances, U.S. distributors intentionally ordered materials made from a lower grade material and then marked and sold them as higher grade. In other cases, local suppliers purchased materials from larger distributors and unknowingly sold the counterfeit and fraudulent materials to their customers.

In addition to industry-specific actions by the NRC, the U.S. government's involvement in the issue included the development of requirements that eventually were passed into law. On November 16, 1990, Congress passed Public Law 101-592, Fastener Quality Act [24]. This Act did the following:

- Required that certain fasteners sold in commerce conform to the specifications to which they are represented to be manufactured
- Provided for the accreditation of laboratories engaged in fastener testing
- Required inspection, testing, and certification of fasteners used in critical applications in accordance with standardized methods to increase fastener quality and reduce the danger of fastener failure

On April 9, 1991, the Office of Management and Budget (OMB) published Policy Letter 91-3, "Reporting Nonconforming Products" [25]. This letter established policies and procedures for using the Government Industry Data Exchange Program (GIDEP) as a government-wide system for exchanging information about nonconforming products and materials.

On August 17, 1992, Public Law 101-592 was followed by the issuance of Federal Register Notice, Department of Commerce, Part II, National Institute of Standards and Technology, 15 CFR Part 280, Fastener Quality [26].

The Federal Acquisition Circular (FAC) FAC 90-9 [27] was published on February 25, 1992. The FAC defines U.S. government requirements for the procurement of products by functional characteristics versus brand names. GG-MATP-01, The Guideline for the Preparation of Material/Equipment Descriptions, effective date 06-23-92 [28] was also issued and provided an example of how to use critical characteristics to describe items and services.

The DOE published a "Suspect/Counterfeit Parts Headmark List" in the *Environment, Safety & Health Bulletin,* DOE/EH-0266, Issue No. 92-4 in August 1992, (DOE Quality Alert) [29].

On December 1, 2011 the U.S. Senate passed an amendment to the National Defense Authorization Act that included Section 818, [30]. Section 818 includes requirements applicable to the defense supply chain for preventing use of CFI. These requirements include a preference for procuring from original component manufacturers (OCMs) or their authorized suppliers, use of "trusted suppliers" (the term is not defined in the Act) when items can not be purchased from OCM or OCM-authorized supplier, reporting incident information to the GIDEP database, adopting internal systems to deter, detect, and avoid CFI, and so forth.

Since the introduction of these measures, the amount of manufacturing occurring in the United States has decreased significantly. There has been a corresponding increase in the amount of counterfeiting and fraud. U.S. government agencies such as the Defense Logistics Agency (DLA) and other military support organizations have seen a significant increase in the amount of commercially procured items that do not meet specifications.

The government's awareness of the amount of counterfeit items entering the U.S. has caused concern. Although many items counterfeited are not used in critical applications, others are. Pipe, circuit breakers, integrated circuits, discrete components, reinforcing bar, and structural steel are just some of the CFIs that have been identified.

3.2 Recent Emphasis on Counterfeiting and Fraud in the Commercial Nuclear Power Industry

3.2.1 Nuclear Regulatory Commission

In August of 2007, then NRC Chairman Commissioner Dale E. Klein delivered the keynote address at the American Nuclear Society's Utility Working Conference [31]. In his speech, Commissioner Klein expressed concern about the industry's exposure to CFIs. In his speech, he said:

> "The resurgence of the nuclear industry will require each and everyone involved to understand that it is not only the safety-related materials or components that require vigilance. The counterfeiting or fraudulent activities involved with the non-safety materials and components within our nuclear power plants during construction and operation will also require enhanced vigilance and diligence in ensuring our supply chain meets our requirements and specifications."

> Chairman Klein challenged the industry by asking "Are we being vigilant enough? Is industry doing enough to: Establish more rigorous safeguards and oversight in procurement? Find quality vendors and ensure that they maintain high standards? Make quality assurance a top priority. That is my charge to you today."[31]

In April of 2008, the NRC published Information Notice 2008-04, "Counterfeit Parts Supplied to Nuclear Power Plants" [6]. This information notice points out several issues involving counterfeit or suspected counterfeit items identified at nuclear plants in the United States, and prompted the EPRI JUTG to revisit the issue of counterfeit items in our industry.

Subsequently, the NRC has actively encouraged industry forums involved in procurement to be proactive in addressing the issue of CFIs.

The NRC has also presented on the topic of CFIs several times at EPRI JUTG meetings, NUPIC meetings, and ANS conferences held in 2008 through 2013. In their numerous presentations, the NRC has stressed the sharing of information between licensees and the supplier community.

In 2011, the U.S. NRC published SECY 2011-0154, "An Agency-wide Approach to Counterfeit, Fraudulent and Suspect Items,"[4] and the NRC Staff Review of Counterfeit, Fraudulent, and Suspect Items [3]. In these documents the NRC discusses agency actions and proposed industry initiatives to address CFI concerns.

3.2.2 U.S. Nuclear Industry

In 2009, EPRI published the original version of this report, 1019163 Counterfeit, Fraudulent and Substandard Items: Mitigating the Increasing Risk [32]. In 2010, EPRI published 1021493, Counterfeit and Fraudulent Items: A Self-Assessment Checklist [5] as well as 1020955 [33], a computer-based training module on CFIs available to EPRI members. In 2011, EPRI completed development of a database that can be used by EPRI members around the world to capture and share information on incidents of suspected CFIs.

In 2011, NEI formed the CFI Task Force (CFITF) in response to safety, regulatory, and economic concerns related to the potential impact of CFI. Utilities, major nuclear suppliers, INPO and EPRI are represented on the CFITF. NEI interactions with the NRC on key CFI issues and the results of a 2013 survey of industry CFI practices provided valuable input used to prepare this report.

In 2012, the Institute of Nuclear Power Operations (INPO) issued an industry event report to its members that summarized operating experience and resources related to CFI. INPO also expanded plant evaluations to include consideration of measures to preclude use of CFI.

3.2.3 International Nuclear Industry

The Nuclear Energy Agency Committee on Nuclear Regulatory Affairs is an organization comprised of representatives from international nuclear regulatory agencies. In October of 2011, the Nuclear Energy Agency Committee on Nuclear Regulatory Activities published NEA/CNRA/R(2011)9, Operating Experience Report: Counterfeit, Suspect and Fraudulent Items [9]. In February of 2013 the Committee followed-up with NEA/CNRA/R(2012)7, Regulatory Oversight of Non-conforming, Counterfeit, Fraudulent and Suspect Items (NSFSI) [10].

4
RECENTLY IDENTIFIED COUNTERFEIT AND FRAUDULENT ITEM INCIDENTS

4.1 Recent Discovery of Counterfeit Items in Nuclear Plants

There are no known instances of counterfeit or fraudulent items failing in operating U.S. plant safety-related equipment or systems. However, there are instances of CFIs that were identified during receipt inspection and rejected before being placed in inventory. There are also a few instances where counterfeit items have been identified in non-safety-related inventory, and in one case installed in non-safety-related systems. In addition, suppliers have reported several incidents of suspected CFIs.

Introduction of these counterfeit items into the nuclear supply chain can be considered "shots on goal," or operational experience that clearly demonstrates the need for licensees and suppliers to implement effective controls that reduce the potential for the introduction of counterfeit parts into nuclear generation facilities.

4.1.1 Fraudulent Items Discovered in Korean Nuclear Plants

The recent discovery of fraudulent items in Korean nuclear plants and resulting plant shutdowns emphasize the serious nature and consequences of CFIs in nuclear power plants. It was widely reported in late 2012 that two nuclear units in Korea were shut down and experienced extended outages while thousands of parts supplied with fraudulent certification were replaced. An investigation was conducted to review all the items procured over the preceding ten years. The investigation found that about 8,000 commercial grade items were supplied with certification fraudulently stating they had been successfully dedicated. The majority of these items were fuses, switches, and cooling fans. Although none of these items failed or experienced other performance problems that impacted plant safety, the operating company decided to shut down two reactors so that all of the installed fraudulent items could be replaced as quickly as possible.

On May 28, 2013, two additional nuclear units were shut down after falsified test reports were discovered for installed safety-related control cables. Outages at four additional reactors were extended to enable replacement of all installed cables that failed the testing [34]. Investigation determined that a testing agency manipulated the test results in their reports to show passing results for control cables which had failed the test.[35] Korean-based suppliers involved in the incidents did not provide items to U.S.-based nuclear facilities.

4.1.2 Counterfeit Electrolytic Capacitors

In March of 2013, a U.S. nuclear plant identified suspect capacitors during receipt inspection. The utility was careful to purchase the capacitors from an OEM-approved supplier. The supplier notified the utility that although the capacitors could not be sourced from the OEM in time to meet the desired delivery date, the capacitors could be sourced from a broker within the desired timeframe. During receiving inspection it was noticed that the electrolytic capacitors were not marked with a date code. The utility followed up with the OEM-approved supplier and the OEM, who confirmed the capacitors were counterfeit.

Figure 4-1 is a photograph taken during inspection that shows "suspect counterfeit" capacitors and "not suspect" capacitors. The OEM later confirmed the suspected counterfeits were indeed counterfeit and the "not suspect" capacitors were authentic.

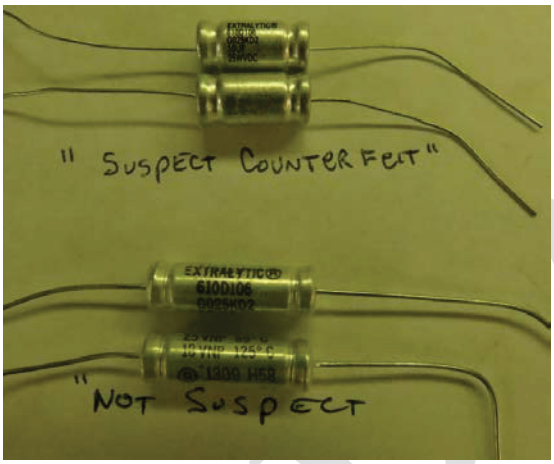


Figure 4-1
Authentic electrolytic capacitors in proximity to counterfeit capacitors

A previous incident was reported in August of 2008 by Millstone Nuclear Power Station, where electrolytic capacitors no longer available from the equipment OEM were determined to be counterfeit through failure of a dimensional inspection and subsequent investigation.

4.1.3 Fire Protection Equipment

In March of 2013 the NRC issued Information Notice 2013-02, Issues Potentially Affecting Nuclear Fire Safety [36]. The notice discusses alerts posted by Underwriter's Laboratories (ul.com) on April 30, July 13, and August 31, 2012 that warn of several counterfeit fire sprinklers and counterfeit UL markings on single jacketed fire hose.

Eight counterfeit items are discussed in the information notice. A search indicated possible matches for one of the eight counterfeit items at three U.S. nuclear facilities. The facilities were notified and none reported discovery of suspected counterfeit items. A second item had a possible match at one U.S. facility. The facility had already investigated and identified the affected stock code as at-risk prior to being notified as they were aware of the UL notice before

the NRC information notice was published. Although no counterfeit fire protection items discussed in the information notice were reported discovered, this example illustrates the potential impact of CFIs and the importance of reviewing available operating experience.

4.1.4 QT/Opto - Fairchild Semiconductor Optocoupler

In August of 2009, a manufacturer that provides instruments to nuclear power plants questioned the authenticity of several Fairchild H24A1 phototransistor optocouplers during a routine inspection. The optocouplers are used in timers that are supplied to several of its nuclear customers.

Upon further investigation, the OEM and an authorized distributor claimed that the optocouplers were not legitimate Fairchild parts. The optocouplers were procured from a company in the United States.

The manufacturer who identified the parts did not alert the seller, but did notify the appropriate authorities. Figure 4-2 below illustrates the differences in packaging and size that caused the manufacturer to verify the authenticity of the parts. The smaller device is packaged incorrectly, and the date code indicates that the suspect device was manufactured after the genuine H24A1 device was discontinued by the OEM.

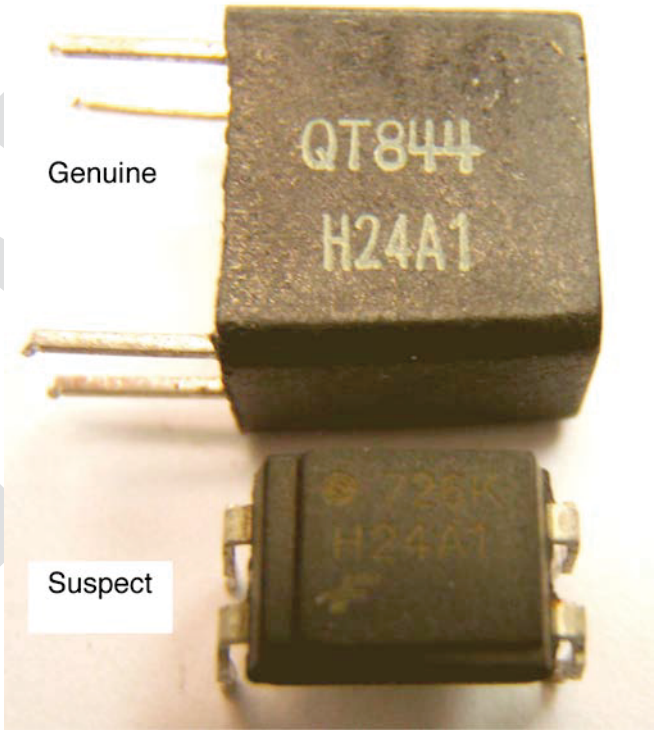


Figure 4-2
Genuine (Above) and Suspect (Below) Phototransistor Optocouplers

4.1.5 Ladish Stop-Check Valve

NRC Information Notice 2008-04 [6] documented an incident where a Ladish stop check valve was installed in a non-safety-related application in Plant Hatch. In 2007, two counterfeit 5 inch 150 pound Ladish stop check valves were discovered; one was installed and the other was in the warehouse.

Visual inspection of the genuine and fraudulent valves depicted in Figure 4-3 suggests that the "L" cast into the valve body of the genuine valve was added to the body of the fraudulent valve by welding and grinding.

In September 2007, personnel investigating a malfunctioning stop check valve in the main generator stator cooling water system at Pilgrim Nuclear Power Station discovered that the valve installed was not a genuine Ladish 5-inch stop check valve. Pictures of the suspected counterfeit valve were sent to the Ladish Valve Company, where it was confirmed that the installed valve was not a Ladish valve. This was a non-safety-related purchase, and vendor oversight and documentation controls were insufficient to identify a substandard part prior to installation.

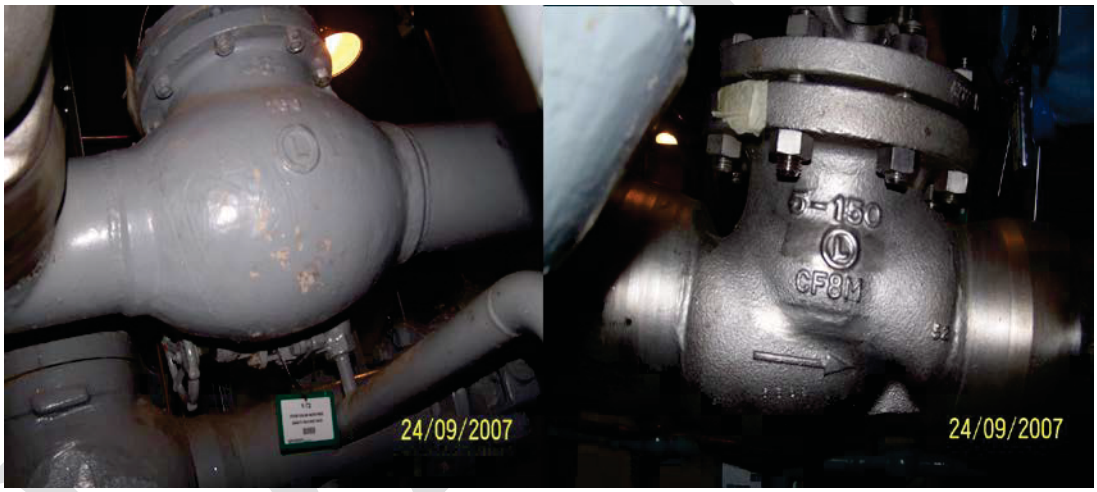


Figure 4-3
Ladish Valve (Left) – Counterfeit Valve (Right)

4.1.6 Circuit Breakers

NRC Information Notice 2008-04 [6] documented an incident where counterfeit Square D circuit breakers were recalled by the U.S. Consumer Product Safety Commission (CPSC) in notices regarding counterfeit breakers distributed by Scott Electric Company from March 2003 through April 2006 [37], Connecticut Electric from February 2005 through August 2006 [38], and North American Breaker Company from May 2005 through May 2006 [39]. The recalled circuit breakers were manufactured in China and were fraudulently labeled "Square D." According to the CPSC, the counterfeit circuit breakers can fail to trip when overloaded, posing a fire hazard to consumers.

Duke Power's Catawba, McGuire, and Oconee Nuclear Power Plants found that they had purchased Square D circuit breakers during the suspected timeframe. Duke inspected their Square D circuit breakers in accordance with instructions provided by the manufacturer and confirmed that Oconee's and McGuire's were genuine. Catawba Nuclear Plant removed four alleged "Square D" circuit breakers from inventory that could not be verified as authentic.

In March of 2008, Calvert Cliffs Nuclear Power Plant personnel identified five counterfeit breakers and removed them from inventory. The breakers did not have the amperage rating painted in white on the breaker's toggle switch.

Discussions with Schneider Electric-Square D during the course of developing this document support the recommendation that the nuclear licensees communicate with original equipment manufacturers. Detailed information in the following pages was provided by Schneider Electric and is also available on Schneider Electric website. Information provided on OEM websites can be an invaluable tool for receipt inspectors. However, this information may be updated frequently, so receipt inspectors may need to check the website during each receipt of associated items. Detailed information is provided in Figures 4-7 and 4-8.

Schneider Electric, the manufacturer of Square D breakers, is one of many manufacturers that are actively and aggressively pursuing the organizations and entities that perpetrate counterfeiting of their products.

Eaton Corporation's is another circuit breaker manufacture that collaborates with industry and governments worldwide to prevent counterfeiting. Eatons's website (www.eaton.com) recently introduced an online Circuit Breaker Authentication tool. Using this resource, the bar code, style number, and date code from an Eaton breaker can be entered online to determine if the breaker is authentic or suspect as shown in Figure 4-4.

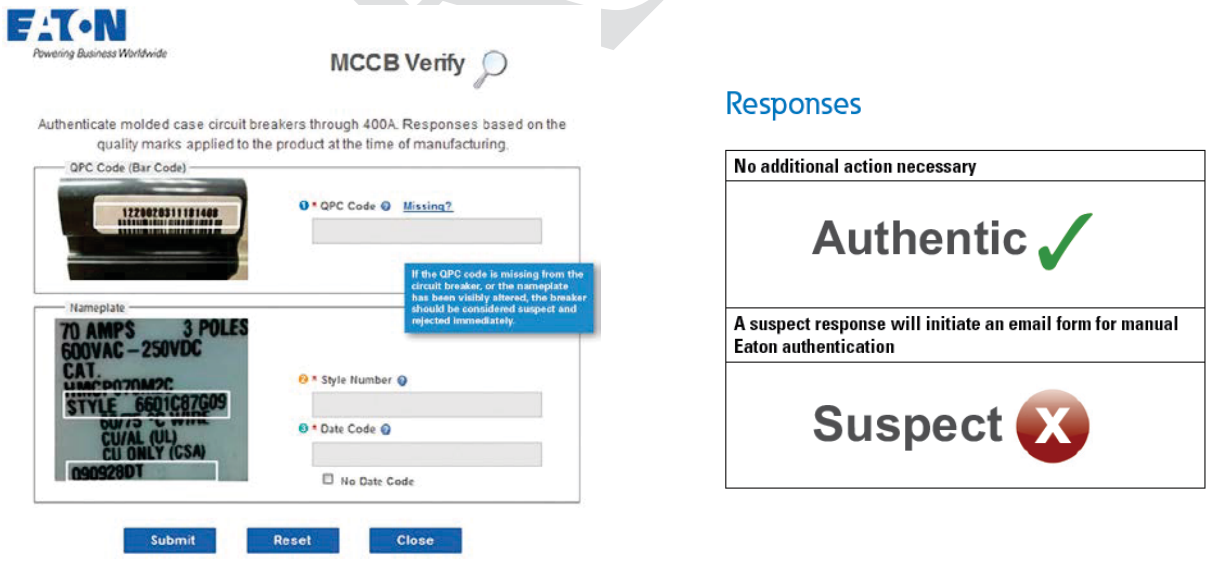


Figure 4-4
Eaton Corporation's online Circuit Breaker Authentication tool

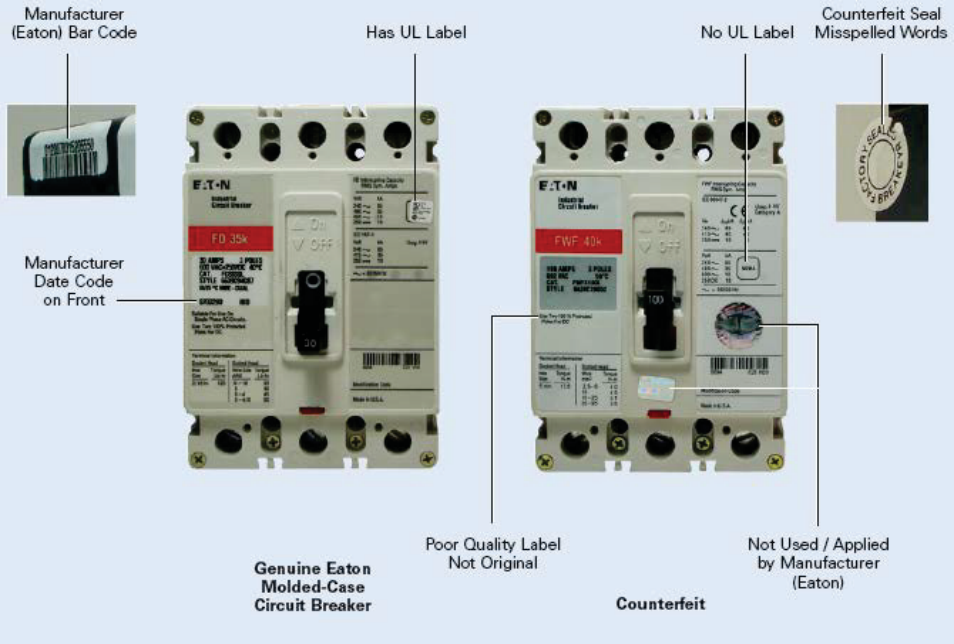


Figure 4-5
Genuine versus counterfeit Eaton Corporation circuit breaker

- **Missing date code**—Removed to hide the age of the circuit breaker.
- **Old date code**—Any product over two years old no longer has any factory warranty.
- **Factory seals broken or removed**—Product has been tampered with and has no warranty or guarantee that it meets performance specifications.
- **Mislabeled products to change size/type**—Product has been tampered with, causing a possible misapplication and a safety hazard.
- **Non-English text**—Product appears with labels in languages other than English.
- **Missing UL® sticker**—Product is likely imported illegally and is not certified to meet U.S. electrical codes.
- **Low-quality labeling and/or misspelled words**—Product is likely a counterfeit and made with sub-standard materials and workmanship.
- **Old Westinghouse or Challenger label**—These products have not been produced since 1999 and 1997 respectively.
- **Not in a carton or in older white cartons**—Product is used and/or outdated.

Figure 4-6
Known characteristics of counterfeit Eaton Corporation circuit breakers

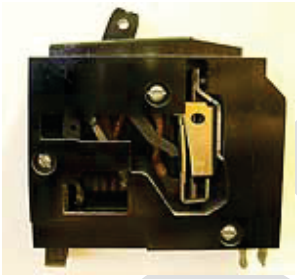
Examples of Counterfeit Square D Breakers	
	**Counterfeit QO Circuit Breaker from Taiwan** • 3200A short circuit rating instead of the normal 10,000A • Contacts weld due to improper materials • Erratic tripping - no calibration • Flexible connector inside the CB is frayed and fails • No temperature compensation • Magnetic trip is inoperable • Does not meet UL standards (or any other standards)
	**Counterfeit QO Circuit Breaker from Mexico** • 3000A short circuit rating instead of the normal 10,000A • No arc chamber insulation • No thermal adjustment - hand bent bimetal • Erratic tripping - no calibration • Low grade phenolic material • No temperature compensation • Magnetic trip is inoperable • Does not meet UL standards (or any other standards)
	**Counterfeit QO Circuit Breaker from Japan** • 5000A short circuit rating instead of the normal 10,000A • Vulnerable to contact welding • No arc chamber insulation • No thermal adjustment - hand bent bimetal • Does not meet UL standards (or any other standards)

Figure 4-7
Illustrations of Counterfeit Schneider Electric Circuit Breakers

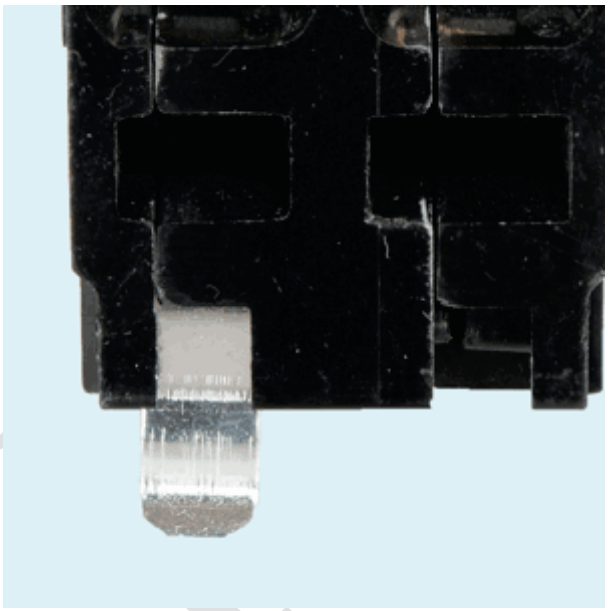
Characteristics of Counterfeit Schneider Electric Circuit Breakers	
	
Some counterfeit labels do not indicate the country of origin.	Many counterfeit breakers have a bright silver rail clip.
	
Some counterfeit breakers have printed logos or logos that appear to be etched. Some counterfeit breakers may be missing the logo.	Ampere ratings molded into the handles of new (post 1999) breakers indicate that the product is counterfeit.

Figure 4-8
Characteristics of Counterfeit Schneider Electric Breakers

4.1.7 Integrated Circuits

Recent industry operating experience includes an incident in January of 2008 at Millstone Nuclear Power Station, where Millstone personnel were unable to calibrate two portal monitors used for monitoring members of the public in case of an evacuation in the Millstone Emergency Planning Zone for the State of Connecticut. The company that assembled the electronic components for the portal monitors subsequently provided Millstone with a bulletin which describes the particular integrated circuit board chip as a counterfeit. The date code and chip codes were incorrect. It appears that these codes were altered to make the chips appear newer than they were.

4.1.8 Flowserve Globe Valves

In September of 2006, Alabama Power's Farley Nuclear Power Plant advised Flowserve Corporation that a 0.75 inch nominal pipe size Class 1500, ASME Section III, Division I, Class 1 Y-Globe valve in Farley's inventory that was labeled as stainless steel (ASME SA-182, Type 316) exhibited characteristics of a carbon steel valve, including rust blooms and magnetism (see Figure 4-6). Upon further investigation, Flowserve confirmed that the valve forging was, in fact, carbon steel incorrectly identified as stainless steel. Flowserve issued notification to the NRC and nuclear customers who had purchased the valves [40] in accordance with the requirements of 10CFR, Part 21 [41]. This notification prompted investigation by all licensees who purchased valves that were determined by the investigation to be at risk. Included are valves with bodies forged by DeKalb Forge Company of DeKalb, Illinois, for Flowserve, Kerotest, and BWIP (Borg Warner).

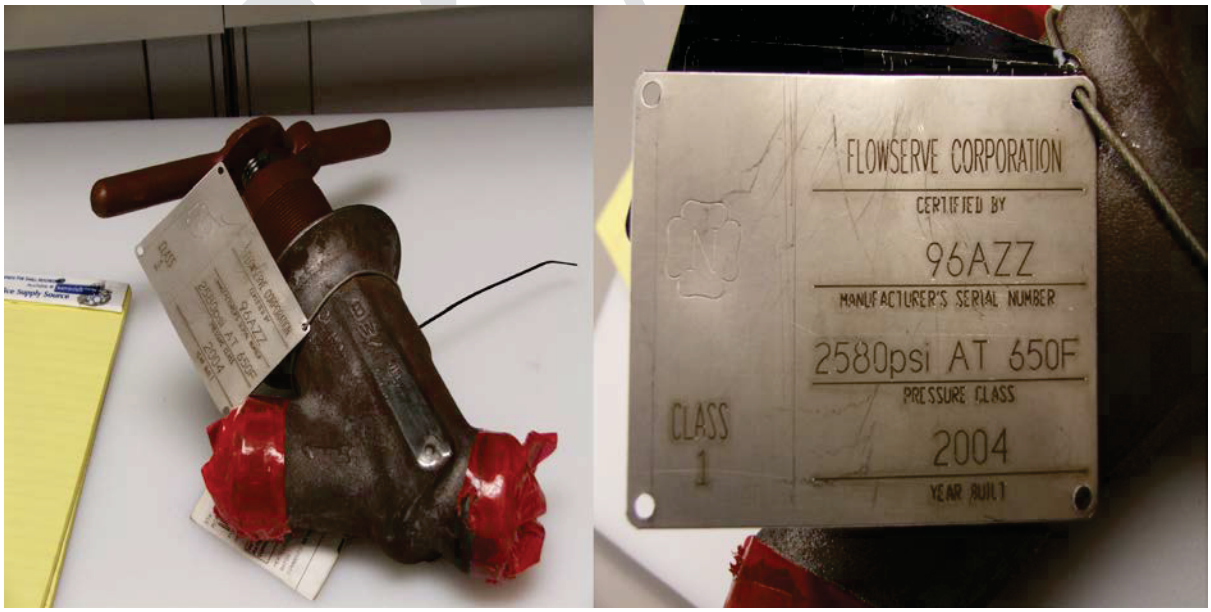


Figure 4-9
Carbon Steel Flowserve Y-Globe Valve Certified and Sold as Stainless Steel

4.2 Recent Incidents in Other Industries

4.2.1 Lifting Slings

In March of 2013, a power plant reported discovery of fraudulently marked polyester lifting slings during an inspection of a contractor's equipment before it was permitted on-site. Markings on the polyester slings indicated that the slings should be removed from service when red core yarns were visible. However, close inspection of the slings revealed that no red core yarns were present.

4.2.2 Lifting Lugs on Flowserve Pump Skids in the Petrochemical Industry

In April of 2009, Shell Canada issued a Learning From Incident (LFI) [42] on substandard lifting lugs found on a Flowserve pump skid. After transporting a skid into its final position, a worker noticed one of the four lifting lugs was loose. Upon slightly turning the lug, the bolt securing the lug fell out of the pump base. Further inspection revealed that all four lifting lug bolts were of insufficient length and did not provide enough exposed thread to properly engage the lifting lug.

4.2.3 Pipe Burst in Datong Power Station in China

In October of 2006, a pipe certified at ASTM A335, P91 is reported to have failed at the Datong Power Station Unit 2 in Qinghai Province, China [43]. The pipe burst resulted in two deaths, one severe scalding, and several other injuries. The pipe was allegedly manufactured in China, but was fraudulently certified by a company in Houston, Texas, as being the correct material.

4.2.4 Radioactive Steel Manufactured in India

An article from *Spiegel Online International* dated February 16, 2009 [44], reports that German authorities have identified a significant amount of contaminated steel. The article, titled "Contaminated Imports: Finds of Radioactive Steel on the Rise in Germany," states that the radioactive steel can be traced back to three steel works in India and that the contaminated products, including bars, valves, and elevator buttons, are probably the result of Cobalt 60 found in recycled food irradiation, medical technology, or other sources being introduced into blast furnaces during the fabrication of steel products.

4.2.5 Fraudulent ISO 9001 Certification

In October of 2008, a fraudulent ISO 9001 certificate was discovered at a DOE facility during verification of supplier-submitted reports prior to award of the procurement. The procurement of valves was for a DOE Category 2 nuclear facility. Because the event involved a U.S.-based company as well as its foreign affiliate, it suggests that that all ISO 9001 certificates should be verified with the issuing Registrar. This incident was documented in the DOE Lessons Learned process. Lesson ID: CWI-ICP-2009-001, Date: 10/8/2008 [45].

Related Technical Point

Note: ISO-9000 certification or registration may not be used as a basis for accepting safety-related items in nuclear power plants. Although an ISO 9001 QA program may indicate that a supplier implements certain controls, a commercial grade survey of the supplier's QA program by the licensee is required to verify that the controls related to the purchased item(s) safety function and critical characteristics are adequately documented and implemented by the supplier. In addition, the licensee's purchase order must include reference to the controls by procedure number or other reference. Finally, the supplier must provide certification to the licensee that the specific controls were implemented for the item(s) provided in accordance with the purchase order.

4.2.6 Fraudulent AWS Certification

In an incident reported to AWS on September 2, 2008, a company forged an AWS stamp and created a bogus Certified Welding Inspector (CWI) number to pass its work off as inspected when it was not. An article reporting this incident in *Inspection Trends* [46] includes a similar incident involving a fraudulently modified CWI wallet card, which an individual carried with him as proof of certification. The individual altered the expiration date to reflect current certification.

4.2.7 Titanium Tubing Manufactured for Use in the V-22 Osprey

The United States Attorney charged a quality assurance supervisor for Anco-Tech with fraudulently issuing a false certificate of conformance for titanium tubing manufactured for use in the V-22 Osprey [47].

4.2.8 Counterfeit Electrical Products Identified by NEMA

Electrical products impacted by counterfeiting that have been identified by NEMA [48] include:

- Conduit fittings
- Circuit breakers
- Control relays
- Control switches
- Electrical connectors
- Electrical receptacles
- Fuses
- High-voltage surge arrestors
- Lamps

5
CONTRIBUTORS TO COUNTERFEITING AND FRAUD

There are many contributors to the abundance of CFIs that are presently found in highly critical applications, general industrial products, and consumer products.

5.1 Profiteering

One obvious common element is the potential for profit. Counterfeiters can sell their products at prices equal to or lower than the price of genuine items without bearing the costs associated with research and development, correct materials and manufacturing, testing, liability, licensing, marketing, and other expenses typically incurred by legitimate manufacturers.

According to the U.S. Immigration and Customs Enforcement National Intellectual Property Rights Coordination Center, tremendous profits are generated from the sale of counterfeit and substandard items, and criminal organizations take advantage of established smuggling infrastructures and routes [49].

5.2 Globalization of the Supply Chain

The quantity of goods manufactured in the United States and other western countries has decreased significantly over the past few decades. The trend in many industries has been to move manufacturing facilities to foreign locations in response to customers who demand less expensive products.

Manufacturing technologies and capabilities are rapidly expanding the regions that produce inexpensive materials and products. The rapid spread of manufacturing and manufacturing capacity provides would-be counterfeiters with the tools required to quickly manufacture products that may appear almost identical to the original.

Unfortunately, the engineering expertise, design experience, knowledge of materials, and ethics accumulated through years of experience and typically found to be characteristic of long-established manufacturers may not always be found in manufacturing facilities that were quickly established to adopt existing manufacturing machinery and technology to fabricate items without necessarily becoming involved in or having accumulated experience in the associated engineering, testing, etc. Manufacturers in this situation are at risk of providing substandard items by either knowingly or unknowingly making changes to raw materials and parts that were not thoroughly evaluated, based on the item's function as opposed to being considered acceptable based on the item's appearance. In addition, manufacturers in this situation may

suddenly be faced with excess capacity, which can be an incentive to use excess capacity to manufacture counterfeit or fraudulent items.

Asia is a region that is worthy of mention. Many cases of CFIs originating in Asia have been reported and documented. "Don't buy from China" was the single most popular response to a question on the DOC survey that asked "What is the best thing you can do to avoid counterfeit and fraudulent items? [12]"

The flow of counterfeit materials is particularly high coming out of Asia. Figure 5-1 shows that although China is clearly the largest source of counterfeit electronics, incidents also originate in other countries, including the United States.

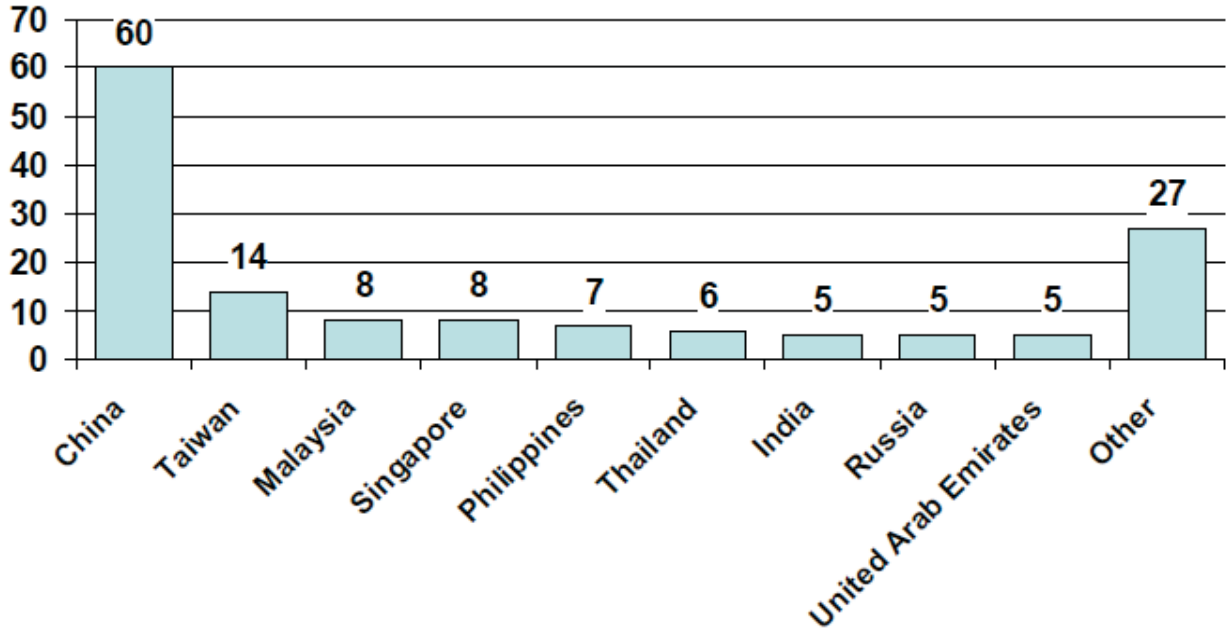


Figure 5-1
Countries Suspected as Sources of Counterfeits (2008 estimates)
(from U.S. Department of Commerce, Survey Results, January 2010 [11])

CFIs may take many forms. CFIs may:

- Be new or used
- Appear to be marked with original branding
- Be marketed via the internet by unauthorized brokers to unsuspecting suppliers
- Be imperfectly manufactured or refurbished
- Be provided with fraudulent certification or quality designations
- Be poorly tested or not tested at all

The "quality" of counterfeited items covers a wide range. Perhaps the "best" CFIs are produced by companies who were, at one point, licensed by an OEM to produce a certain quantity of items and who sell more than the licensed quantity or who sell nonconforming or rejected items (seconds) in secondary marketplaces. These items may be almost identical in appearance and function to the genuine articles. However, there is risk that they may fail early or fail catastrophically, compromising personnel safety and resulting in damage to plant equipment. Perhaps the worst are counterfeits that are quickly manufactured and labeled with a genuine part number, but are noticeably different in both appearance and function from the genuine article.

According to the DOC survey results, the most frequently encountered counterfeits were products with invalid markings, nonworking original component manufacturer (OCM) products, and new items re-marked and sold as a higher grade. Figure 5-2 is taken from the DOC survey that focused primarily on electronic components and microcircuits.

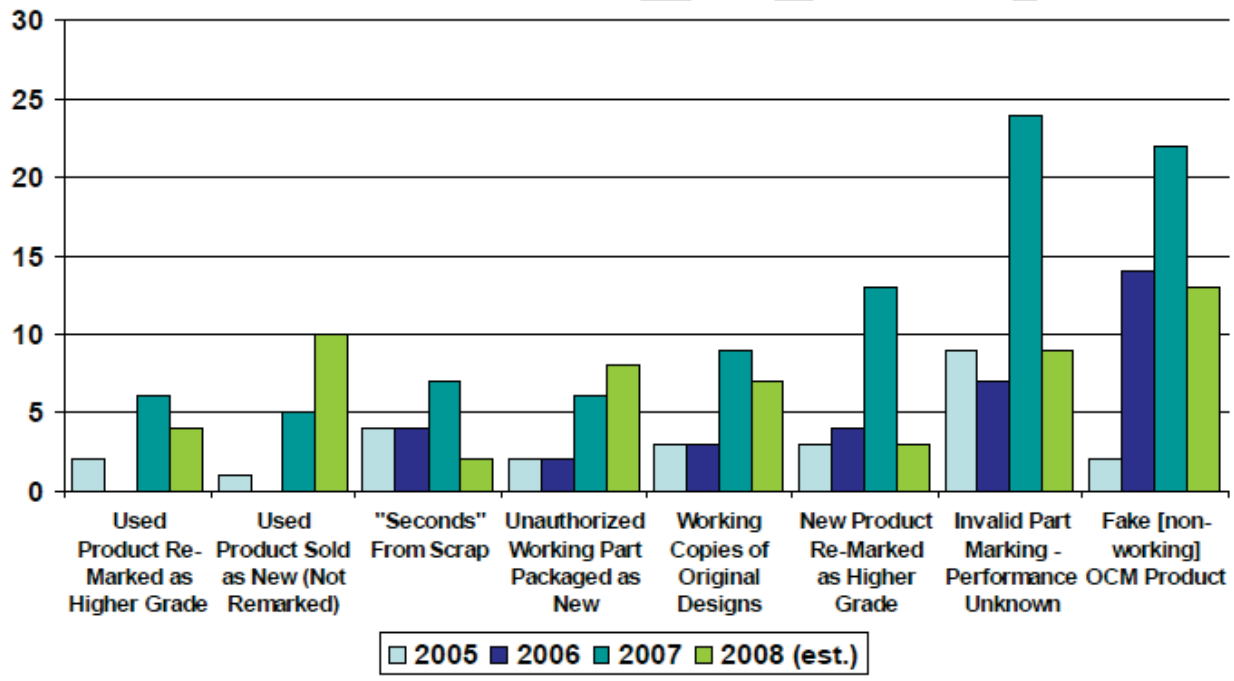


Figure 5-2
Counterfeit Incidents by Type of Problem (2005-2008)
(from U.S. Department of Commerce, Survey Results, January 2010 [53])

5.3 Low Cost Items

In addition, counterfeiters target low-value, high-demand items that are not likely to be subject to enhanced inspection. Figure 5-3 below is taken from results of the survey. The figure shows that although some expensive items are targeted, the item price typically targeted by counterfeiters ranges from $0.11 to $500.00.

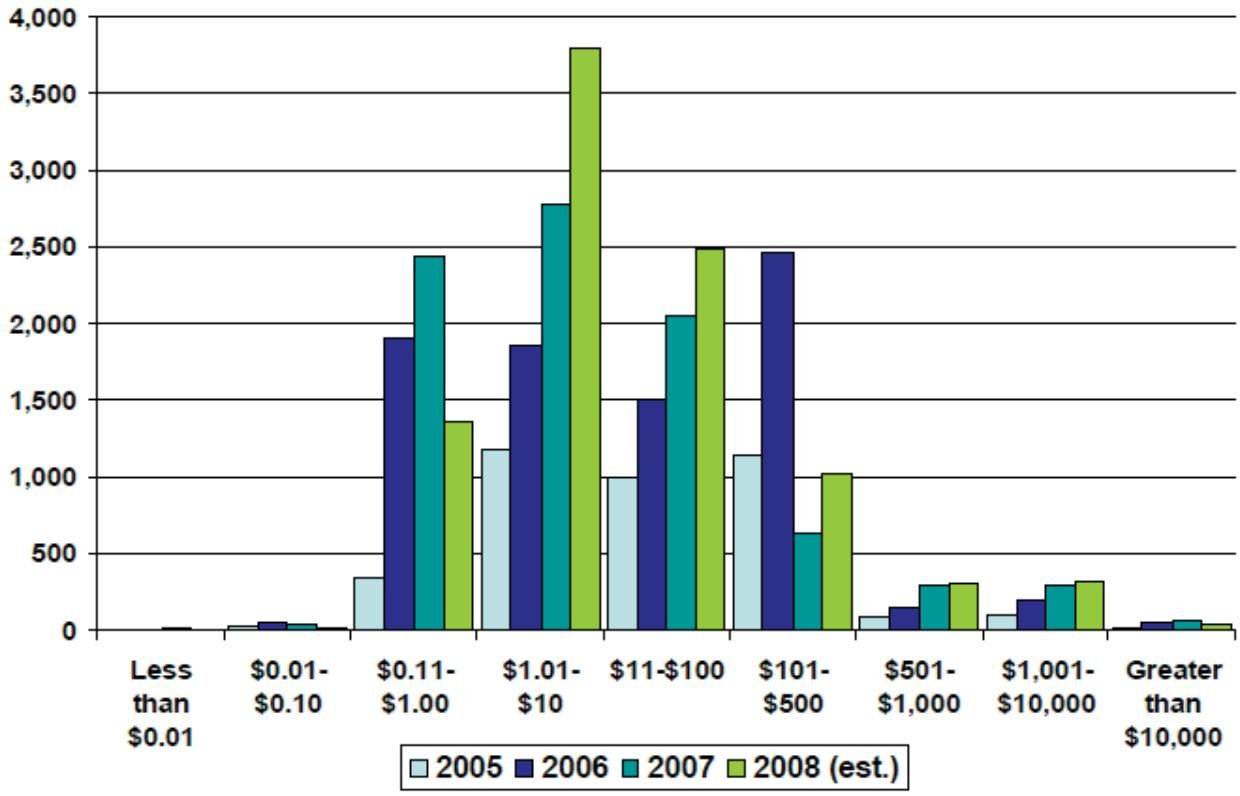


Figure 5-3
Counterfeit Incidents by Product Resale Value
(from U.S. Department of Commerce, Survey Results, January 2010 [11])

5.4 Lack of Awareness, Complacency, or Loosening of Existing Controls

Counterfeit items ranging from footwear to integrated circuits are being discovered in large numbers. However, it is possible that customers who have long-standing relationships with their suppliers simply assume that their suppliers are addressing the issue of CFIs until a received or installed item fails testing and investigation reveals that failure may be related to a substandard or fraudulent item. As the number of items originating from new sources increases, well intentioned but unaware and unsuspecting suppliers can find themselves unknowingly purchasing and using counterfeit or fraudulent materials or parts.

In some cases, utilities and their suppliers that are not fully aware of the extent of the CFI issue may fail to implement sufficient controls. In other cases, utilities and suppliers who are fully aware of the extent of the CFI issue may simply assume that it does not have the potential to impact them. Lack of training and awareness of the extent of the CFI problem and the associated risks can certainly contribute to proliferation of the problem.

5.5 Changes in Technology

New technologies or standards introduced to the marketplace present yet another challenge, as a plant or supplier's inventory of items meeting new standards may unknowingly become mixed with inventory of items meeting the old standards — even when they are not completely interchangeable. An example would be electronic components that are produced to meet RoHS standards. RoHS is an acronym for reduction of hazardous substances that refers to European Union Directive 2002/95 that imposes standards that ban or restrict selling new electrical devices containing certain levels of mercury, lead, hexavalent chromium, and cadmium as well as some flame retardants.

Although changes like this may appear subtle at first, a change to the chemical composition of leads on electronic devices can impact the quality of connections made through soldering, result in changes to soldering procedures, and even prompt changes to manufacturing processes and related components. Precautions must be taken to ensure that items are specified correctly and completely in purchase documents to ensure compliance with the (original) standard and to prevent mixing of stock manufactured to old and new standards in inventory.

5.6 Obsolescence and Short Product Lifecycles

5.6.1 Obsolescence

Obsolescence can be a double-edged sword when it comes to counterfeiting and its impacts. Recently obsolete items that are in high demand are prime targets for counterfeiters because these items are difficult to obtain, but are still in high demand. However, obsolete items that are not in wide demand are less efficient targets for counterfeiters since they will not be able to sell as many items.

Figure 5-4 indicates that counterfeiters will target both obsolete items and items currently in production. Surprisingly, it appears that the vintage of safety-related equipment in the current nuclear fleet has perhaps played a role in insulating the fleet from CFIs. Although much of the equipment and many of the parts purchased to support operating plants are obsolete, demand for these items is currently so low that counterfeiters would rather

focus their efforts on producing items that will yield a larger return on their investment. Therefore, counterfeiters often target highly recognized brands and high-volume, low-cost items that are in high demand and are found installed in many applications.

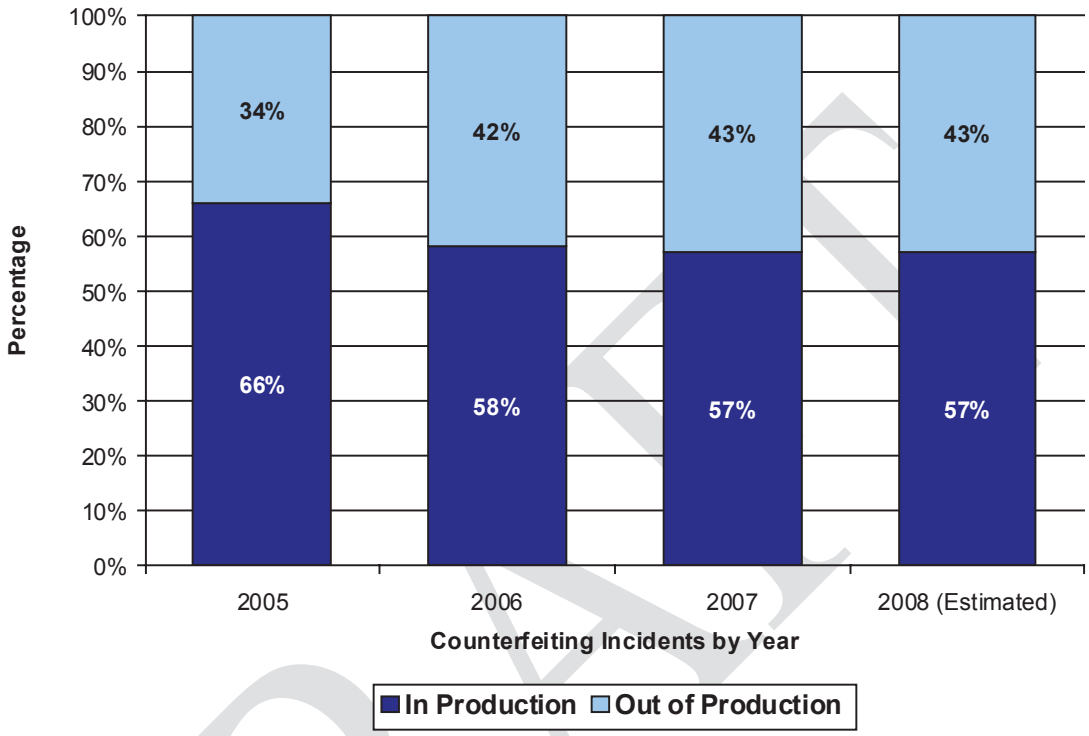


Figure 5-4
Percentage of Counterfeiting Incidents Related to In-Production vs. Out-of-Production Items (from U.S. Department of Commerce Survey Results [12])

5.6.2 Short Product Lifecycles

As technologies advance at an ever-increasing pace, product life cycles become shorter. This is particularly true with respect to digital devices and microelectronics. Most of the commercial nuclear facilities in the United States have been in operation for over 20 years and contain equipment that was designed and manufactured years before initial operation.

As an example of product lifecycles, the evolution of personal computer microprocessors over a 25-year period can be considered. Advances in manufacturing and materials technology continue to reduce the size of transistors and increase the capacity and speed of microprocessors. In 1978, Intel released the 8086; its fourth-generation microprocessor that was first used in the IBM personal computer in 1981. Subsequently, Intel released the 80286, 80386, 80486, Pentium, Pentium Pro, Pentium II, Pentium III, Pentium 4, Pentium M/Centrino, and Pentium D microprocessors as indicated in Table 5-1, showing data that are available on Intel's website [50].

Table 5-1
Evolution of the Intel PC Microprocessor

Year	Microprocessor	Initial Clock Speed	Number of Transistors
1978	8088	5 MHz	29,000
1982	80286	6	134,000
1985	80386	16	275,000
1989	80486	25	1,200,000
1993	Pentium™	66	3,100,000
1995	Pentium Pro™	200	5,500,000
1997	Pentium II™	300	7,500,000
1999	Pentium III™	500	9,500,000
2000	Pentium 4™	1.5 GHz	42,000,000
2002	Pentium M™	1.7 GHz	55,000,000
2005	Pentium D™	3.2 GHz	291,000,000

Each time a new microprocessor was released, the technology enabled the manufacture and sale of PCs with enhanced capabilities, as well as the development of increasingly sophisticated software and peripheral supporting devices. In this example, advances in technology result in shorter product lifecycles because the marketability of the first microprocessors rapidly decreases with the release of subsequent microprocessors. As marketability decreases, the manufacturer must react by focusing their resources on the development and production of new products to remain competitive. Production of the old products is phased out.

Unavailability of the 80286 microprocessors from the OEM creates a market for counterfeit or fraudulent 80286s. Although unavailability of an 80286 microprocessor may not impact a typical business that replaces PCs every few years, it can present a significant challenge for the organization responsible for maintaining an expensive asset with an expected life of more than 20 years that is controlled by an 80286. Significant design changes may be required to use the 80386 because changes in architecture and clock speed might make it incompatible with interfacing devices and systems used to control the asset. Therefore, they may be forced to find 80286s from a source other than the OEM until the design changes can be implemented.

In addition, the 80286 PCs being disposed of by the business that is replacing them with 80386 PCs might end up being dismantled so that the components can be “recycled” and resold by counterfeiters as new replacements that are desperately needed by organizations trying to maintain their assets that rely on the obsolete 80286 microprocessors. As product life cycles get shorter, the demand for out-of-production items increases as does the amount of used product that can be fraudulently represented and resold as new product.

5.7 Enforcement Challenges

Government agencies in the United States and worldwide are involved in enforcing laws that pertain to counterfeiting, fraud, and intellectual property. Enforcement is difficult for many reasons. The sheer magnitude of the problem makes enforcement difficult. In addition, by the time authorities are alerted to the existence of an incident, the entity who sold the item has had the opportunity to hide the evidence because their customer probably called them to inquire, ask for a return authorization, or complain before they called the authorities. Another difficulty is the complex and convoluted route CFIs travel before reaching the end user. Some items are sold via the internet, while others pass through many brokers, distributors, and agents, who each take possession of the items. Identifying the entity that introduced the counterfeits or altered the documentation can be difficult.

Even when the responsible parties are identified and damages are awarded in a court of law, it is often difficult or impossible for the OEM or OCM to recover damages from the small, independent manufacturers, brokers, and businesses that produce and distribute CFIs, as well as the ones with ties to foreign governments. The parties responsible can simply shut down their operation and start up a new one.

6
PREVENTION OF COUNTERFEIT AND FRAUDULENT ITEMS

Measures implemented by the nuclear industry over the past several decades continue to serve us well. This guidance expands upon earlier guidance and provides greater emphasis on preventive measures.

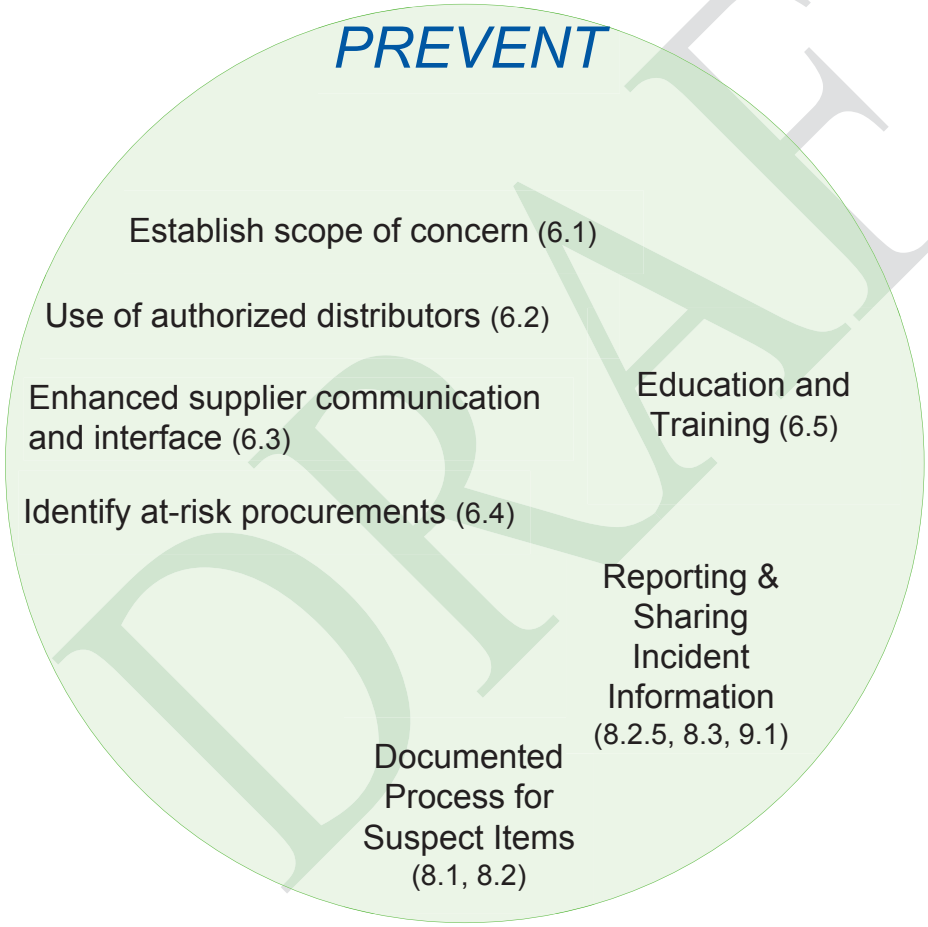


Figure 6-1
Key Measures for Preventing Counterfeit and Fraudulent items

Figure 6.1 captures preventive measures that are included in Figure 1-1. In addition to a brief description of each preventive measure, the number of the Section that discusses how to accomplish the measure is included.

6.1 Establish an Appropriate Scope of Concern

The issue of CFIs is not limited to the specific types of equipment discussed in Appendix C of EPRI NP-6629 [13] and U.S. NRC Generic letter 89-02 [7]. Section 1 of this report discussed the broad range of concern that includes safety-related, non-safety-related, and non-plant items such as lifting and rigging equipment. The scope of concern should be effectively communicated to appropriate individuals and departments in the organization so that appropriate measures are taken. For example, items such as ammunition that may be of concern might not be received under normal warehouse processes, so the organization(s) responsible for procurement and receiving of ammunition would need to be aware of the concern regarding supply of reloaded ammunition in order to take appropriate countermeasures.

6.2 Use Authorized Distributors

The second most noted response to a question on the DOC survey that asked "What is the best thing you can do to avoid counterfeit and fraudulent items ?" was "Be wary of brokers" [12]. Brokers who are not authorized by the OEM or OCM are not subject to restrictions on how and where they can source the items they sell. Legitimate brokers who will literally go to the ends of the earth to locate hard-to-find items for their customers provide a needed service. However, brokers may not always be cognizant of the history or chain of custody associated with the parts they sell and may not possess the capability to adequately test or inspect the items. Therefore, brokers and unauthorized distributors are more likely (than authorized distributors) to supply CFIs, used, or refurbished parts.

When not procuring directly from an OEM/OCM, use of authorized distribution networks is a best practice frequently mentioned during benchmarking. To the extent possible, items should be procured only from authorized distribution networks. Authorized distribution networks typically employ a rigorous process for assuring component authenticity. However, as illustrated by the electrolytic capacitor example in Section 4.1.2, procurements from an authorized distributor may need to be considered at-risk if the authorized distributor is sourcing the items from an entity other than the OEM/OCM.

A statement on a supplier's website or advertisement indicating they are an OEM/OCM-authorized distributor should not be considered adequate confirmation of the supplier's current status. Authorization should be confirmed with the OEM/OCM. In addition to product authentication information, many OEMs and OCMs provide information about authorized distributors on their websites.

6.3 Enhanced Supplier Communication and Interface

Perhaps the most obvious method of reducing exposure to CFIs is to communicate with suppliers. Discuss the issue with your suppliers to identify concerns and expectations. The experience can be a productive exchange of information for both parties and can enhance the relationship. In the context of this discussion, *suppliers* encompasses suppliers of both safety- and non-safety-related items, including original equipment and component manufacturers as well

as distributors; engineering, procurement, and construction firms (EPCs); and other suppliers of basic components.

6.3.1 Request Information from Suppliers on Known CFI Issues

Figure 6-2 indicates the ways in which the 498 suppliers involved in the DOC survey discovered CFIs. It is not surprising that one of the most common ways that counterfeits are identified is when the items are returned to the supplier or manufacturer as defective. This would suggest that suppliers or manufacturers have the most current and complete knowledge of CFI incidents related to the items they provide. Therefore, opening lines of communication with suppliers and requesting information about CFI issues can be one of the most effective ways to obtain current information.

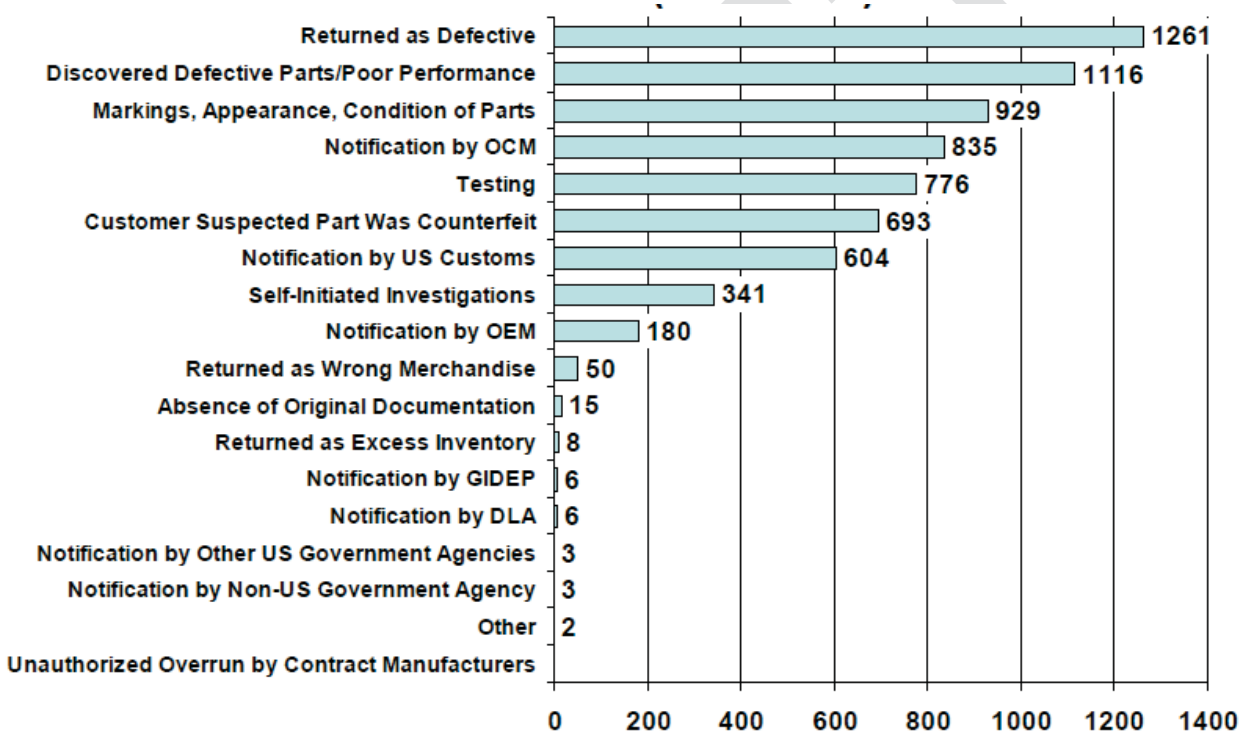


Figure 6-2
Ways Counterfeit Items Are Identified
(from U.S. Department of Commerce, Survey Results, January 2010 [11])

In addition to requesting and establishing a means of obtaining and capturing information from suppliers, enhanced communication includes enhanced qualification of suppliers and enhancing contractual requirements.

6.3.2 Enhanced Qualification of Suppliers

Suppliers with Approved Quality Programs

Suppliers that provide basic components are subject to periodic audits. Because CFIs are an emerging issue of growing concern, assessment checklists should be modified to include pertinent criteria and questions that may be used by auditors. NUPIC and NIAC have modified their checklists to include assessment of a supplier's inspection/testing processes for identifying suspect (including counterfeit/fraudulent) items or components that may not be those ordered. Licensees and their suppliers should consider similar changes and/or including questions similar to those below on their supplier assessment checklists.

Commercial Suppliers

The criteria used to qualify suppliers that provide augmented quality and standard commercial maintenance, repair, and operation (MRO) items can also be enhanced. Typically, these suppliers are qualified on the basis of factors such as financial viability.

Soliciting the response of these suppliers to questions such as those included below should be considered when qualifying commercial suppliers.

Supplier Evaluation Questions

Questions that might be considered in evaluating a supplier include:

1. Does the supplier employ or are they familiar with authentication technologies that can be used to ensure positive identification of authentic items?
2. Does the supplier consider counterfeiting to be a problem? If so, do they dedicate resources to the problem? Do they train their staff on the issue?
3. Does the supplier provide a mechanism for customers to confirm that the supplier is authorized by the original manufacturer to distribute items being purchased (within their approved distribution network)?
4. Does the supplier accept returned merchandise? If so, is it inspected before being placed into stock for resale? Has the supplier experienced the return of suspect items?
5. Does the supplier screen items and materials to ensure that they are genuine?
6. What do they do in the event that a counterfeit item is identified?
7. To whom do they report the discovery of an incident involving a suspected counterfeit or fraudulent item? Are provisions in place to quarantine the items to prevent comingling with acceptable inventory and to notify customers who might have been impacted?
8. Does the supplier use any sources of information to identify incidents of counterfeit items that might impact their products?

9. Does the supplier use contract manufacturers? If so, do they have contractual provisions that require proper disposal of any manufacturing overages and nonconforming items?
10. How does the supplier identify and dispose of items that are rejected at the receiving dock or as the result of quality control inspections? Are measures taken to prevent these items from being cleaned up and sold as legitimate by unscrupulous entities?
11. Does the supplier test purchased items and raw materials that are considered critical to the design and function of the products you purchase?
12. Who can be contacted and what resources can the supplier make available in the event that you have questions about an item they have manufactured or sold?
13. Would the supplier be willing to notify the licensee in writing when items being provided were not obtained from an authorized distributor?

Suppliers whose responses to these types of questions indicate that they are aware of the risk associated with CFIs and that they are prepared to deal with CFIs may be considered good candidates. Licensees and suppliers may wish to educate suppliers who are not familiar with the issue and work with them to enhance their programs, or they may choose to select alternate suppliers and sub-tier suppliers who are already effectively addressing the issue of CFIs.

6.3.3 Evaluation of Proposals

The methodology and criteria used to evaluate suppliers' proposals should be assessed. Price has become increasingly important and is often the most heavily weighted factor in determining which supplier is awarded a purchase order. In addition, performance incentives for personnel involved in the purchasing and contracting processes often include criteria based on total savings.

Experience validates the adage, "If it's too good to be true, it probably isn't." One situation described during benchmarking involved failure of aircraft systems related to the failure of CFIs supplied for a procurement that was awarded based on cost savings of less than 10 cents each on discrete electronic components.

Proposal evaluation and incentive policies that influence selection of the lowest-cost proposal should be reviewed to ensure that they do not result in selection of the lowest cost bid without evaluating other criteria such as:

- Is the supplier an OEM-approved distributor?
- Does the supplier have proven capabilities?
- Is the supplier willing to certify that the items are genuine?

6.3.4 Clear Specifications and Contractual Requirements

Suppliers are under significant pressure to reduce prices, and in some situations, a supplier may unintentionally sell an item that is not acceptable to their customer. To ensure that the supplier is

aware of important requirements, clear and concise specifications and item descriptions should be included on procurement documents for all items included in the scope of concern.

Descriptions included in procurement documents for critical items should identify important characteristics as opposed to simply referencing a part or model number. This allows inspections at receipt to include verification of the complete item description as well as the part or model number.

In addition, contractual requirements that address CFIs should be included in procurement documents. The purpose of contractual requirements is to notify the supplier that CFIs are a concern and to inform the supplier of actions that may be taken if items they provide are identified as suspect and/or are determined to be counterfeit or fraudulent.

Standard procurement clauses should relay the licensees' expectation of the vendor/supplier regarding CFIs, and licensees should pursue any incidents involving CFIs as indicated in the clause. Examples of standard contractual clauses that address CFIs are included in Appendix B of this report. It is highly recommended that standard clauses be submitted to an organization's legal counsel for review and approval prior to implementation.

6.3.5 Enhance and Assess Supplier Awareness

It may be useful to periodically transmit a letter or brief survey to suppliers to determine if they are aware of CFIs and are taking precautions to avoid them. The letter could also request notification in the event a CFI incident that impacts products you purchase is detected, request information on how to ensure the products.

6.3.6 Safeguard Intellectual Property

In some cases, it is necessary to provide design information to suppliers to ensure that the correct replacement items are furnished. In such cases, care should be taken to legally safeguard the design information, particularly when the information is being provided to organizations other than the OEM, OES, or entity with rights to manufacture the items in question. This may involve limiting distribution of design information on a "need to know" basis and obtaining nondisclosure (or other appropriate) agreements prior to disclosing the information.

6.4 Identification of "At-Risk" Procurements

Identification of at-risk procurements promotes *prevention* of CFIs. Implementing enhanced inspection and testing to provide reasonable assurance of authenticity for items identified as at-risk is more targeted at *detection*. Both topics are addressed in this section since the concept of "at-Risk" procurements initiates in *prevention*.

6.4.1 "At-Risk" Procurements

When alternate sources must be used due to obsolescence, expedited schedule, or other reasons, the procurement should be flagged as "at-risk" so that appropriate precautions may be taken to provide reasonable assurance of authenticity.

A procurement should be identified as "at-risk" if the purchasing agent, material analyst, or procurement engineer or other personnel are aware of exposure to risk factors known to be associated with CFIs including (but not limited to one or a combination of) the following:

- The product is known to be susceptible to counterfeiting
- The product is a commodity known to be susceptible to counterfeiting (as opposed to an engineered product)
- OE has identified receipt of suspected counterfeit or fraudulent items of similar type (i.e. manufacturer/supplier and part/model number combination)
- The supplier will not accept a purchase order (for example, the supplier only permits credit Card orders)
- The supplier is new (without an established record)
- The supplier is unknown or unverified (for example, an internet-based) supplier or broker
- The supplier is not the OEM or is not authorized by the OEM or the licensee to provide the items being purchased (authorization critical for items such as Lifting/Rigging; Safety; Fire Protection; and so forth)
- The supplier takes exception to anti-counterfeiting/fraud language in the purchase order
- The supplier is dismissive or non-responsive to purchaser concerns and inquiries regarding supplier protections against and experience with CFIs
- The cost/unit quoted is significantly lower than other quotes or previous purchase prices (on orders imposing similar requirements)
- The items being ordered are known to originate from regions known to provide counterfeit items of that type (such as integrated circuits originating from China)

6.4.2 Implementation of Precautions for "at-Risk" Procurements

Enhanced inspection and testing criteria should be specified for items that are procured via "at-risk" procurements.

These precautions might include additional receipt inspection/testing requirements commensurate with the item's criticality such as:

- Inspections and tests to confirm critical performance attributes of the item

- Assuring that markings or labels of consensus standards or testing agencies, such as Underwriters Laboratory (UL) or Nationally Recognized Testing Laboratories (NRTL) are legitimate
- OEM or OCM recommended inspections to authenticate the item

Recommended inspection requirements and acceptance criteria related to authenticating an item can sometimes be found on the OEM or OCM website or by contacting them directly.

For large lots of items or in cases where destructive inspection/testing is specified, industry accepted sampling plans such as EPRI TR-017218-R1 [50] should be used.

Escrow payments are a precaution employed throughout the DOE complex as a measure to address procurements considered at-risk. Payment (or partial payment) for larger orders or complex items is deposited into an escrow account and is released to the supplier only after completion of enhanced inspections and tests by the purchaser

6.5 Education and Training

Education and training of sourcing, receiving, and quality control receiving inspection personnel promotes *prevention* of CFIs. Education of personnel such as storekeepers who handle items after they are accepted for use, maintenance, production, assembly and craft personnel also promotes *detection* of CFIs. Both topics are addressed in this section as education and training are initially targeted at *preventing* CFIs.

Perhaps the most important and effective means to avoid CFIs is through training personnel and making them aware of the issue. Training raises the level of awareness and communicates the potential impact that CFIs can have on plant operations as well as nuclear and industrial safety.

The probability that CFIs will be identified increases significantly when personnel are familiar with the types of items that are known to be counterfeited and the characteristics that indicate items or associated documentation may not be genuine.

Training on CFIs should be provided to everyone involved in the procurement process from the specification of items to installation. Groups that should be considered include management, engineering, procurement, vendor quality, maintenance, warehouse, and source and receipt inspection.

Training should address the role that each individual within each discipline plays in identifying potential CFIs. Refresher training should be offered periodically and should include a review of the types of CFIs that have been recently reported. Training should include photograph and (when possible) hands-on examples of CFIs so that personnel can develop a tactile appreciation for the differences (or lack thereof) when examining the items.

U.S. NRC Information Notice 2012-22, Counterfeit, Fraudulent, Suspect Item (CFSI) Training Offerings [51] provides a comprehensive list of applicable training.

6.5.1 Buyers and Purchasing Agents

Buyers, purchasing agents, and contract negotiators should be familiar with the issue of CFIs. These individuals are the primary interface with suppliers and should be trained to:

- Recognize and identify "at-risk" procurements
- Follow processes or procedures to ensure the appropriate organization considers imposing precautions such as enhanced inspection or testing for "at risk" procurements
- Screen commercial suppliers to determine if they are aware of and take precautions against CFIs
- Communicate concerns about CFIs to every supplier
- Request that suppliers provide information about known incidents of CFIs involving products they provide
- Award procurements to authorized distributors or OEMs/OCMs whenever possible
- Look for signs that suppliers may be providing CFIs, such as bids that are significantly lower than other bids or the item's historical average unit cost

6.5.2 Receiving Inspectors and Warehouse Staff

Receiving inspectors and warehouse personnel (who process item receipts and put-away items) play a key role in preventing the introduction of CFIs. These individuals should be:

- Familiar with the guidance included for identifying fraudulent items in Appendix C of EPRI NP-6629, Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants [13] U.S. NRC Generic Letter 89-70, "Possible Indications of Misrepresented Vendor Products," [8] and U.S. NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products [7]
- Trained to follow processes or procedures for procurements identified to be "at-risk" (reference section 6.4) and ensure that appropriate precautions such as enhanced inspection or testing are conducted for them
- Trained to identify abnormalities in packaging, labeling, product marking, workmanship or certification that may indicate items are counterfeit or fraudulent items
- Trained to identify physical signs evident on hardware that may indicate items are counterfeit or fraudulent items
- Trained to ascertain and recognize both legitimate and suspicious manufacturer markings, trademarks, logos, and so forth that may indicate if items are counterfeit or fraudulent
- Aware of where and how to report CFIs or items suspected of being counterfeit or fraudulent items (such as the plant corrective action system)
- Trained to follow a consistent plan of action every time items suspected of being counterfeit or fraudulent items are identified, including quarantining and controlling items, contacting the OEM/OCM, and carefully deciding if the suspect items should be returned to the supplier

- Trained to check existing operating experience or data on CFIs to the extent practical when receiving items

6.5.3 Maintenance, Production, Assembly and Craftspeople

Scrutiny by maintenance, production, assembly and craftspeople may be the last opportunity to avoid installation of CFIs. These individuals are often in a position to visually compare the item being removed with the replacement item and to identify any differences between the two items in orientation, labeling, configuration, or other characteristics.

These individuals should attend periodic training where operational experience along with examples of CFIs specific to their discipline are presented for "hands-on" examination along with their genuine counterparts. A general awareness of the CFI issue along with experience gained through handling actual examples of CFIs will greatly increase the probability that CFIs will be identified before installation.

In addition, the following types of concepts can be communicated:

- Include CFI precautions in pre-job briefings when appropriate
- Communicate the importance of identifying any discrepancies between installed and replacement items, and obtaining confirmation of acceptability before installing replacement items.

6.5.4 Engineering

Appropriate engineering staff should also attend training in CFIs. These individuals may benefit by being able to more readily identify "at-risk" procurements. Engineering organizations may also be responsible for specifying enhanced inspections and testing necessary to reasonably assure that items purchased "at-risk" are authentic and may be included as participants in source inspections of complex equipment.

6.5.5 External Audit and Inspection Personnel

Staff that perform audits, surveys, and source inspection/surveillances of suppliers and sub-tier suppliers should be trained in the types of questions that should be asked when conducting these activities and to identify suppliers as "at-risk" when concerns are identified.

A list of suggested questions is included in Section 6.3.2 and more detailed assessment questions are included in EPRI 1021493, "Counterfeit and Fraudulent Items: A Self-Assessment Checklist. [4]"

6.5.6 External Organizations

External organizations such as suppliers and service providers that play an active role in the procurement of items can also benefit from training that is delivered and updated periodically to address the latest industry experience and knowledge related to CFIs. Opportunities to share training with external organizations such as those listed below should be considered when appropriate:

- Manufacturers and suppliers
- Distributors
- Contractors and service providers

Training developed for licensees can communicate and promote understanding of licensee CFI concerns. Training developed by suppliers and equipment OEMs/OCMs often contains detailed information about their products as well as feedback provided by their entire customer base. This training can enhance licensees' product-specific knowledge.

7
DETECTION OF COUNTERFEIT AND FRAUDULENT ITEMS

Conduct effective receiving inspections is a thought that immediately comes to mind when asked what can be done to address the problem of CFIs. Although receiving inspections are certainly an important method of detecting CFIs, other opportunities for detecting CFI should also be taken as appropriate.

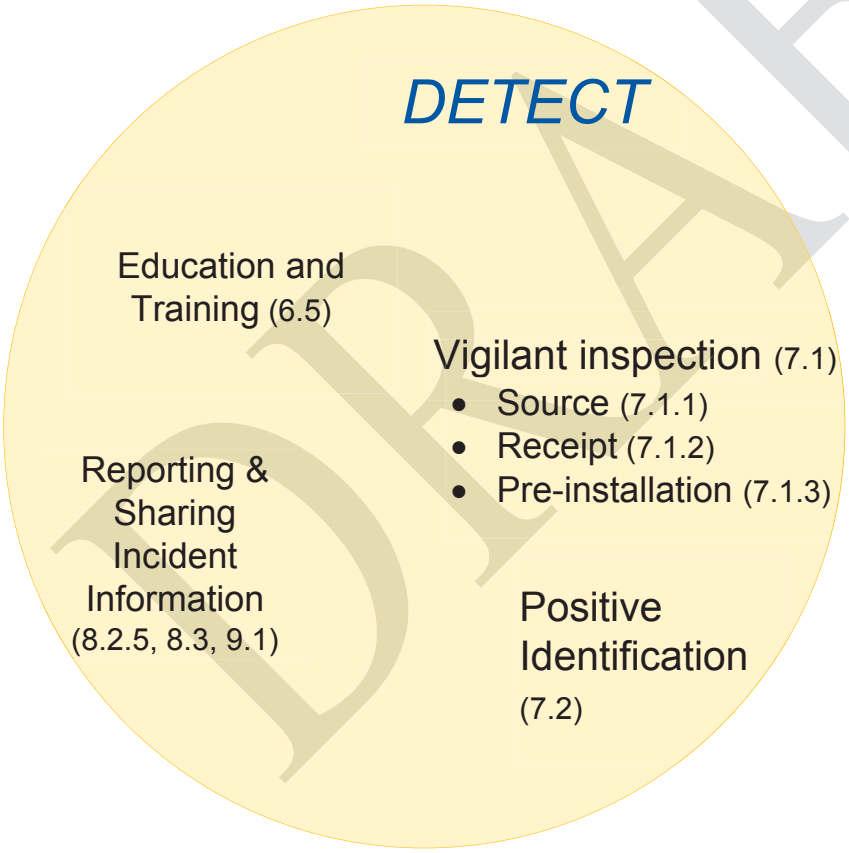


Figure 7-1
Key Measures for Detecting Counterfeit and Fraudulent items

Figure 7-1 captures detective measures that are included in Figure 1-1. In addition to a brief description of each detective measure, the number of the Section that discusses how to accomplish the measure is included.

7.1 Vigilant Inspection

Considerations for performing vigilant inspections to detect CFIs include:

- Individuals who perform as well as individuals that plan source and receipt inspection of items should consult available operating experience when determining inspection criteria.
- The inspection guidance contained in NRC Information Notice No. 89-70 [8] and EPRI NP-6629, Appendix C [13], is effective and should continue to be followed. Applicable information from EPRI NP 6629 Appendix C [13] should be included or referenced in procedures and training for receiving inspectors, source inspection personnel, and warehouse personnel.
- In cases where an item is known to have been counterfeited in the past, the OEM/OCM should be consulted for advice and guidance on inspecting the item.
- Using digital photographs of authentic items that can be associated with stock codes in plant information systems so that the photographs can be compared to incoming items during receiving activities
- When appropriate, verifying the authenticity of certification or test results provided by entities other than the supplier by contacting the entity that provided the certification or test result
    - This may not apply in all cases, such as verification of documentation supporting certification provided by ASME Quality System Certificate or Certificate of Authorization holders.
    - This type of verification may be appropriate in situations where documentation from a supplier without a QA program approved by the purchaser is relied upon to accept an item for use. Implementation of this type of precaution may have led to much earlier detection of the fraudulent certifications in Korea (discussed in Section 5.1.1)
- Involve and consult other personnel who are knowledgeable of the product when suspicious indications are observed

7.1.1 Source Inspection

When appropriate, staff trained as noted in Section 6.5.4 and 6.5.5 can participate in source inspections of complex equipment prior to acceptance.

7.1.2 Pre-Receipt Inspection by Engineering and Receipt Inspection

When appropriate, engineering and other technical staff trained as noted in Section 6.5.4 can participate in inspections of complex equipment conducted as part of the acceptance process during receiving activities prior to placing the item into usable inventory.

Receiving and warehouse staff trained as discussed in Section 6.5.2 should perform appropriate receipt inspection of supplied items including safety-related, non-safety-related and non-plant items.

7.1.3 Pre-Installation Inspection

Maintenance, production, assembly and craft personnel trained as noted in Section 6.5.3 Staff trained as noted in Section 6.5.3 should identify any discrepancies noted between items being installed and items being removed

Maintenance, production, assembly and craft personnel trained as noted in Section 6.5.3 should identify any discrepancies noted between items being installed and design documents.

Note that these precautions should already be taking place as part of the overall design control and configuration management program.

7.1.4 Ad-hoc Inspection

Warehouse staff trained as noted in Section 6.5.2 should identify any discrepancies noted between new items and items already in-stock during processes such as put-away and cycle-counting of inventory.

7.2 Positive Identification

A detective measure primarily available to manufacturers is the use of positive identification techniques or authentication technologies. When appropriate, a manufacturer that uses this type of identification could share information with a customer to help the customer assure that received items are authentic.

Although use of these techniques are not widespread, certain manufacturers and trade organizations have implemented measures that are intended to enable consumers to verify purchased items are authentic. A paper titled Authentication Technologies for Brand Protection [48] that was published by the National Electrical Manufacturers Association (NEMA) discusses various technologies for product packaging that can be used to inhibit counterfeiting and tampering, as well as overt, covert, forensic and digital technologies that can be used to discourage counterfeiting and identify items that are not authentic.

Overt measures are familiar authenticity markings or labels that are clearly visible to customers. Semi-overt measures are visible, but require additional knowledge or tools to be read completely. Covert measures are authenticity markings that may only be read with the use of a special device that decodes the identification marking or makes it legible such as a viewer or certain frequency of light. Similar to covert measures, forensic measures are not visible, but require very specialized equipment or laboratory analysis to be detected.

Underwriters Laboratories (UL) anti-counterfeiting program employs semi-overt measures in the form of holographic labels in conjunction with guidance that describes how to determine the

labels are authentic including orientation of the label. UL aggressively trains law enforcement officials in how to authenticate UL markings [48].

Certain manufacturers make subtle changes to their packaging, logos or other identification markings periodically as an anti-counterfeiting measure. Unless there is active communication with the manufacturer, these changes may result in unnecessary problems during receiving. To prevent receiving problems, procedural guidance should be prepared to direct receiving personnel to the most current source of information available from the manufacturer instead of including specific instructions in the procedure that may be updated by the manufacturer before the item is reordered.

Another emerging technology that shows limited promise in the field of positive identification is radio frequency identification (RFID). RFID involves microcircuits (chips) with build in transponders (transmitter/receivers) that always will react to a radio signal sent by associated RFID readers or transceivers (transmitter/receivers). When a RFID chip receives the designated radio query, it responds by transmitting a code unique to the chip. The chips are typically powered by the radio signal itself, although active and passive versions of RFID chips are available. RFID chips could be embedded in products by the manufacturer so that customers equipped with the proper transceiver could scan received product to confirm authenticity as well as traceability to procurement documents and associated certification.

8
CONTROL OF COUNTERFEIT AND FRAUDULENT ITEMS

When a suspected counterfeit or fraudulent item is detected, it is important to control the item to ensure it is not used and that it is correctly investigated and dispositioned.

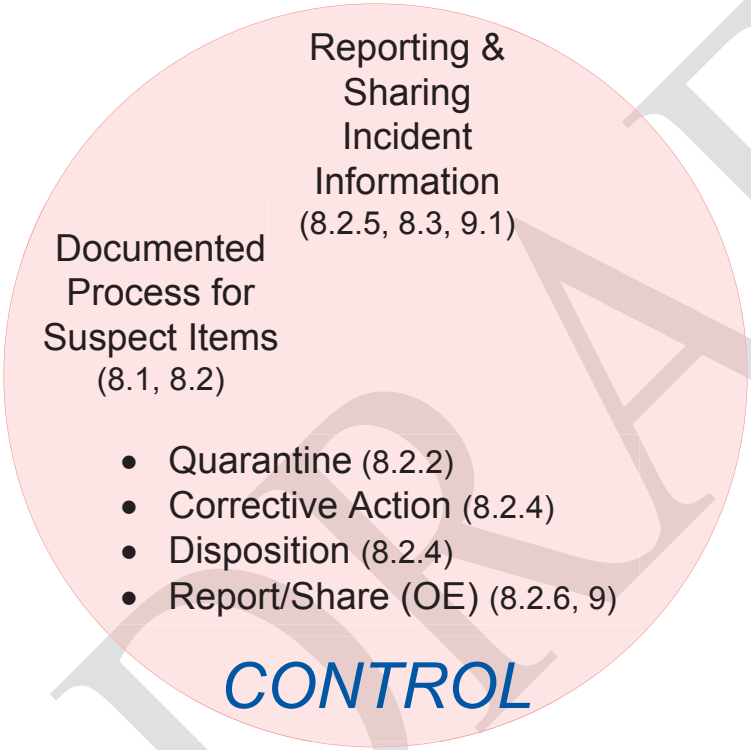


Figure 8-1
Key Measures for Controlling Counterfeit and Fraudulent items

Figure 8-1 captures measures to control CFI that are included in Figure 1-1. In addition to a brief description of each control measure, the number of the section that discusses how to accomplish the measure is included.

8.1 Documented Process for Addressing a Suspect Item Incident

The way in which an organization will respond to a suspected and/or confirmed counterfeit or fraudulent item incident should be documented in an appropriate procedure or directive to enable training and to assure the response will be consistent with established protocol.

A generic process for controlling suspected counterfeit items is included in Section 8.2 of this report. Important elements included in the generic process for controlling suspected CFIs include:

- Quarantine and clearly identify items as suspect
- Gather information necessary to document the incident
- Use of the corrective action system to document, track, and disposition the incident
- Making appropriate notifications (OEM, OCM, OES, and so forth)
- Careful consideration when determining if the supplier should be notified
- Careful consideration when determining if the item should be returned to the supplier
- Reporting the incident as operating experience to appropriate databases
- Notifying authorities when appropriate
- Physical disposition of the suspect items

8.2 Generic Process for Controlling and Reporting Suspect Items

The process depicted in Figure 8-2 is a generic process for controlling suspect items. The process guidance following Figure 8-2 reflects ideas and best practices identified during industry meetings and benchmarking.

Existing practices for controlling suspect items should be assessed against these generic process elements and updated as appropriate. For example, existing practice upon receiving a nonconforming item may be to call the supplier, return the items, and request a replacement. Some organizations experienced in addressing counterfeiting issues describe this practice as "returning criminal evidence" and recommend quarantining the items and either destroying them or returning them only to the manufacturer, even when they may have been purchased from a supplier other than the manufacturer. For this reason, the process guidance includes considerations to assist in deciding if and when a supplier should be notified or if a suspect item should be returned to the supplier.

Sections 8.2.1 through 8.2.8 provide additional information and discussion on each step in the generic process.

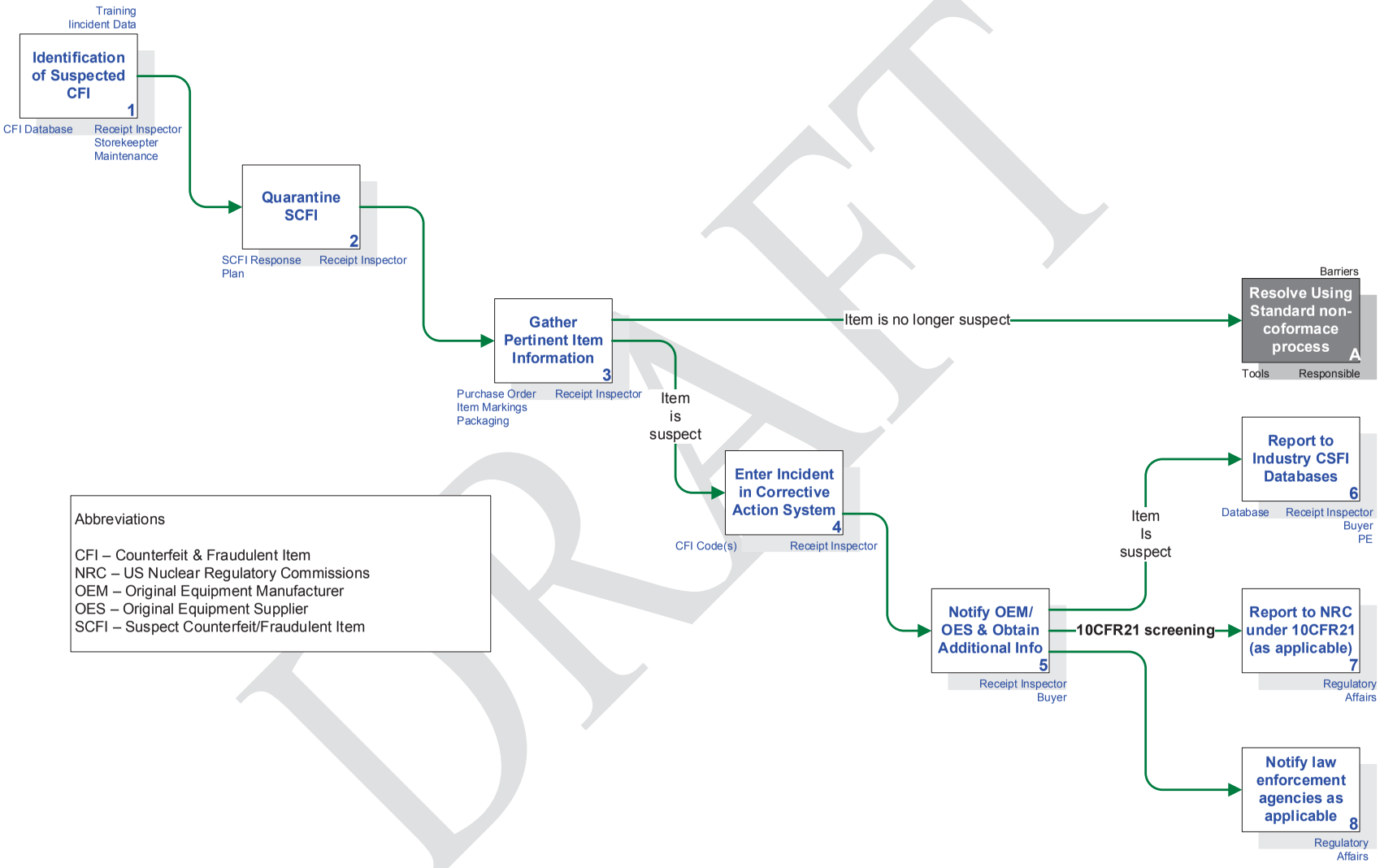


Figure 8-2
Generic Process for Controlling and Reporting Suspect Items

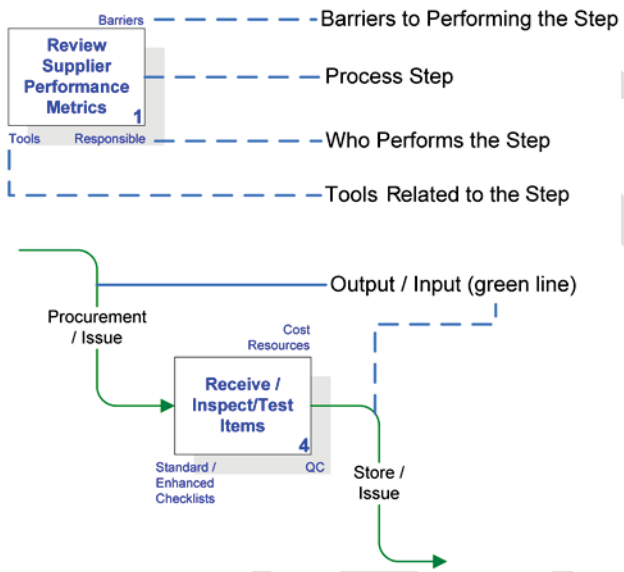


Figure 8-3
Process Flow Chart Key

8.2.1 Identification of Suspected CFI

Controls should be implemented to identify CFIs during the receiving and installation processes and during investigation of decreased performance or failure.

8.2.2 Quarantine Suspect CFI

If an item is suspected of being counterfeit or fraudulent, it should be physically separated from useable inventory and clearly identified as non-usable. It is also advisable to retain associated shipping containers and packaging and keep them with the suspect items.

Processes and procedures should include instructions for how to physically identify, segregate and quarantine suspected or confirmed counterfeit or fraudulent items so that they are prevented from entering usable inventory.

8.2.3 Gather Pertinent Item Information

Information about the suspect item should be collected for use in defining and documenting the issue and determining the authenticity of the item. The types of information to collect are identified in Appendix D.

If information gathered indicates the item is no longer suspect, the incident should be handled in accordance with normal receiving discrepancy processes. Otherwise, incident information should be entered into the corrective action or equivalent process regardless of safety classification, criticality classification, and so forth.

8.2.4 Enter Incident in Corrective Action System

As a minimum, incidents of suspect items should be documented in a corrective action system or similar system where the incident information can be accessed for use in preventing and resolving additional incidents of its kind.

8.2.4.1 Reporting Provisions

The corrective action system should include provisions for any required regulatory reporting. For example, if the item is a basic component that has been accepted into inventory or installed, it may be appropriate to initiate a notification in accordance with the requirements of 10CFR, Part 21, Reporting of Defects and Noncompliance [41].

It may be appropriate to include provisions in the corrective action program that trigger reporting incidents of suspected and confirmed CFI to industry operating experience databases.

8.2.4.2 Disposition of Suspected or Confirmed Counterfeit and Fraudulent Items

As previously mentioned, CFIs must be quarantined upon discovery to preclude their use. Eventually, the items will need to be physically dispositioned. Careful consideration should be afforded when determining how to physically disposition suspected or confirmed counterfeit or fraudulent items. Different actions may be appropriate for different types of items and different types of suppliers. Depending upon the situation and information obtained from the OEM/OCM, supplier, and so forth, it might be appropriate to:

- Destroy the items so they are permanently removed from the supply chain and cannot be resold
- Return the items to the OEM/OCM or supplier for further investigation and work closely with them to prevent recurrence
- Turn the items over to appropriate enforcement authorities

Communication with the OEM/OCM and enforcement authorities may be appropriate prior to determining how to disposition the items.

Other factors also include:

- Is the supplier an OEM/OCM or Authorized distributor? In such cases, the supplier will likely use the items to prevent recurrence and there is less risk that the items will be remarketed.
- Is the supplier a broker or a new or seldom used supplier that does not have a business relationship with the OEM/OCM? In these cases the supplier might be more likely to remarket the returned suspect items to others.
- Consider the quantity of items received. If a single item was procured, it may not be prudent to send it back to the vendor until a more detailed evaluation is completed. If a larger quantity was procured, it may be prudent to return some of the items to the OEM / OES for evaluation (while retaining the remaining procured quantities).
- If the item was procured from a supplier with an approved QA program meeting the requirements of 10CFR50, Appendix B [2], 10CFR Part 21 [41] reporting considerations may apply.
- Based on available information and on the level of cooperation from the OEM/OES/supplier, it may be cost-prohibitive to perform a lengthy investigation, and it may be prudent to just reject the item and not perform any further investigation.
- Another factor to consider is the potential for the NRC to need access to the quarantined item(s) for further evaluation.

Significant financial issues may be involved for high volume or high cost items, so all of these factors should be carefully considered. However, decisions regarding the disposition of suspect items should be properly documented in detail to justify the actions taken, and when appropriate can be worked jointly with the regulator for evaluation purposes.

8.2.5 Notify Manufacturer and Obtain Authentication Information

8.2.5.1 Notification of the Supplier

An issue pointed out by OEMs/OCMs during benchmarking is that some organizations immediately call the *supplier* (as opposed to manufacturer) of a suspected counterfeit or fraudulent item and return it in exchange for another. Although typical of many organizations, this response to receipt of a counterfeit or fraudulent item can exacerbate OEMs/OCMs' and law enforcement's efforts to eliminate counterfeiting. First, the supplier is "tipped off" that their practices are in question. Second, returning the suspected or confirmed counterfeit or fraudulent items is in effect returning evidence of the crime to the entity that committed the crime. For this reason, it is advisable as a general rule of thumb to report the incident to the original manufacturer before notifying the supplier (when the supplier is not the original manufacturer).

However, the primary objective for licensees and their suppliers is to assure that counterfeit or fraudulent items are not introduced into nuclear plants (enforcement is a secondary concern). In certain cases, the prudent course of action may be to notify the supplier. An example would be when a suspect item is received from a supplier with an approved quality assurance program meeting the requirements of 10CFR50, Appendix B. In such a case, expedient notification of the supplier would:

- Provide the supplier with an opportunity to quickly notify other nuclear customers
- Cause the suppler to perform an investigation and quarantine any similar items in their control

In other cases, it may prudent to notify the OEM/OCM and not notify the supplier.

8.2.5.2 Notification of the Manufacturer

Original manufacturers typically appreciate notification as they stand to lose the most when products bearing their name are not genuine or fail to operate properly. In some cases, manufacturers will only entertain notification from and provide information to entities who purchased the manufacturer's items from an authorized distribution channel.

Manufacturers lose revenue when counterfeit items are purchased instead of authentic items. Even if failures are eventually determined to be the result of counterfeiting, manufacturers' reputations can be damaged. Therefore, manufacturers are typically concerned when their brands are counterfeited. In addition, the manufacturer should be aware of any ongoing investigations involving their products and is in a position to alert the proper enforcement authority.

In some cases, such as those involving items that are no longer in production, a manufacturer may defer to an authorized distributor or other organization that is capable of providing product authentication information.

When notifying the manufacturer, request information about how to determine if the item is authentic. In addition, inquire as to the status of the supplier of the suspected counterfeit or fraudulent items, and determine if the supplier should be notified. Industries with experience in prevention of CFIs recommend that suspect items be confiscated and that they should not be returned to the supplier (for credit or exchange) from which they were purchased unless the supplier is an authorized distributor for the manufacturer. Although this is a typical response, returning the items to an unauthorized distributor or broker eliminates the possibility that the items could be used by the manufacturer or enforcement authorities in their anti-counterfeiting efforts.

8.2.6 Report to Industry CFI Database(s)

Provide the information to the appropriate industry databases so that the information is available for use by others in preventing a recurrence.

Protocols for sharing information about CFI incidents with industry databases are discussed in Section 9. Licensees should report to operating experience databases maintained by INPO and WANO as appropriate. EPRI members should access scfi.epri.com online or by email to input suspect item incident data.

Suppliers can submit input to the EPRI database via email. In addition, suppliers can report to industry databases that specialize in the types of items they use. As an example, ERAI maintains a commercially available database of non-conforming material and high-risk electronic components.

8.2.7 Regulatory Reporting Screening

In cases where the item is accepted for safety-related use prior to identification as a counterfeit or fraudulent item, reporting may be required in accordance with the requirements of 10CFR, Part 21 [41].

8.2.8 Notify Appropriate Law EnforcementnAuthority (Non-NRC)

Lists of enforcement agencies and industry organizations are included in Appendix C. Experience indicates that while notification regarding the discovery of a small quantity of items will not result in a full-scale investigation, authorities will record the information.

8.3 Effective Reporting, Gathering, and Sharing of Incident Information

Effective gathering, reporting, and sharing of incident information is included in the "control" portion of the Figure 8-1 and the corresponding text because these tasks are initiated after suspect items are discovered. However, as indicated in Figure 1-1, Effective reporting of incident information also plays important roles in prevention and detection of CFI.

A special code for incidents involving suspect items can be developed and used to report items in corrective action systems in a way that makes them easy to retrieve. When possible, the following information should be gathered and recorded when documenting suspect item incidents:

- OEM
- Date
- Supplier who furnished the item
- Manufacturer of the genuine item
- Part number
- Lot, batch, or serial number
- Type of equipment the item is used to support and/or unique equipment identification number
- Description of the condition
- When the condition was identified (during receiving, installation, after failure)
- What prompted identification (OEM bulletin, operational experience, performance problems, failure)
- Contact name
- Information or source of information that may be used to vet similar suspect items

An example of a generic reporting template is included in Appendix D of this report.

9
INCIDENT DATA SHARING PROTOCOL FOR U.S. LICENSEES

The commercial nuclear industry has long recognized the value of sharing information and for that reason has established venues for collecting and sharing operating experience including information on incidents of suspected CFIs.

From a business perspective, it is not always practical to conduct a conclusive investigation to determine the authenticity of suspected CFIs. Benchmarking conducted during the development of this report indicated such investigations can span years, involve world-wide travel, and are not always conclusive.

From an operational perspective, the primary objective is to ensure suspect items are not introduced to plant systems, structures, and components. Therefore, timely sharing of information on *suspected* CFIs is important. Sharing information on suspect items poses legal challenges and risks. Therefore, such information is typically shared between parties who are bounded by a legal agreement.

Commercial nuclear operators in the U.S. have established protocols for the use of two data sharing tools.

- First, the Institute of Nuclear Power Operation (INPO) has requested all licensees report incidents of CFIs to INPO as operating or construction experience
- Second, EPRI has established a website (scfi.epri.com) that can be used by EPRI members to report and search for incidences of suspected CFIs

9.1 Operating and Construction Experience Reporting

U.S. licensees should be reporting incidents of CFIs to INPO as operating experience. The discovery of counterfeit or fraudulent items installed in plant systems, structures and components has historically been reported as OE.

In February of 2010, INPO requested licensees to report CFIs discovered prior to installation as operating or construction experience. This includes items discovered during receiving as well as items discovered after being accepted into warehouse inventory.

International licensees can and should report counterfeit incidents of CFIs to WANO as construction or operating experience.

9.2 EPRI Suspect Counterfeit and Fraudulent Item Database

In August of 2011, scfi.epri.com became operational and available as an incident data collection and sharing tool for EPRI members. EPRI encourages input from any source. However, access to the database is currently restricted to EPRI members. Vendors and other non-EPRI members may report CFI incidents by contacting the "ask EPRI" number available at epri.com.

Features of scfi.epri.com include

- Provides rapid dissemination of targeted information when a suspect CFI incident has been identified
- Permits inspectors, buyers, and other key staff to quickly and easily search (via web access) for incidents of counterfeit, fraudulent, or substandard items related to the items they are specifying, purchasing, or inspecting
- Leverages existing industry make and model number information to automate notification to licensees that might be impacted by reported incidents that involve equipment they own.
- Leverages existing industry stocked item information to automate notification to licensees that might be impacted by reported incidents that involve items they stock
- Is scalable so that new sources of information can be added as they become available
- Includes provisions for adding photographs and other information that can be used to discriminate between authentic products and CFIs

Scfi.epri.com includes features that permit proactive, targeted notification to licensees that might be impacted by leveraging relationships with two commercially available industry databases. Rolls Royce maintains the Proactive Obsolescence Management System (POMS) which includes plant equipment manufacturer/model number information provided by its subscribers. Curtiss-Wright/Scientech maintains the Rapidly Available Parts Information Database (RAPID) which includes information about items maintained in inventory by its subscribers.

When an incident is entered in EPRI's database, the part/model number information for the suspect item is provided to Rolls Royce and Scientech, a business unit of Curtiss-Wright Flow Control Corporation. These organizations query their databases and provide EPRI with the names of EPRI members that might stock or use the item. EPRI in turn notifies these members that the items are at-risk and provides them with a copy of the incident report.

10
BENCHMARKING SUMMARY

10.1 NEI / EPRI Survey

In February of 2013, NEI requested supplier and utility members to complete an electronic survey that was developed by EPRI based upon EPRI 1021493 [5]. Respondents represented 16 commercial licensees and 4 suppliers to the commercial nuclear industry. The survey results provided input to the development of this guidance document concerning opportunities for the industry to make near term improvements in several areas identified below.

10.1.1 Training

- Ensure management is aware of the threat posed by CFI.
- Provide CFI training to personnel involved in:
  - Contracts
  - Engineering
  - Maintenance
  - Manufacturing and Assembly
  - Procurement Engineering
  - Purchasing
  - Quality Assurance
  - Receiving and Source Inspection
  - Follow guidance included in NRC Generic Letters 89-02 [7], 89-70 [8], and EPRI NP-6629 [13]

10.1.2 Operating Experience

- Obtain access to commercial databases that include information on CFI incidents that pertain to your equipment or products
- Report to industry operating experience databases such as scfi.epri.com
  - Incorporate the practice of reporting incidents into documented procedures and processes

10.1.3 Processing Customer Returns

- Suppliers should inspect and screen items returned from customers to ensure they are authentic

10.1.4 Programs and Processes

- CFI Incident Response
  - Enter CFI incidents in the corrective action system
  - Collection of pertinent data
  - Retain packaging for use in the investigation
  - Notify customers as appropriate
  - Report to authorities
  - Screen for reporting in accordance with 10CFR21 [41]
- Define “at-risk” procurement
  - Identify criteria for identifying at-risk procurements (for example cost, lead-time, source, type of items, origin, and so forth)
  - Identify the types of enhanced testing and inspection that may be appropriate for at-risk procurements
  - Flag “at-risk” procurements in the information system
- Purchasing
  - Source from OEM/OCM or OEM/OCM authorized distributors
  - Maintain lists of approved suppliers
  - As applicable, maintain lists of entities that should not be used as suppliers
  - Do not purchase from unknown suppliers or dubious sources
  - If it is necessary to purchase from a new, unknown, or dubious source, identify the procurement as “at-risk”
- Institute appropriate controls when intellectual property is transmitted to entities other than the owner of the intellectual property (for example, use nondisclosure agreements)
- Identify and evaluate non-identical replacements for obsolete items
- Receiving Inspection
  - Follow guidance included in EPRI NP-6629 [13] and NRC Generic Letters 89-02 [7] and 89-70 [8]

10.2 Other Benchmarking

During the research and investigation for this report, the TAG benchmarked programs and anti-counterfeiting techniques used by the U.S. DOE, industry organizations such as the Aerospace Industries Association (AIA) and the National Electrical Manufacturers Association (NEMA) Underwriters Laboratories (UL) and suppliers who aggressively combat counterfeiting such as Square D-Schneider Electric, Eaton Controls, SMT Corporation, and ERAI.

In addition, during development of the original report, the CFI Technical Advisory Group (TAG) held a benchmarking meeting May 19, 2009, at EPRI's offices in Washington, DC. This meeting was followed the next day by a meeting of the TAG to develop guidance for the nuclear industry on reducing the risk associated with CFIs.

Twenty-six individuals attended, who represented:

- Aerospace Industries Association
- Dominion Energy
- Duke Energy
- Energy Solutions/Parallax (EPRI Consultant)
- EPRI
- GE-Hitachi Nuclear Energy
- Nuclear Energy Institute
- Progress Energy
- Southern Nuclear Operating Company
- South Texas Nuclear Operating Company
- Square D-Schneider Electric
- Tennessee Valley Authority
- University of Maryland Center for Advanced Lifecycle Engineering
- U.S. Department of Commerce
- U.S. Department of Energy
- U.S. Nuclear Regulatory Commission
- XCEL Energy

10.2.1 Overview

EPRI arranged this benchmarking meeting to support development of guidance for the nuclear industry on ways that the risk associated with CFIs can be reduced.

10.2.2 Purpose

The purpose of the benchmarking meeting was to gather information on what other agencies or companies have done to address the issue of counterfeit and fraudulent materials and components. Prior to the meeting, a questionnaire was provided that requested the following information on each of the attendees' existing processes:

- Regulations, orders, and other guidance addressing counterfeit materials or parts
- Vehicle used to report discovery of counterfeit items within their supply chain.
- Type of database used to track and share discoveries internally:
  - Are discoveries at suppliers reported to the database?
  - Is access to the database controlled?
  - Is information managed and reviewed for accuracy by a central authority?
- Is information shared externally?
- Actions taken to mitigate or correct issues of CFI

In addition, each agency or company representative was asked to share the single most important challenge or lesson they have learned regarding CFIs. Each representative was also asked to share any other pertinent thoughts or recommendations on this topic.

10.3 Benchmarking Summaries

10.3.1 University of Maryland Center for Advanced Lifecycle Engineering (CALCE)

A representative from CALCE emphasized that recent events provide indication that even when parts are obtained from the original equipment manufacturer (OEM), they may not be "good" parts. He discussed the need for manufacturers to inspect returned items and to ensure that the raw materials they use meet specifications. He discussed the fact that counterfeiters are becoming better at what they do. He also mentioned that there are textbook and legal definitions for terms such as "defective" and that these definitions can be important when discussing these types of issues.

10.3.2 Department of Energy (DOE)

Representatives from the DOE led a presentation on the DOE's Suspect, Counterfeit, and Defective Items (S/C DI) and Occurrence Reporting, and Operating Experience programs. The comprehensive presentation discussed definitions, counterfeiting perspectives, how and why DOE tracks S/C DIs, common indicators of S/C DIs, the DOE Offices of Health, Safety and Security's responsibilities, the process used to track S/C DIs, and criminal sanctions associated with S/C DIs.

The DOE Suspect/Counterfeit Item (S/CI) Program is mandated through DOE Orders. The hierarchy of documents is:

- DOE O 414-1D, Quality Assurance, requires the implementation of the S/CI program [52].
- DOE G 414-1.2B, Quality Assurance Program Guide Enhancements, Section 5, Guidance on Suspect and Counterfeit Items [53]
- DOE Order 232-2, Occurrence Reporting and Processing of Operations Information, identifies the required S/CI reporting thresholds [54].

DOE's Office of Corporate Safety Analysis (HS-30) maintains the Occurrence Reporting and Processing System (ORPS) database of all the reports generated by the agency and their contractors across the entire DOE complex. HS-30 segregates the S/CI reports and creates a Data Collection Sheet (DCS) and posts pertinent reports on the S/CI website for all DOE staff and DOE contractors to view. In addition, HS-30 reviews other databases, such as the Institute of Nuclear Power Operations (INPO) database, for pertinent information and generates additional DCSs that are entered into the DOE S/CI database.

DOE reviews ORPS reports and submits pertinent reports to the Government Industry Data Exchange Program (GIDEP) database to be shared with the participants and sponsors.

Discoveries of S/CIs at suppliers or distributors are not required to be reported into the ORPS database. The program is focused on enhancing the supply chain process to ensure that S/CIs are discovered before being shipped to DOE contractors.

DOE mandates training on S/CIs and initially provided training to all of the DOE sites and contractors on a periodic cycle. The current process sites can develop their own training or hire a recognized expert to provide them with the traditional hands-on training.

It was noted by DOE representatives that there was increased reporting of S/CI discoveries following the initial hands-on and refresher training sessions at nearly every DOE site. The message that DOE wanted to convey was that the level of awareness has increased as well as the number of individuals who are vigilant and more observant of the materials and components around them.

10.3.4 Government-Industry Data Exchange Program (GIDEP)

GIDEP is managed by the U.S. Department of Defense with participation by various U.S. agencies.

GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities, and equipment.

Preliminary discussions with GIDEP officials indicate that nuclear licensees could be provided with access to GIDEP that would permit contributing to and using the information. The NRC does have access to GIDEP.

It is worth mentioning that results from the DOC survey [12] discussed below reported 9356 incidents of CFIs identified by suppliers of electronics to the U.S. government. Less than two dozen of these incidents were reported to GIDEP [55].

10.3.5 Department of Commerce Survey and Best Practices

A representative from the U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation delivered a presentation titled "Counterfeits and the U.S. Industrial Base." The presentation included a comprehensive discussion on the Office of Technology Evaluation's (OTE's) background, as well as definitions and results of a counterfeit electronics study conducted by the OTE that included five related surveys distributed to 498 survey participants including:

- 106 microchip and discrete electronic manufacturers
- 37 electronic printed board producers/assemblers
- 144 electronic parts distributors and brokers
- 147 prime government contractors and subcontractors
- 64 Defense logistics agencies, arsenals, and depots.

The results of the study are enlightening. The study was performed to assess the impact of counterfeit electronics on U.S. supply chain integrity, critical infrastructure, and industrial capabilities and recommend best practices to mitigate risk to U.S. supply chain.

The survey, titled "Counterfeits and the U.S. Industrial Base" [12] was conducted at the request of and sponsored by the Naval Air Systems Command (NAVAIR) with support from the Semiconductor Industry Association (SIA). The final report titled *Defense Industrial Base Assessment: Counterfeit Electronic* [11] was published by the U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation in 2010.

The presentation highlighted the counterfeiting issues confronting the electronics industry and the customers utilizing the materials. Some of the identified industry best practices are covered in the following sections.

10.3.5.1 Original Component Manufacturer (OCM) Best Practices

- Ensure proper disposal of all scrap. Crush all defective/unused products to prevent re-circulation.
- Train all employees on how to identify and handle counterfeit parts.

- Tighten contractual obligations with contract manufacturers regarding the disposal of unused product.

10.3.5.2 Circuit Board Assembler Best Practices

- Audit OCMs/OEMs to ensure that the purchased part is made within their facility and not contracted out.
- Perform destructive testing if a part cannot be verified by other means.
- Establish qualifications for supplier purchases.

10.3.5.3 Authorized Distributor Best Practices

- Ask for Certificates of Compliance for all products purchased.
- Educate the sales team regarding the risk of parts brokers.
- Create a central database for identifying counterfeit suppliers.
- Do not approve returns in greater quantities than the original purchase.

10.3.5.4 Independent Distributors/Broker Best Practices:

- Always purchase parts via escrow payments. Suppliers that believe in their product will not mind waiting for their money.
- Audit all inventory purchased before anti-counterfeiting measures were put in place.
- Follow the guidance contained in the Independent Distributors of Electronics Association standard for inspecting electronic components, IDEA-STD-1010-A [56], when performing incoming inspections.
- Use authentic pictures to visually verify parts.

10.3.5.5 Sub-Contractor Best Practices

- Share all information on discovered counterfeit parts with industry and authorities.
- Incorporate language into supplier contracts to minimize liabilities and impose penalties for counterfeits.
- Plan for and attempt to design out obsolescence from systems.
- Create annual training sessions for staff to keep counterfeit detection up to date.

10.3.5.6 DOD Organization Best Practices

- Train personnel on how to identify and intercept counterfeit parts.
- Eliminate the requirement to purchase from the lowest bidder, and encourage purchasing based on best value.

- Implement internal testing/screening procedures for counterfeits.

10.3.6 Schneider Electric – Square D

A representative from Square D's North American Operating Division, (a brand of Schneider Electric) discussed the issues that Square D has encountered over the past few years with counterfeit products. The representative indicated that CFIs are a multimillion-dollar problem. Not only is there a loss of dollars for manufacturers, electrical contractors, and distributors, but there is a loss of image as well. More important than either of those is the injury or loss of life when a knockoff product causes a fire or electrocutes a homeowner."

Schneider Electric, Square D takes counterfeiting of their products seriously and intends to pursue every means possible to stop this illegal activity and to make the industry and public more aware of this critical safety concern. The company has an anti-counterfeiting organization within Schneider Electric that is committed to eradicating counterfeits from the marketplace by:

- Suing U.S. companies selling counterfeits
- Reporting counterfeit sellers to the Consumer Product Safety Commission (CPSC)
- Engaging U.S. authorities to prevent counterfeit imports and criminally pursue offenders
- Working with foreign agencies and governments to shut down counterfeit manufacturers
- Informing concerned parties about counterfeit products
- Rallying with industry to fight counterfeiting

Because counterfeit products can also enter the supply chain through the return of materials or components to the distributor, distributors need to closely monitor and tighten controls on the return of materials back into their inventories from customers. Square D audits their authorized distributors on this process to ensure that the supply chain remains uncontaminated. Through this continuous audit process by Square D, the company can recommend that the best way to avoid counterfeit products is to buy only from authorized distributors.

11
REFERENCES

1. U.S. CBP Publication 0172-0113, Intellectual Property Rights Fiscal Year 2012 Seizure Statistics, U.S. Customs and Border Protection Office of International Trade, US. Department of Homeland Security, Washington, DC: 2013
2. U.S. Code of Federal Regulations, Title 10, Chapter 1, Appendix B to Part 50, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Washington, DC: August 2007.
3. U.S. NRC *Staff Review of Counterfeit, Fraudulent, and Suspect Items*, ADAMS Acquisition number ML1121130293, United States Nuclear Regulatory Commission, Washington, DC: 2011.ICE, CBP increase seizure totals of counterfeit and pirated goods in 2008, U.S. Immigration and Customs Enforcement website, January 8, 2009, http://www.ice.gov/pi/nr/0901/090108washington.htm.
4. U.S. NRC SECY-11-0154, "*An Agency-wide Approach to Counterfeit, Fraudulent and Suspect Items,*" ADAMS acquisition number ML112200150, United States Nuclear Regulatory Commission, Washington, DC: 2011.
5. *Counterfeit and Fraudulent Items: A Self-Assessment Checklist*, EPRI, Palo Alto, CA: October, 2010. 1021493.
6. U.S. NRC Information Notice 2008-04, "Counterfeit Parts Supplied to Nuclear Power Plants," United States Nuclear Regulatory Commission, Washington, DC: 2008.
7. U.S. NRC Generic Letter 89-02, "Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products" (Agencywide Reports Access and Management System (ADAMS) Accession No. ML031140060), United States Nuclear Regulatory Commission, Washington, DC: March 1989.
8. U.S. NRC Information Notice No. 89-70, "Possible Indications of Misrepresented Vendor Products," United States Nuclear Regulatory Commission, Washington, DC: October 1989.
9. 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.
10. 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.
11. *Defense Industrial Base Assessment: Counterfeit Electronics*, U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation, Washington, DC: 2010.
12. "Counterfeits and the U.S. Industrial Base," presented at Electric Power Research Institute (EPRI) CFSI Benchmarking Meeting by Mark H. Crawford, Senior Trade & Industry

Analyst, U.S. Department of Commerce Bureau of Industry & Security, Office of Technology Evaluation, May 19, 2009.

13. *Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants*. NP-6629, EPRI, Palo Alto, CA: May, 1990.
14. "Managing Suspect and Counterfeit Items in the Nuclear Industry," IAEA-TECDOC-1169, International Atomic Energy Agency, Vienna, Austria: August 2000.
15. *Scottsdale Man Pleads Guilty to False Statements Related to Nuclear Reactor Equipment Repair,* U.S. Department of Justice Press Release, U.S. Department of Justice, Washington, DC. December 5, 2012
16. *Massachusetts Man Charged with Selling Counterfeit Semiconductors for Use on Nuclear Submarines,* U.S. Department of Justice Press Release, U.S. Department of Justice, Washington, DC. July 15, 2013.
17. "Audit Report on the Procurement of Safety Class/Safety-Significant Items at the Savannah River Site," DOE/IG-0814, U.S. Department of Energy, Washington, DC: April 2009.
18. U.S. Code of Federal Regulations, Title 10, Chapter 1, Part 50, Deliberate Misconduct, Washington, DC: 1998.
19. U.S. NRC Secretary Letter (SECY) 89-010, Advance Notice of Proposed Rulemaking (ANPR), "Acceptance of Products Purchased for Use in Nuclear Power Plant Structures, Systems, and Components," United States Nuclear Regulatory Commission, Washington, DC: March, 1989
20. *Guidelines for Preparing Specifications for Nuclear Power Plants*. EPRI, Palo Alto, CA: April 1988. NP-5638
21. *Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications*. EPRI, Palo Alto, CA: June, 1988. NP-5652
22. *Guidelines for the Technical Evaluation of Replacement Items in Nuclear Power Plants*. EPRI, Palo Alto, CA: December, 1989. NP-6406.
23. NUMARC 90-13, "Nuclear Program Improvements," Nuclear Management and Resources Council, Incorporated, October 1990.
24. Public Law 101-592, Fastener Quality Act, 104STAT. 2493, 101st Congress, Washington, DC: 1990.
25. Policy Letter 91-3, "Reporting Nonconforming Products," U.S. Office of Management and Budget, Washington, DC: 1991.
26. Code of Federal Regulations, Title 15, Part 280, Fastener Quality, Washington, DC: 2007.
27. Federal Acquisition Circular (FAC) 90-9. Washington, DC: 1992.
28. Guideline for Preparation of Material/Equipment Descriptions, GG-MATL-01, Revision 0, Washington, DC: 1992.
29. Department of Energy Quality Alert, "Suspect/Counterfeit Parts Headmark List" in the *Environment, Safety & Health Bulletin,* DOE/EH-0266, Issue No. 92-4, U.S. Department of Energy, Washington, DC: August 1992.

30. Public Law Number 112-81 Section 818 (introduced as Amendment No. 1092 to S. 1867, 112the Congress, First Session). Report 112-329, National Defense Authorization Act, National Defense Authorization Act for Fiscal Year 2012, Conference Report to accompany House Rule 1540, December 12, 2011.

31. Speech S-07-038, "The NRC and the Safety Business," Remarks Prepared for NRC Chairman Dale E. Klein, U.S. NRC, Presented at the American Nuclear Society Utility Working Conference, Amelia Island in August 2007, Washington, DC: 2007.

32. *Plant Support Engineering: Counterfeit, Fraudulent, and Substandard Items: Mitigating the Increasing Risk.* 1019163, EPRI, Palo Alto, CA: October, 2009.

33. *Counterfeit, Fraudulent, and Substandard Items: computer-based training*. 1020955, EPRI, Palo Alto, CA: October 2009.

34. *South Korean Nuclear Operator Raided in Cable Probe*, Associated Press, The Asahi Shimbun, Japan: June 2013

35. Scandal in South Korea Over Nuclear Revelations, New York Times, New York, NY: August 4, 2013.

36. U.S. NRC IN 2013-02, "Issues Potentially Affecting Nuclear Fire Safety, ADAMS acquisition number ML122840031, United States Nuclear Regulatory Commission, Washington, DC: 2013.

37. Consumer Product Safety Commission Release #07-036, "Scott Electric Co. Inc. Recalls Counterfeit Circuit Breakers Due to Fire Hazard," U.S. Consumer Product Safety Commission, Washington, DC:2006.

38. Consumer Product Safety Commission Release #08-FINAL, "Connecticut Electric Recalls Counterfeit Square D Circuit Breakers Due to Fire Hazard," U.S. Consumer Product Safety Commission, Washington, DC:2007.

39. Consumer Product Safety Commission Release #08-151, "North American Breaker Co. Recalls Counterfeit Circuit Breakers Due to Fire Hazard," U.S. Consumer Product Safety Commission, Washington, DC:2007.

40. U.S. NRC 10CFR Part 21 Report 2006-23-00, "Flowserve, Incorrect Identification of the Material Used to Manufacture Y-Globe Valve," Adams Access Number ML063120160, Washington, DC: 2006.

41. U.S. Code of Federal Regulations, Title 10, Chapter 1, Part 21, Reporting of Defects and Noncompliance, Washington, DC: 1992.

42. Shell Canada Upgrader, Scotford Upgrader - Expansion 1: ES&H Alert #001, April 23, 2009, Lifting Lug on Flowserve Pump Skids.

43. Asian Inspection Community, Oil and Gas Engineers Knowledge Platform, P91 Pipe Failure in China Power Facility, posted January 28, 2007.

44. Contaminated Imports: Finds of Radioactive Steel on the Rise in Germany, *Spiegel Online International,* Christian Schwagerl, February 16, 2009, http://www.spiegel.de/international/world/0,1518,607840,00.html

45. Lessons Learned CWI-ICP-2009-001, Department of Energy Office of Health, Safety, and Security, Washington, DC: 2008.

46. "Certification Fraud: A Serious Problem for Everyone," Peter Howe, Managing Director, Technical Operations, AWS Certification Dept., *Inspection Trends*, American Welding Society, Miami, FL, January 2009.

47. In the United States District Court for the Eastern District Of Pennsylvania, United States Versus Barbara McCoy, Violations: " 18 U.S.C. § 1001(a)(2) (false statements – four counts), 18 U.S.C. § 2 (aiding and abetting) , June 28, 2001.

48. "Authentication Technologies for Brand Protection," National Electrical Manufacturers Association (NEMA), Rosslyn, VA: 2009.

49. Response to Growing Threat, U.S. Immigration and Customs Enforcement National Intellectual Property Rights Coordination Center website, Washington, DC: July 2008, http://www.ice.gov.pi/ipctr/.

50. *Guideline for Sampling in the Commercial-Grade Item Acceptance Process,* EPRI, Palo Alto, CA: 1999. TR-017218-R1.

51. U.S. NRC IN 2012-22, "Counterfeit, Fraudulent and Suspect Item Training Offerings," ADAMS acquisition numbers ML12137A248 and ML12318A26, United States Nuclear Regulatory Commission, Washington, DC: 2013.

52. Quality Assurance, DOE Order O 414.1-D, U.S. Department of Energy, Washington, DC: 2007.

53. DOE G 414-1.2B, Quality Assurance Program Guide Enhancements, Section 5, Guidance on Suspect and Counterfeit Items, Department of Energy, Washington, DC: August 16, 2011.

54. DOE M 232-2, Occurrence Reporting and Processing of Operations Information, U.S. Department of Energy, Washington, DC: August 19, 2003.

55. Impact of Counterfeit Components and DOD's Actions (Presented to GIDEP Management Council), Naval Air Systems, Washington, DC: July 2009.

56. "Acceptability of Electronic Components Distributed in the Open Market," IDEA-STD-1010-A, Independent Distributors of Electronics Association, Buena Park, CA: 2006.

57. "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition." SAE AS-5553A, Society of Automotive Engineers, Warrendale, PA: 2013.

58. DOE G 414.1-3, Suspect/Counterfeit Items Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance, U.S. Department of Energy, Washington, DC: November 2004.

59. *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition – Distributors*," SAE AS-6081, Society of Automotive Engineers, Warrendale, PA: 2012.

60. *Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel*, SAE AS6174, Society of Automotive Engineers, Warrendale, PA: 2012.

61. *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*, ARP6178, Society of Automotive Engineers, Warrendale, PA: 2011.

62. "Counterfeit Parts," *Environment, Safety & Health Bulletin*, DOE/EH-0266, Issue No. 92-4, U.S. Department of Energy, Washington, DC; August 1992.

63. *Acceptability of Electronic Components Distributed in the Open Market*, IDEA-STD-1010-B, Independent Distributors of Electronics Association, Buena Park, CA: 2006.

64. *Process management for avionics - Counterfeit prevention - Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components,* IEC/TS 62668-1 Ed 1.0, International Electrotechnical Commission, Geneva, Switzerland: 2012.

A
REGULATORY GUIDANCE AND INDUSTRY NOTIFICATIONS

Regulatory Guidance and Notifications	
1983 March	U.S. NRC Information Notice No. 83-07, “Nonconformities with Materials Supplied By Tube Line Corporation”
1983 July	U.S. NRC IE Bulletin No. 83-06, “Nonconforming Materials Supplied by Tube-Line Corporation Facilities at Long Island City, New York; Houston, Texas; and Carol Stream, Illinois”
1983 November	U.S. NRC Information Notice No. 83-79, “Apparently Improper Use of Commercial Grade Components in Safety-Related Systems”
1984 June	U.S. NRC Information Notice No. 84-52, “Inadequate Material Procurement Controls on the Part of Licensees and Vendors”
1985 May	U.S. NRC Information Notice No. 84-52, “Supplement 1: Inadequate Material Procurement Controls on the Part of Licensees and Vendors”
1985 December	U.S. NRC Information Notice No. 85-101, “Applicability of 10 CFR 21 to Consulting Firms Providing Training”
1986 March	U.S. NRC Information Notice 86-21,“Recognition of American Society of Mechanical Engineers Accreditation Program for N Stamp Holders” (Also see Supplements 1 and 2, 04/16/91)
1987 November	U.S. NRC Compliance Bulletin No. 87-02, “Fastener Testing to Determine Conformance with Applicable Material Specifications”
1987 December	U.S. NRC Information Notice No. 87-66, “Inappropriate Application of Commercial-Grade Components”
1988 April	U.S. NRC Information Notice No. 88-19, “Questionable Certification of Class 1E Components”
1988 May	U.S. NRC Bulletin No. 88-05, “Nonconforming Materials Supplied by Piping Supplies, Inc. at Folsom, New Jersey And West Jersey Manufacturing Company At Williamstown, New Jersey”
1988 November	U.S. NRC Bulletin No. 88-10, “Nonconforming Molded-Case Circuit Breakers”
1988 December	U.S. NRC Information Notice No. 88-95, “Inadequate Procurement Requirements Imposed by Licensees on Vendors”
1988 June	U.S. NRC Information Notice No. 88-35, “Inadequate Licensee Performed Vendor Audits “

Regulatory Guidance and Notifications	
1988 July	U.S. NRC Information Notice No. 88-46, “Licensee Report of Defective Refurbished Circuit Breakers”
1988 July	U.S. NRC Information Notice No. 88-48, “Licensee Report of Defective Refurbished Valves”
1989 April	U.S. NRC Information Notice No. 88-97, “Supplement 1: Potentially Substandard Valve Replacement Parts”
1989 March	U.S. NRC Generic Letter 89-02, “Actions to Improve the Detection of Counterfeit and Fraudulently Marketed Products”
1989 March	U.S. NRC SECY 89-010, Advance Notice of Proposed Rulemaking (ANPR), “Acceptance of Products Purchased for Use in Nuclear Power Plant Structures, Systems, and Components
1989 January	U.S. NRC Information Notice No. 89-03, “Potential Electrical Equipment Problems”
1989 April	U.S. NRC Information Notice No. 89-39, “List of Parties Excluded from Federal Procurement or Non-Procurement Programs”
1989 May	U.S. NRC Generic Letter 89-09, “ASME Section III Component Replacements”
1989 May	U.S. NRC Information Notice No. 89-45, “Metalclad, Low-Voltage Power Circuit Breakers Refurbished with Substandard Parts”
1989 July	U.S. NRC Information Notice No. 89-56, “Questionable Certification of Material Supplied to the Defense Department by Nuclear Suppliers”
1989 August	U.S. NRC Bulletin No. 88-10, “Supplement 1: Nonconforming Molded-Case Circuit Breakers”
1989 August	U.S. NRC Information Notice No. 89-59, “Suppliers of Potentially Misrepresented Fasteners”
1989 October	U.S. NRC Information Notice No. 89-70, “Possible Indications of Misrepresented Vendor Products”
1990 July	U.S. NRC Information Notice No. 90-46, “Criminal Prosecution of Wrongdoing Committed by Suppliers of Molded-case Circuit Breakers and Related Components”
1990 September	U.S. NRC Information Notice No. 90-57, “Substandard, Refurbished Potter & Brumfield Relays Misrepresented As New”
1990 September	U.S. NRC Information Notice No. 90-60, “Availability of Failure Data in the Government-Industry Data Exchange Program”
1992 July	U.S. NRC Information Notice 92-51, “Misapplication and Inadequate Testing of Molded-Case Circuit Breakers”
1992 August	U.S. NRC Information Notice 92-56, “Counterfeit Valves in the Commercial Grade Supply System”
1992 September	U.S. NRC Information Notice 92-68, “Potentially Substandard Slip-On, Welding Neck, and Blind Flanges”
1993 June	U.S. NRC Information Notice 93-42, “Failure of Anti-Rotation Keys in Motor-Operated Valves Manufactured by Velan“

Regulatory Guidance and Notifications	
1993 June	U.S. Information Notice 93-43, "Use of Inappropriate Lubrication Oils in Safety Related Applications"
1993 September	U.S. NRC Information Notice 93-73, "Criminal Prosecution of Nuclear Suppliers for Wrongdoing"
1994 July	U.S. NRC Information Notice 94-50, "Failure of General Electric Contactors to Pull In at the Required Voltage"
1994 December	U.S. NRC Information Notice 94-86, "Legal Actions Against Thermal Science, Inc., Manufacturer of Thermo-Lag"
1995 February	U.S. NRC Information Notice 95-12, "Potentially Nonconforming Fasteners supplied by A&G Engineering II, Inc."
1996 February	U.S. NRC Part 21 Notice 1996-06-04, Substandard Capscrews Provided by Cardinal to Aerofin
1995 October	U.S. NRC Part 21 Notice 1995-212, Substandard Capscrews Provided by Cardinal to Aerofin
1996 July	U.S. NRC Information Notice 96-40, "Deficiencies in Material Dedication and Procurement Practices and in Audits of Vendors"
1997 January	U.S. NRC Part 21 Notice 1997-06-0 through 3, Counterfeit Worm Shaft Gear in Limitorque Actuator from Surplus Market
2007 May	U.S. NRC Information Notice 2007-19, "Fire Protection Equipment Recalls and Counterfeit Notices"
2007 December	U.S. NRC Letter to ACLASS, Accreditation Services
2007 December	U.S. NRC Information Notice 2007-40, "Inadequate Implementation of 10 CFR Part 21 Requirements by Vendors Who Supply Basic Components to Nuclear Power Plant Licensees"
2008 April	U.S. NRC Information Notice 2008-04, "Counterfeit Parts Supplied to Nuclear Power Plants"
2011 October	U.S. NRC SECY-11-0154, "*An Agency-wide Approach to Counterfeit, Fraudulent and Suspect Items,*" ADAMS acquisition number ML112200150
2011 November	U.S. NRC *Staff Review of Counterfeit, Fraudulent, and Suspect Items*, ADAMS Acquisition number ML1121130293
2013 January	U.S. NRC IN 2012-12, "Counterfeit, Fraudulent and Suspect Item Training Offerings"
2011 October	NEA/CNRA/R(2011)9, "*Operating Experience Report: Counterfeit, Suspect and Fraudulent Items,*" Organization of Economic Cooperation and Development Nuclear Energy Agency
2013 February	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.

B
STANDARD CFI PROCUREMENT CLAUSES

B.1 Standard Procurement Clauses

The following clauses can be used to communicate requirements concerning CFIs to suppliers. A generic clause was developed for use by commercial nuclear facilities during the execution of this research. This appendix also contains standard clauses and language mandated for use or used voluntarily by other industries.

B.1.1 Generic Clause for Commercial Nuclear Power Plants

The following clause can be used as written or used as a starting point in the development of a similar clause designed to be included in licensee and supplier procurement documents to communicate expectations regarding and the potential consequences of providing counterfeit items. The clause can be applied to all orders, regardless of quality classification, types of items being procured, or cost of items being procured.

It is highly recommended that any clause that addresses this issue be reviewed by the purchaser's general counsel prior to use.

B.1.1.1 Delivery of Suspect/Counterfeit Items

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

If suspect/counterfeit items are furnished under this order or are found in any of the goods delivered hereunder, such items will be dispositioned by (Utility Name) and / or the original manufacturer, and may be returned to the Seller in accordance with the warranty provisions applicable to the Order. The Seller shall promptly replace such suspect/counterfeit items with

items meeting the requirements of the Order. In the event the Seller knowingly supplied suspect/counterfeit items, the Seller shall be liable for reasonable costs incurred by the Purchaser for the removal, replacement and reinstallation of said goods in accordance with the warranty provisions applicable to the Order.

B.1.2 Other Industry Examples

B.1.2.1 Aerospace Industry

The aerospace industry and NAVAIR are currently implementing the guidance contained in SAE AS-5553A, a 2013 update of SAE AS-5553 [57]. This standard titled "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" includes several standard clauses that address confiscating products and financial responsibility, detection of counterfeit parts, documentation, and traceability.

B.1.2.2 Department of Energy

The following clause can be found in DOE G 414.1-3 [58]:

> Notwithstanding any other provisions of this agreement, the Subcontractor warrants that all items provided to the Contractor shall be genuine, new and unused unless otherwise specified in writing by the Contractor. Subcontractor further warrants that all items used by the Subcontractor during the performance of work at the [name DOE site here], include all genuine, original, and new components, or are otherwise suitable for the intended purpose. Furthermore, the Subcontractor shall indemnify the Contractor, its agents, and third parties for any financial loss, injury, or property damage resulting directly or indirectly from material, components, or parts that are not genuine, original, and unused, or not otherwise suitable for the intended purpose. This includes, but is not limited to, materials that are defective, suspect, or counterfeit; materials that have been provided under false pretenses; and materials or items that are materially altered, damaged, deteriorated, degraded, or result in product failure.
>
> Types of material, parts, and components known to have been misrepresented include (but are not limited to) fasteners; hoisting, rigging, and lifting equipment; cranes; hoists; valves; pipe and fittings; electrical equipment and devices; plate, bar, shapes, channel members, and other DOE G 414.1-3 11, November 3, 2004, heat treated materials and structural items; welding rod and electrodes; and computer memory modules. The Subcontractor's warranty also extends to labels and/or trademarks or logos affixed, or designed to be affixed, to items supplied or delivered to the Contractor. In addition, because falsification of information or documentation may constitute criminal conduct, the Contractor may reject and retain such information or items, at no cost, and identify, segregate, and report such information or activities to the appropriate Department of Energy officials.

B.1.2.3 Other Examples of Clauses Addressing Counterfeit and Fraudulent Items

Materials and items furnished by the Seller to (Customer Name) under this Agreement shall not include suspect, counterfeit, fraudulent parts, nor shall such parts be used in performing any work under this Agreement, whether on or off the (Customer Name) site.

A suspect item is one in which there is an indication by visual inspection, testing, or other information that it may not conform to established Government or industry-accepted specifications or national consensus standards. A counterfeit item is suspect item that is a copy or substitute without legal right or authority or one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer. Such items may be labeled to represent a different class of parts, or used and/or refurbished parts, complete with false labeling, that are represented as new parts.

Suspect counterfeit items do not include non-conforming items resulting from inadequate design or production quality control. Such items shall be handled in accordance with Buyers nonconforming item procedures.

If suspect, counterfeit, fraudulent parts are furnished under this Agreement and are found on the (Customer Name) site, such items shall be impounded by (Customer Name). The Seller shall promptly replace such items with items acceptable to the (Customer Name), and the Seller shall be liable for all costs relating to impoundment, removal, and replacement. (Customer Name) may turn such items over to the law enforcement authorities, i.e., U. S. Office of the Inspector General, for investigation and reserves the right withhold payment for the suspect items pending the results of the investigation.

The rights of (Customer Name) in this clause are in addition to any other rights provided by law or under this Agreement.

- The Seller is hereby notified that the delivery of suspect/counterfeit parts is of special concern to (Utility). If any parts covered by this Order are described using a manufacturer part number or using a product description and/or specified using an industry standard, the Seller shall be responsible to ensure that the replacement parts supplied by the Seller meet all requirements of the latest version of the applicable manufacturer data sheet, description, and/or industry standard. If the Seller is not the manufacturer of the goods, the Seller shall make all reasonable efforts to ensure that the replacement parts supplied under this Order are made by the Original Equipment Manufacturer (OEM) and meet the applicable manufacturer data sheet or industry standard. Should the Seller desire to supply a replacement part that may not meet the requirements of this paragraph, the Seller shall notify the Purchaser of any exceptions and receive the Purchaser's written approval prior to shipment of the replacement parts to the Purchaser. If suspect/counterfeit parts are furnished under this order or are found in any of the goods delivered hereunder, such items will be dispositioned by (Utility) and/or the supplier and may be returned to the Seller. The Seller shall promptly replace such suspect/counterfeit parts with parts acceptable to (Utility), and the Seller shall be liable for all costs, including but not limited to (Utility)'s internal and external costs, relating to the removal and replacement of said parts.

- **Accountability/Liability:** "If suspect/counterfeit parts are furnished under this agreement and are found on the (Nuclear Licensee's) Premises, such items shall be impounded by (Nuclear Licensee). The Seller shall promptly replace such items with items acceptable to the (Nuclear Licensee), and the Seller shall be liable for all costs relating to impoundment, removal, and replacement. (Nuclear Licensee) may turn such items over to (U.S. Office of Inspector General, FBI, etc.) for investigation and reserves the right withhold payment for the suspect items pending the results of the investigation."
- **Suspect/Counterfeit Parts:** "Suspect/counterfeit parts" are parts that may be of new manufacture, but are labeled to represent a different class of parts, or parts that are used and/or refurbished, complete with false labeling, but are represented as new parts. Three categories of suspect/counterfeit parts exist:
  - Fasteners, including bolts and nuts, made of carbon steel (designated as Grade 5 or Grade 8) or stainless steel, with headmarks or stamps shown on the headmark list that was prepared by the United States Customs Service
  - Piping valves and flanges bearing labels of ASME or that falsely indicate that the items meet recognized ASTM consensus standards
  - Used or refurbished molded-case electrical circuit breakers or similar type switch gear

  Supplies furnished to (Customer Name) under this Agreement shall not include suspect/counterfeit parts nor shall such parts be used in performing any work under this Agreement, whether on or off the (Customer Name) site.

  If suspect/counterfeit parts are furnished under this Agreement and are found on the (Customer Name) site, such parts shall be impounded by (Customer Name), or they shall be removed by the Seller as directed by (Customer Name). The Seller shall promptly replace such parts with supplies acceptable to (Customer Name), and the Seller shall be liable for all costs relating to impoundment, removal, and replacement.

  The rights of (Customer Name) in this clause are in addition to any other rights provided by law or under this Agreement.

C
EXISTING SOURCES OF INFORMATION

This appendix provides a listing of information available on the subject of CFIs. Included are existing guidance documents and standards, regulations, and databases, as well as enforcement agencies and websites containing pertinent information.

C.1 Guidance Documents and Standards

C.1.1 Aerospace Industry

SAE AS-6081 "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition - Distributors" [59] is an aerospace standard that identifies practices to:

- Identify reliable sources of electronic parts
- Assess and mitigate risk of distributing fraudulent parts
- Control suspect parts
- Report suspect and confirmed parts to potential users and authorities

SAE AS 5553A, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," [57] is an aerospace standard that has been adopted by NASA. At the time of publishing, it is being considered for adoption by the Department of Defense. The standard is maintained by the Society of Automotive Engineers (SAE).

SAE AS6174, "Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel," [60] discusses practices to maximize availability of authentic materiel (made from the proper materials using the proper processes with required testing,), procure materiel from reliable sources, assure authenticity and conformance of procured materiel, control materiel identified as counterfeit, and report counterfeit materiel to other potential users and government investigative authorities

ARP6178: Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors [61]. This SAE Aerospace Recommended Practice is applicable to organizations that procure electronic components from sources other than the original component manufacturer and provides insight regarding assessment of distributors that sell electronic components without contractual authorization from the original component manufacturer.

Draft Aerospace Industry Standards

Draft AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition –Counterfeit Electronic Parts; Avoidance Protocol, Distributors. This standard will discuss practices to identify reliable sources to procure parts, assess and mitigate risk of distributing fraudulent/counterfeit parts, control suspect or confirmed fraudulent/counterfeit parts, and report suspect and confirmed fraudulent/counterfeit parts to other potential users and appropriate authorities.

Draft AS6301, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Verification Criteria. This document will include criteria to be used by accredited certification bodies to determine compliance and grant certification to AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors.

Draft AIR6273, Terms and Definitions - Fraudulent/Counterfeit Electronic Parts. This document will be used and cited as a standard reference by other SAE G-19 Committee documents that address the mitigation of Fraudulent/Counterfeit Electronic Parts.

Draft AS6171, Test Methods Standard; Counterfeit Electronic Parts. This document will address practices to detect suspect counterfeit electronic parts, to maximize the use of authentic parts, and to ensure consistency across the supply-chain for test techniques and requirements.

Draft AS6496, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution. This document will identify the requirements for mitigating counterfeit products in the authorized distribution supply chain by authorized distributors.

C.1.2 DOE

"Counterfeit Parts," in *Environment, Safety & Health Bulletin,* DOE/EH-0266, Issue 92-4 issued in August 1992 [62]

"Suspect/Counterfeit Parts Headmark List" in the *Environment, Safety & Health Bulletin*, DOE/EH-0266, Issue No. 92-4, August 1992, (DOE Quality Alert) [21]

DOE G 414.1-3 "Suspect/Counterfeit Items Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements [29]

C.1.3 EPRI

EPRI NP-6629, *Guidelines for the Procurement and Receipt of Items for Nuclear Power Plants,* (Appendix C), May 1990 [13]

C.1.4 IAEA

IAEA-TECDOC-1169, "Managing Suspect and Counterfeit Items in the Nuclear Industry," International Atomic Energy Agency, Vienna, August 2000 [14]

C.1.5 IDEA

IDEA-STD-1010-A "Inspection Standard for Detecting Counterfeit Components" [56]

IDEA-STD-1010-B "Acceptability of Electronic Components Distributed in the Open Market" [63]

C.1.5 IEC

IEC/TS 62668-1 Ed 1.0: Process management for avionics - Counterfeit prevention - Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components [64]. This document identifies requirements for avoiding the use of counterfeit, recycled and fraudulent components used in critical industry applications.

Draft IEC/TS 62668-2 Ed. 1.0: Process management for avionics - Counterfeit prevention - Part 2: Managing electronic components from non-franchised sources.

C.1.6 ISO

Draft ISO 16678: Anti-counterfeiting tack and trace method using unique identifier numbering is currently in development.

C.1.7 NAVAIR

NAVAIR has adopted the Independent Distributors of Electronics Association standard IDEA-STD-1010-A, "Acceptability of Electronic Components Distributed in the Open Market" [56]. Technicians who inspect incoming electronics are trained in the standard and must pass an assessment afterward.

C.1.8 NEMA

The NEMA white paper titled "Authentication Technologies for Brand Protection" [48] provides information on positive identification of authentic items.

C.1.9 NRC

U.S. NRC Information Notice No. 89-70, "Possible Indications of Misrepresented Vendor Products," United States Nuclear Regulatory Commission, October 1989 [8].

C.2 Regulations

C.2.1 Policy Letter 91-3, Reporting Nonconforming Products

Policy Letter 91-3, "Reporting Nonconforming Products" [25] establishes policies and procedures for using a government-wide system for exchanging information among agencies about nonconforming products and defines GIDEP (operated by the DOD) as the central database for receiving and disseminating information.

At the time of publishing of this document, GIDEP is reviewing a draft circular. The draft circular is intended to supersede Policy Letter 91-3 and will require all government agencies responsible for regulating industry to require each industry to report all nonconforming products and obsolescence issues to GIDEP.

C.2.2 The Fastener Quality Act of 1990

The Fastener Quality Act of 1990 [24] requires that fasteners conform to the consensus standards and specifications to which they are represented to be manufactured, for example, ASTM Grade 5 fasteners. It also provides requirements for the accreditation of laboratories engaged in fastener testing and requires inspection, testing, and certification of fasteners used in critical applications.

C.2.3 DOE G 414.1-3, Suspect/Counterfeit Items Guide, for Use with 10 CFR Part 830 Subpart A, Quality Assurance Requirements and DOE O 414.1C, Quality Assurance

DOE has mandated the use of the Suspect/Counterfeit Item Guide [58] across the DOE Complex.

C.2.4 Anti-Counterfeiting Consumer Protection Act of 1996

On July 2, 1996, the Anti-Counterfeiting Consumer Protection Act of 1996 [67] was signed into law in response to increased involvement of organized crime in counterfeiting activities, as well as the effects of counterfeiting on U.S. businesses, consumers, and the economy.

C.2.5 Section 818, Detection and Avoidance of Counterfeit Electronic Parts

Public Law Number 112-81 Section 818 (introduced as Amendment No. 1092 to S. 1867, 112th Congress, First Session). Report 112-329, National Defense Authorization Act, National Defense Authorization Act for Fiscal Year 2012. This law includes measures to prevent CFIs from entering the defense supply chain.

C.3 Manufacturers and Industry Associations

C.3.1 Amidyne Group

This website maintained by the Amidyne Group includes a synopsis of current events related to counterfeiting.

C.3.2 Authorized Service Directory (ASD)

This website provides a listing of authorized distributors for electronics and is a joint effort involving the Semiconductor Industry Association and Rochester Electronics.

C.3.3 International Anti-Counterfeiting Coalition (IACC)

This not-for-profit organization is based in Washington, DC, and is devoted solely to combating product counterfeiting and piracy.

C.3.4 Canadian Anti-Counterfeiting Network (CACN)

This is a coalition of individuals, companies, firms, and associations that have joined together in the fight against product counterfeiting and copyright piracy in Canada and around the world.

C.3.5 Consumer Product Safety Commission (CPSC)

This website is maintained by CPSC and provides information on the recall of defective products; the website is available to the public.

www.cpsc.gov

C.3.6 Eaton

This website contains general information and news on counterfeiting as well as product-specific information for molded case circuit breakers.

eaton.com/counterfeit

C.3.7 ERAI

The ERAI site provides information on counterfeit electronics. For a fee, members can upload their bill of materials to identify parts that are known to have been counterfeited.

www.erai.com

C.3.8 International Chamber of Commerce Counterfeiting Intelligence Bureau (CIB)

Formed in 1985, the CIB protects industry from the damage that counterfeiting causes by gathering intelligence, making undercover inquiries, organizing the seizure of counterfeits, and providing expert advice and training to its members, which mostly comprise large multinational companies, trade associations, law firms, and technology producers.

C.3.9 National Electrical Manufacturers Association (NEMA)

The NEMA website contains information on counterfeiting as well as links to pertinent reports and videos.

http://www.nema.org/gov/anti-counterfeiting/

C.3.10 SIA Semiconductor Industry Association (SIA)

The SIA site contains information on the counterfeiting of semiconductors.

http://www.sia-online.org/cs/anticounterfeiting

C.3.11 Square D – Schneider Electric

This website contains general information and news on counterfeiting as well as product-specific information for molded case circuit breakers.

http://www.schneider-electric.us/support/product-support-resources/counterfeiting/counterfeit-examples/

C.3.12 SMT Corporation

SMT Corporation maintains and extensive test lab and specializes in identification of counterfeit electronics.

www.smtcorp.com

C.3.12 Underwriters Laboratory (UL)

The UL website provides useful information on certifications and markings (examples of counterfeit labels); this website is available to the public.

www.ul.com

C.3.13 U.S. Chamber of Commerce Coalition against Counterfeiting and Piracy (CACP)

The CACP is committed to increasing the understanding of the negative impact of counterfeiting and piracy by working with Congress and the administration to drive greater government-wide efforts to address this threat.

http://www.theglobalipcenter.com/index.php/cacp

C.4 Enforcement Agencies

C.4.1 Air Force Office of Special Investigations (AFOSI)

877.246.1453

hqafosi.watch@ogn.af.mil

C.4.2 Defense Criminal Investigative Service (DCIS)

800.424.9098

http://www.dodig.mil/hotline

C.4.3 Federal Bureau of Investigation (FBI)

202.324.3000

https://tips.fbi.gov

C.4.4 Immigration and Customs Enforcement (ICE)

866.347.2423

C.4.5 INTERPOL

http://www.interpol.int/Public/FinancialCrime/IntellectualProperty/Default.asp

C.4.6 Naval Criminal Investigative Service (NCIS)

800.264.6485

C.4.7 NASA Office of Inspector General

800.424.9183

http://oig.nasa.gov/cyberhotline.html

C.4.8 Nuclear Regulatory Commission (NRC)

www.nrc.gov

C.4.9 Royal Canadian Mounted Police (RCMP)

http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/index-eng.htm

C.4.10 Strategy Targeting Organized Piracy (STOP)

STOP is an initiative involving the U.S. Department of Commerce, the U.S. Department of Justice, the U.S. Department of Homeland Security, the U.S. Food and Drug Administration, and the U.S. State Department.

http://www.stopfakes.gov/

C.4.11 U.S. Army Criminal Investigative Division (USACID)

703.806.0174

http://www.cid.army.mil/reportacrime.html

C.4.12 U.S. Customs and Border Protection (CBP)

http://www.cbp.gov/xp/cgov/trade/priority_trade/ipr/

C.4.13 U.S. Immigrations and Customs Enforcement (ICE)

http://www.ice.gov/pi/cornerstone/ipr/index.htm

C.4.14 The World Customs Organization (WCO)

http://www.wcoomd.org/home_wco_topics_epoverviewboxes_responsibilities_epipr.htm

C.5 Databases

There are numerous databases maintained by government agencies or support organizations. Usually general information is available to the public; however, the databases of discoveries and associated details are protected and require approval for receiving a password and accessing the information. Examples of the various sources of information outside the nuclear industry are listed here.

C.5.1 DOE's Suspect/Counterfeit Item (S/CI) Database

The DOE's Suspect/Counterfeit Item (S/CI) and Defective Item (DI) databases are controlled and require a password for access. Access is limited to DOE Complex organizations.

The GIDEP database is controlled and requires a password for access. Access is limited to entities that provide goods and services to the U.S. Government.

The FAA Suspect Unapproved Parts (SUP) database contains fraud and counterfeit information. It is controlled and requires a password for access.

The Pharmaceutical Security Institute (PSI) Counterfeiting Information System (CIS) is administered by the CIS and is accessible to member organizations.

http://www.psi-inc.org/counterfeitSituation.cfm

D
GENERIC REPORTING TEMPLATE

A reporting template serves as a human performance tool to help assure that pertinent information is collected for incidents of suspected CFIs.

The template included in this appendix lists the types of information EPRI requests when incidents are reported to the EPRI database and may be used as a starting point for development of reporting templates. However, different types of licensee and supplier organizations may need to customize a reporting template to serve the specific needs of their business and of any commercial or industry databases to which they report.

Suspect CFI Incident Report

Incidents reported may not yet be confirmed cases of suspected counterfeit or fraudulent items (CFIs). Reporting suspect items is encouraged as a preventative measure. Additional notification will be provided when available for incidents confirmed to be false by the original equipment manufacturer

Issue Date:

Report Number:

Report Type:

Part 1: Item Information

ITEM TYPE (NOUN, ADJECTIVE, ADJECTIVE FORMAT):	**ADDITIONAL DESCRIPTION:**
SUSPECT ITEM SUPPLIER (PROVIDED ITEM)	**SUSPECT ITEM SUPPLIER PART/MODEL NO:**
ORIGINAL EQUIPMENT MANUFACTURER (AUTHENTIC)	**OEM (AUTHENTIC) PART/MODEL NO.**
ORIGINAL EQUIPMENT SUPPLIER (AUTHENTIC)	**OES (AUTHENTIC) PART/MODEL NO.**
ASSEMBLY LEVEL	**DISCIPLINE**
LOT, BATCH, OR SERIAL NUMBER INFO (COUNTERFEIT):	**DATE/DATE CODE (COUNTERFEIT):**
WHEN IDENTIFIED	**PROMPTED DISCOVERY**
COMMENTS:	

Part 2: Reporting Information

IS SUSPECT SUPPLIER APPROVED DISTRIBUTOR/AGENT? ☐ Yes ☒ No

WAS SUSPECT ITEM SUPPLIER NOTIFIED? ☐ Yes ☒ No

The original equipment manufacturer or other reliable source (not the suspect item supplier themselves) should be contacted to determine if the supplier who provided the suspect item is an approved distributor/agent. If suspect item supplier is not an approved distributor/agent, it is recommended that they <u>not</u> be notified prior to contacting the OEM and reporting the incident to proper authorities. If possible, suspect items should not be returned.

WAS OEM NOTIFIED?: ☒ Yes ☐ No

OEM should always be notified first so they may determine status of the suspect item supplier, inform authorities conducting ongoing investigations and assist in confirming or refuting authenticity of the item(s)

WAS NRC NOTIFIED? ☐ Yes ☒ No

NRC should be notified if the suspect item is reportable in accordance with the requirements of 10CFR, Part 21, Reporting of Defects and Noncompliance, Appendix B

Suspect CFI Incident Report

Part 3: Status

WAS ITEM CONFIRMED TO BE COUNTERFEIT OR FRAUDULENT? ☒ Yes ☐ No ☐ Under Investigation
COMMENTS:

Part 4: Contact Information

ORGANIZATION THAT IDENTIFIED SUSPECT ITEM:	**CONTACT NAME:**
FACILITY:	**PHONE NUMBER:**
ORGANIZATION TYPES	**EMAIL:**

Part 5: Incident Description and Guidance

Please include photographs of the authentic and counterfeit items as well as any information that might be useful for others in determining if they are in possession of similar suspect item	
COMMENTS:	
PHOTO OF AUTHENTIC ITEM	**PHOTO OF SUSPECT ITEM**