



Counterfeit Part Awareness, Avoidance, & Risk Mitigation

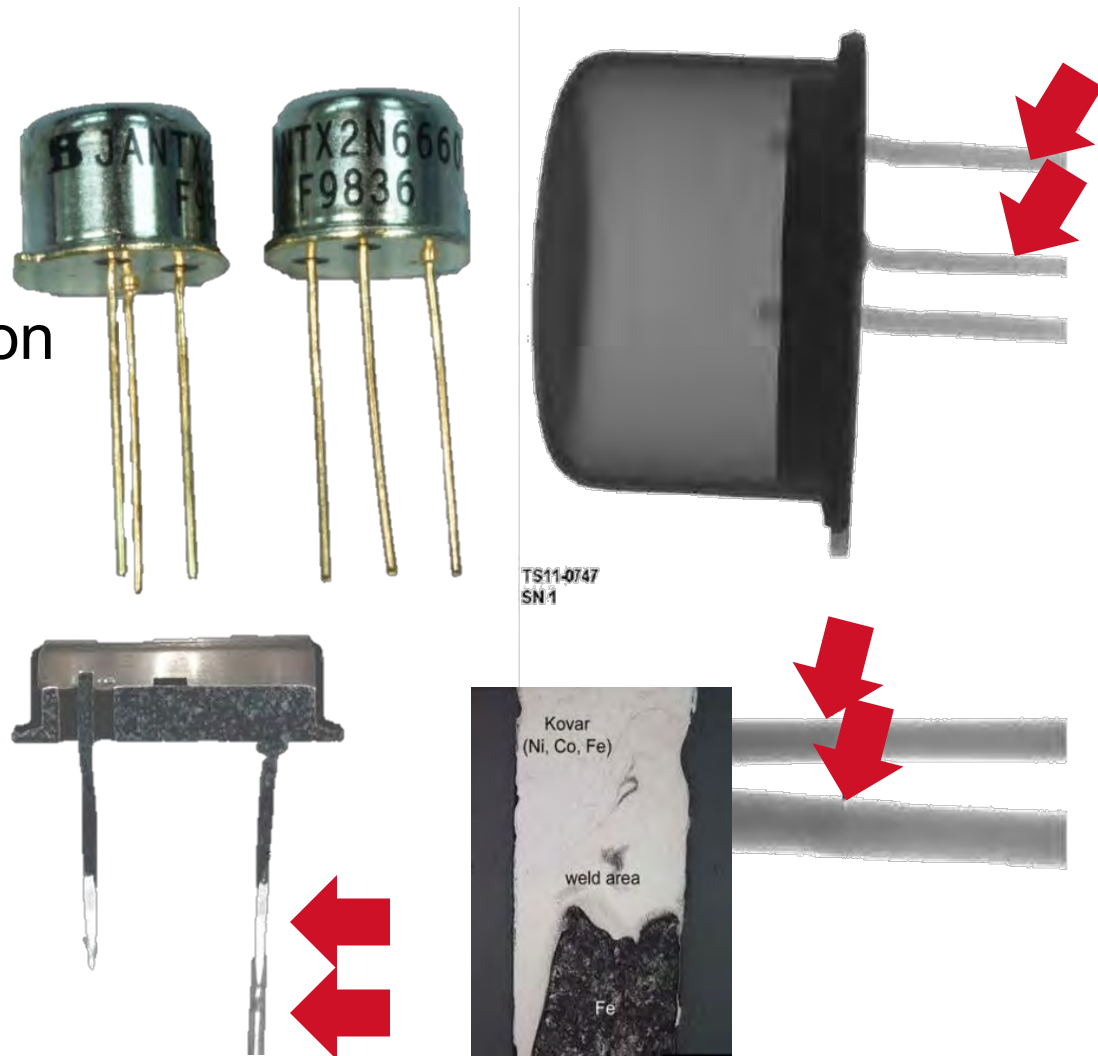
George Young
April 2015
ASQLA

THIS PRESENTATION CONTAINS GENERAL, CONDENSED SUMMARIES OF ACTUAL REGULATORY OR RAYTHEON COMPANY REQUIREMENTS, OTHER COMPANY AND ORGANIZATIONS PRODUCTS OR SERVICES.

THE PRESENTATION IS FOR INFORMATION PURPOSES ONLY. IT IS NOT MEANT TO BE AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE OR ENDORSEMENT OF ANY SPECIFIC REGULATORY ITEM, PRODUCT OR SERVICE.

Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



Example of welded lead replacements

Counterfeit Definition(s) SAE AS5553

3.1 Suspect Part

A part in which there is an indication that it may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent part or counterfeit part provided below.

3.2 Fraudulent Part

Any suspect part misrepresented to the Customer as meeting the Customer's requirements.

3.3 Counterfeit Part

A fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud.

NOTE: The following diagram (Figure 2) depicts the above interrelationship between Suspect, Fraudulent and Counterfeit Parts. A Suspect Part may be determined to be, fraudulent or counterfeit through further evaluation and testing. All counterfeit parts are fraudulent, but not all fraudulent parts are counterfeit.

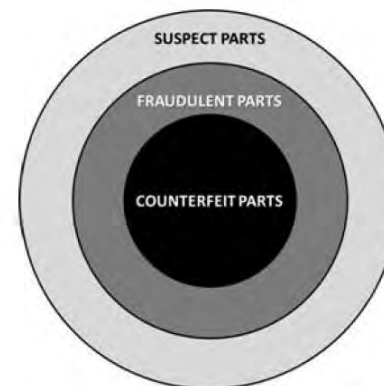


FIGURE 2 - INTERRELATIONSHIP BETWEEN SUSPECT, FRAUDULENT, AND COUNTERFEIT PARTS

Counterfeit Definition(s) DFARS 252.246-7007

“Counterfeit electronic part” means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

“Suspect counterfeit electronic part” means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

Counterfeit Definition(s) Raytheon TC-001

Counterfeit Items include, but are not limited to, goods or separately-identifiable items or components of goods that:

- (i) are an illegal or unauthorized copy or substitute of an OM item;
- (ii) are not traceable to an OM sufficient to ensure authenticity in OM design and manufacture;
- (iii) do not contain proper external or internal materials or components required by the OM or are not constructed in accordance with OM design;
- (iv) have been re-worked, re-marked, re-labeled, repaired, refurbished, or otherwise modified from OM design but not disclosed as such or are represented as OM authentic or new; (v) have not passed successfully all OM required testing, verification, screening, and quality control processes; or
- (vi) an item with altered or disguised documentation, package labeling, or item marking intended to mislead a person into believing a non-OM item is genuine, or that an item is of better or different performance when it is not.

Misrepresent & Intent / common theme across many definitions

Other Terms & Definitions

SAE AS5553

ELECTRICAL, ELECTRONIC, AND ELECTROMECHANICAL (EEE) PART:

Electrical, electronic, and electromechanical parts are components designed and built to perform specific functions, and are not subject to disassembly without destruction or impairment of design use. Examples of electrical parts include resistors, capacitors, inductors, transformers, and connectors. Electronic parts include active devices, such as monolithic microcircuits, hybrid microcircuits, diodes, and transistors. Electromechanical parts are devices that have electrical inputs with mechanical outputs, or mechanical inputs with electrical outputs, or combinations of each. Examples of electromechanical parts are motors, synchros, servos, and some relays

DFARS 252.246-7007

“Electronic part” means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112-81). The term “electronic part” **includes any embedded software or firmware.**

Other Terms & Definitions

SAE AS5553

BROKER:

In the independent distribution market, Brokers are professionally referred to as Independent Distributors. See definitions for “Broker Distributor” and “Independent Distributor.”

INDEPENDENT DISTRIBUTOR:

A distributor that purchases parts with the intention to sell and redistribute them back into the market. Purchased parts may be obtained from Original Equipment Manufacturers (OEMs) or Contract Manufacturers (typically from excess inventories), or from other Distributors (Franchised, Authorized, or Independent). Resale of the purchased parts (redistribution) may be to OEMs, Contract Manufacturers, or other Distributors. Independent Distributors do not normally have contractual agreements or obligations with OCMs. See definition of “Authorized (Franchised) Distributor.”

DFARS 252.246-7007

No definition provided

Other Terms & Definitions

SAE AS5553

AUTHORIZED (FRANCHISED) DISTRIBUTOR:

Distributor when they perform Authorized Distribution.

AUTHORIZED DISTRIBUTION:

Transactions conducted by an OCM-Authorized Distributor distributing product within the terms of an OCM contractual agreement. Contractual Agreement terms include, but are not limited to, distribution region, distribution products or lines, and warranty flow down from the OCM. Under this distribution, the distributor would be known as an Authorized Distributor. For the purposes in this Standard, Franchised Distribution is considered synonymous with Authorized Distribution.

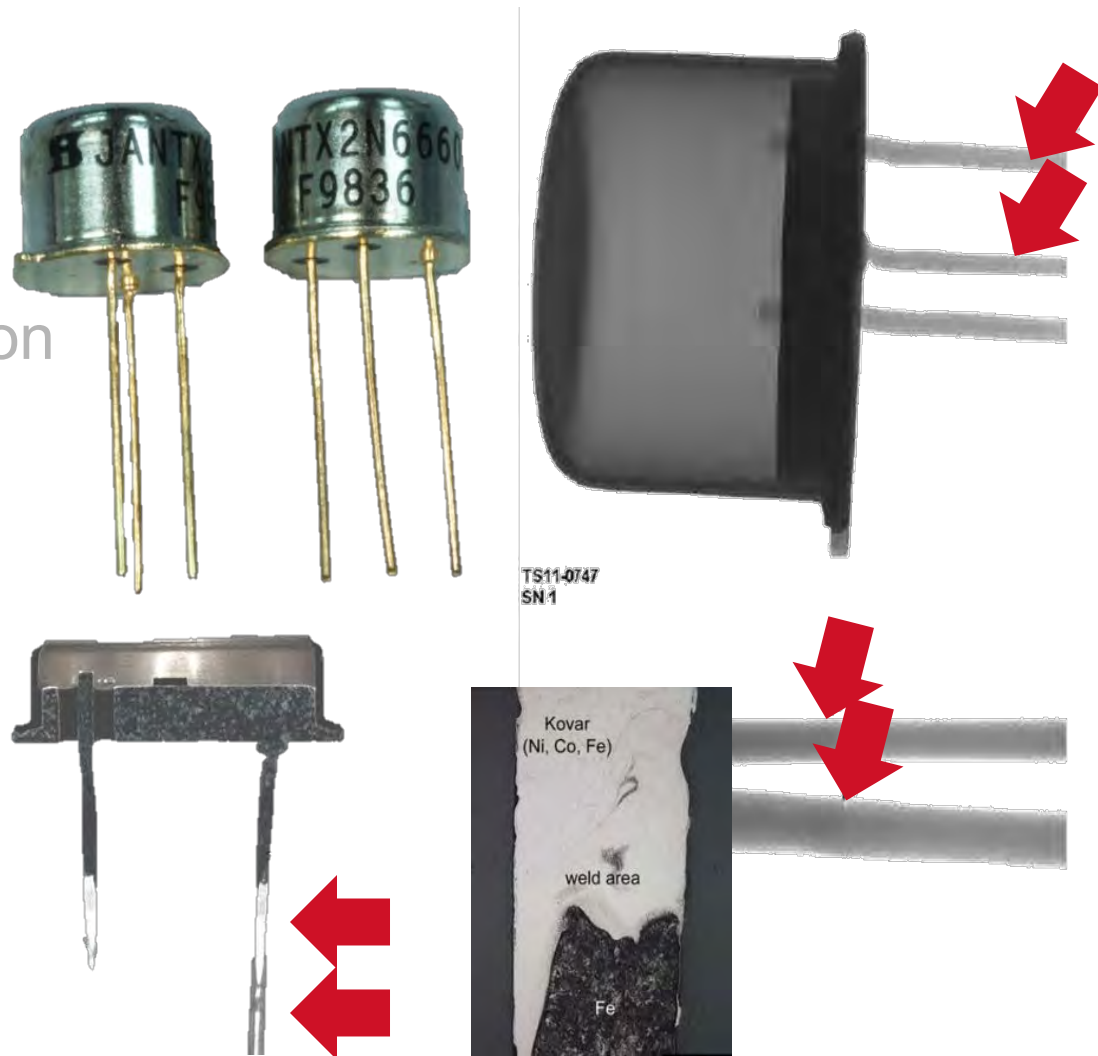
DFARS 252.246-7007

No definition provided however System Criteria (5) provides the following

(5) Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources...

Counterfeit Avoidance & Risk Mitigation

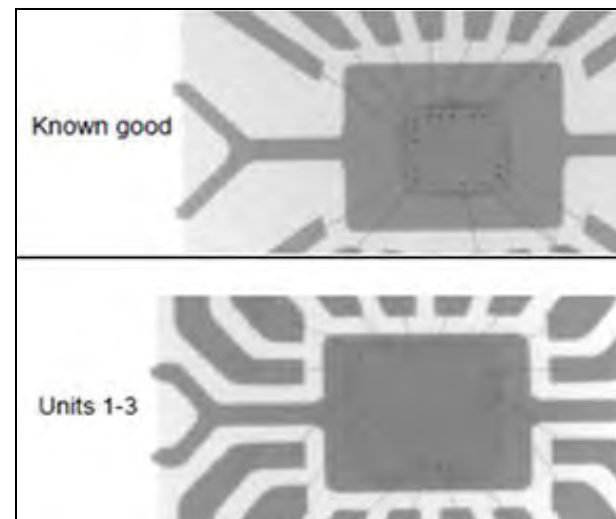
- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



Example of welded lead replacements

Overview of Counterfeit Parts

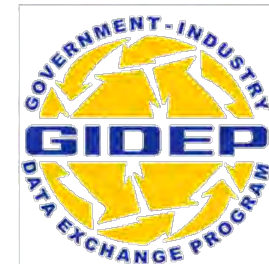
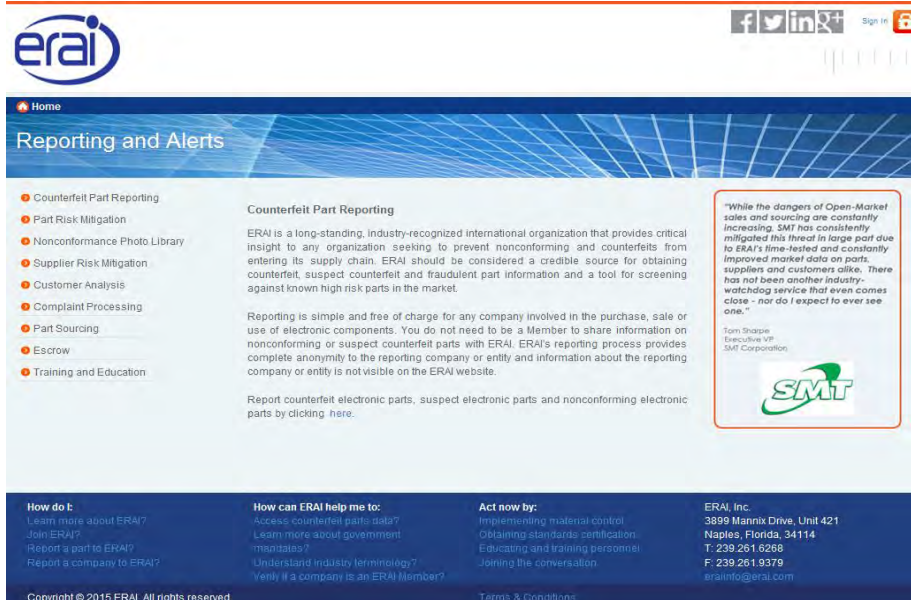
- Counterfeiting affects all industries; electronics is a focus
- E-waste is a main source of supply
- Obsolescence provides a source of demand
- Distributed mainly through non-franchised distributors
- Increasing incident volume and variety
- Counterfeiting is price independent



Counterfeits impact all industries

Counterfeit Risk

- **68 GIDEP Alerts** in 2014
 - Majority are for electronic components
 - Two alerts since 2013 involve authorized distribution
 - Non electronic component items: network switches, hard drives, UL / Test Lab marks, tape



GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM ALERT		
1. TITLE (Class, Function, Type, etc.)	2. DOCUMENT NUMBER	
Suspect Counterfeit, Tape, Metallized Polyvinyl Fluoride	3. DATE (DD-MM-YY)	
GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM ALERT		
1. TITLE (Class, Function, Type, etc.)	2. DOCUMENT NUMBER	
Suspect Counterfeit, Disk Drive Unit	3. DATE (DD-MM-YY)	
GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM ALERT		
1. TITLE (Class, Function, Type, etc.)	2. DOCUMENT NUMBER	
Suspect Counterfeit, Integrated Circuit (Flash Erasable, Reprogrammable CMOS PAL Device)	3. DATE (DD-MM-YY)	

- **Over 700 Suspect Counterfeit Reports in ERAI Alerts During the Past 12 Months**

http://www.era.com/ca_Counterfeit_Awareness

Persistent Risk Requires Robust Processes


Counterfeit Risk

GOVERNMENT - INDUSTRY DATA EXCHANGE ALERT	
1. TITLE (Class, Function, Type, etc.)	
Suspect Counterfeit, Microcircuit, 32Kx8 Autostore nvSRAM	
Suspect Counterfeit, Cover, Electrical Connector	
Suspect Counterfeit, 4-Port Gigabit and 24-Port Ethernet Switch/Router	

DLA Federal Supply Group Focus

- FSG 59 (Electrical and Electronic Equipment Components)
- FSG 29 (Engine Accessories)
- FSG 47 (Pipe, Tubing, Hose, and Fittings)
- FSG 53 (Hardware & Abrasives)
- FSG 25 (Vehicular Equipment Components)
- FSG 31 (Bearings)

Suspect Counterfeit, Capacitor, Fixed Electrolytic

ERAI 6200 +
GIDEP 600 +
Trend 

AGENCY ACTION NOTICE	
1. TITLE	
PROCUREMENT FRAUD INVOLVING BRISTOL ALLOYS, INC. (CAGE 30RA)	
1. TITLE	
CPSC ALERT: COUNTERFEIT SMOKE ALARMS DISTRIBUTED	
1. TITLE	
COUNTERFEIT REFRIGERANTS – INFORMATION	
1. TITLE	
Suspect Counterfeit, Disk Drive Unit	
POTENTIAL COUNTERFEIT COMBAT APPLICATION TOURNIQUET (C-MEDICAL MATERIEL)	
1. TITLE	
COUNTERFEIT CIRCUIT BREAKERS RECALLED BY SPECIALTY LAMP INTERNATIONAL DUE TO FIRE HAZARD	

Electronics is Primary Risk but not the only Risk

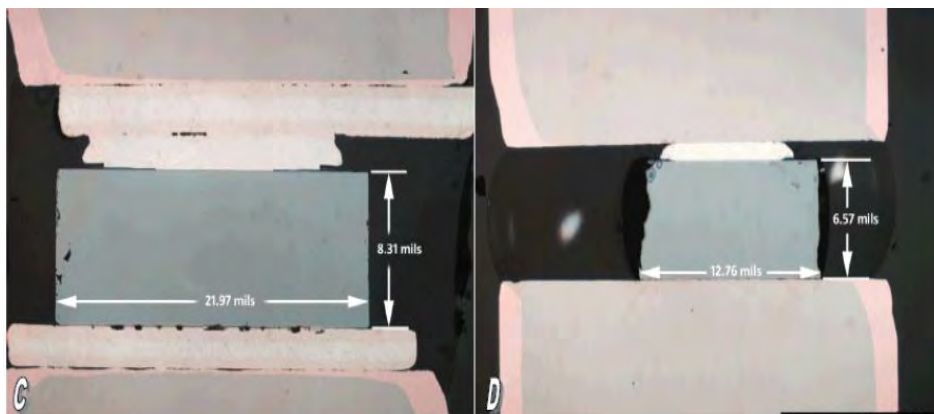
Counterfeiting “Raw Materials”



Part Removal & Storage



Counterfeit Examples

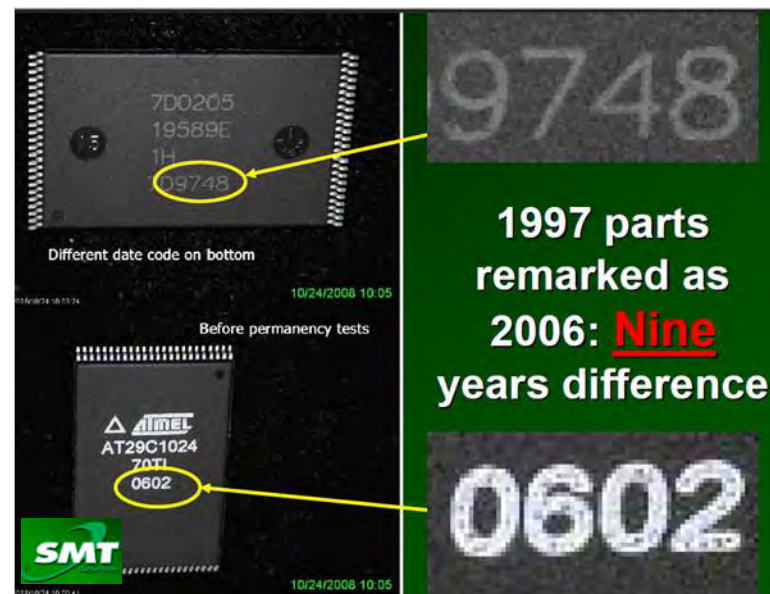
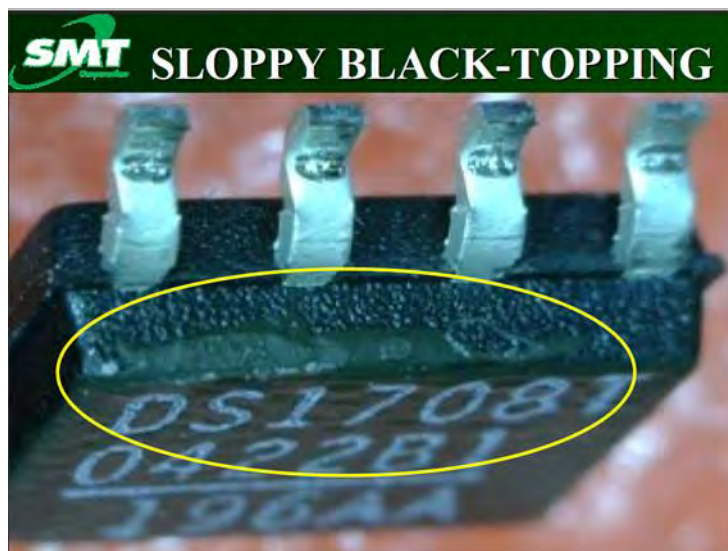


Authentic

Counterfeit


14V 0.5W Zener Diode

- Smaller die
- No / poor metallurgical bond
- Smaller package with pure tin terminations vs OEM tin / lead termination
- OEM stated parts were not manufactured by them. Smaller die size indicative of commercial part produced by another manufacturer.



Additional Counterfeit Examples





DEPARTMENT OF
DEFENSE

DEFENSE
CRIMINAL
INVESTIGATIVE
SERVICE

FOR MORE
INFORMATION,
PLEASE
CONTACT
HEADQUARTERS
DCIS
CRIM INTEL:

Criminal Intelligence Bulletin

2007-001

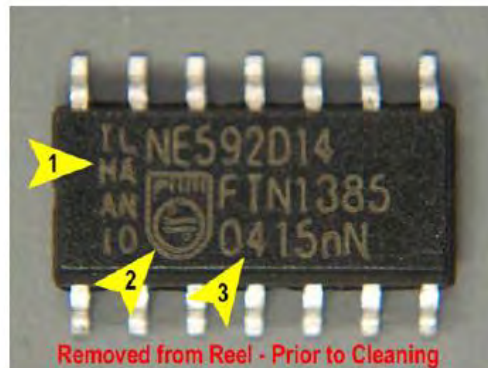
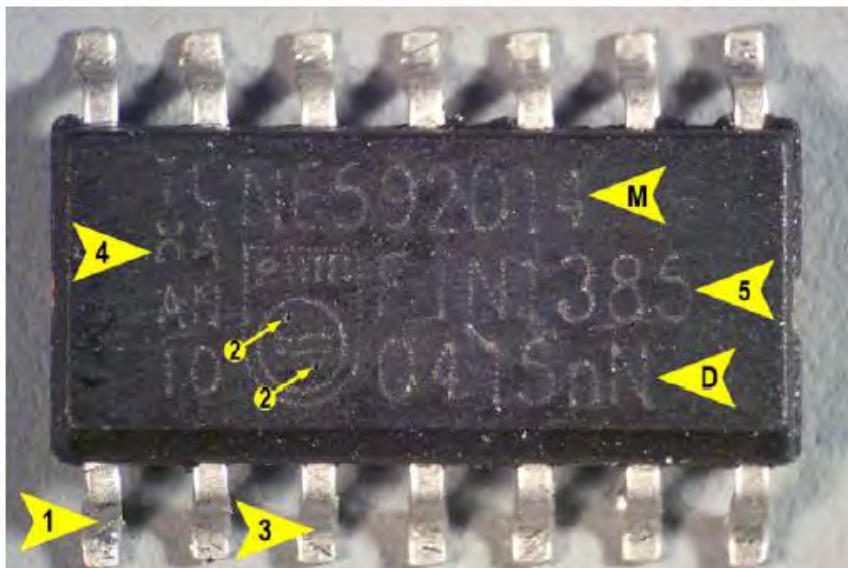
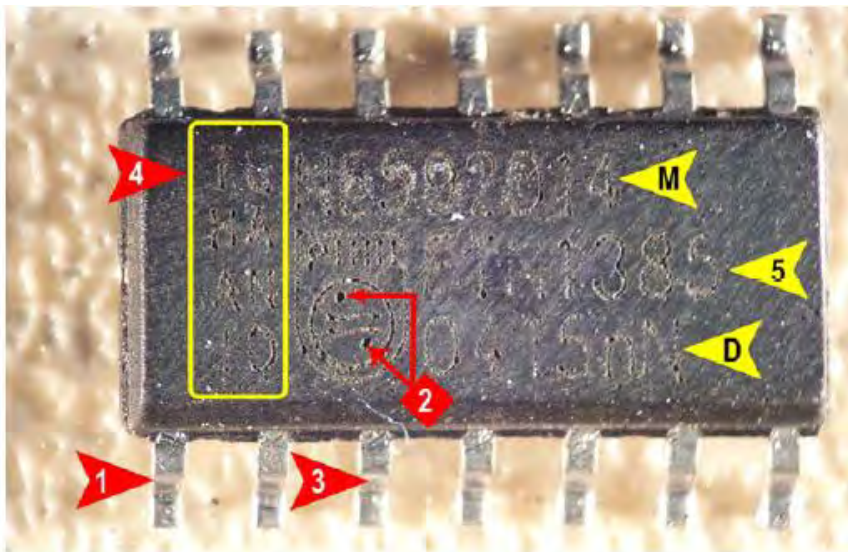
Counterfeit CISCO Products

The purpose of this Criminal Intelligence Bulletin is to alert the Law Enforcement (LE) community to the threat posed by imitation CISCO products used in DoD systems.

At least five DCIS investigations have uncovered counterfeit CISCO routers, network cards, and switches being supplied to DoD, including Army, Navy, and Air Force. Several DoD entities (listed below) have procured counterfeit CISCO products and deployed them throughout the Global Information Grid. Using counterfeit products is significant because the items are not made with the same level of quality control as the authentic product and are often found to have improper shielding, which can lead to radiation exposure and fire hazards. Imitation parts also have a higher failure rate than their authentic versions, and are neither a designated nor authorized item in any DoD procurement contract.

There is also the possibility that these products could perform malicious network ac-

Remarking example



CCA failure analysis

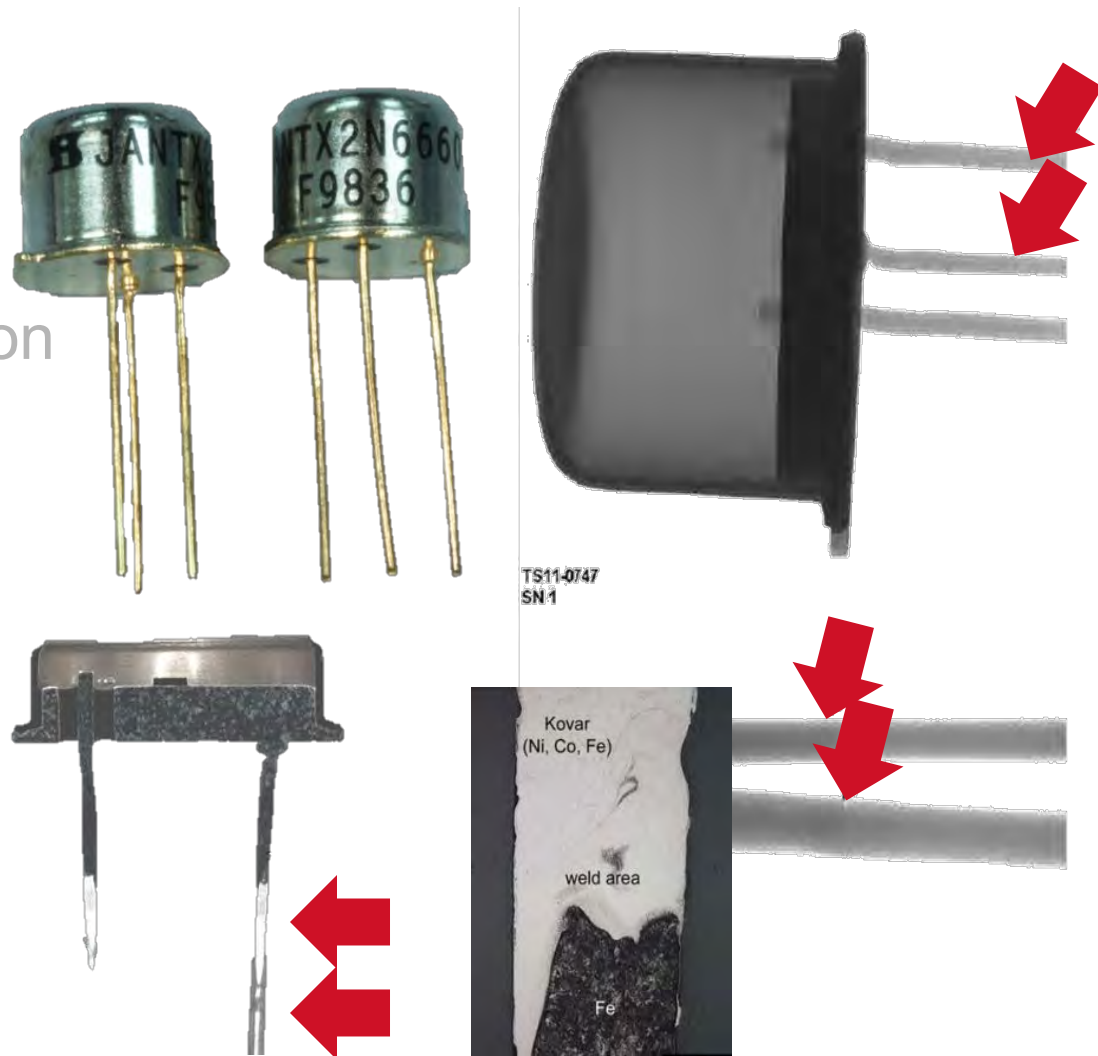
CCA produced by contract manufacturer.

Component manufacturer identified on the part confirmed they did not produce parts with this date code.

Remarking via Laser, also evidence of a cover coat. Multiple die configurations found.

Counterfeit Avoidance & Risk Mitigation

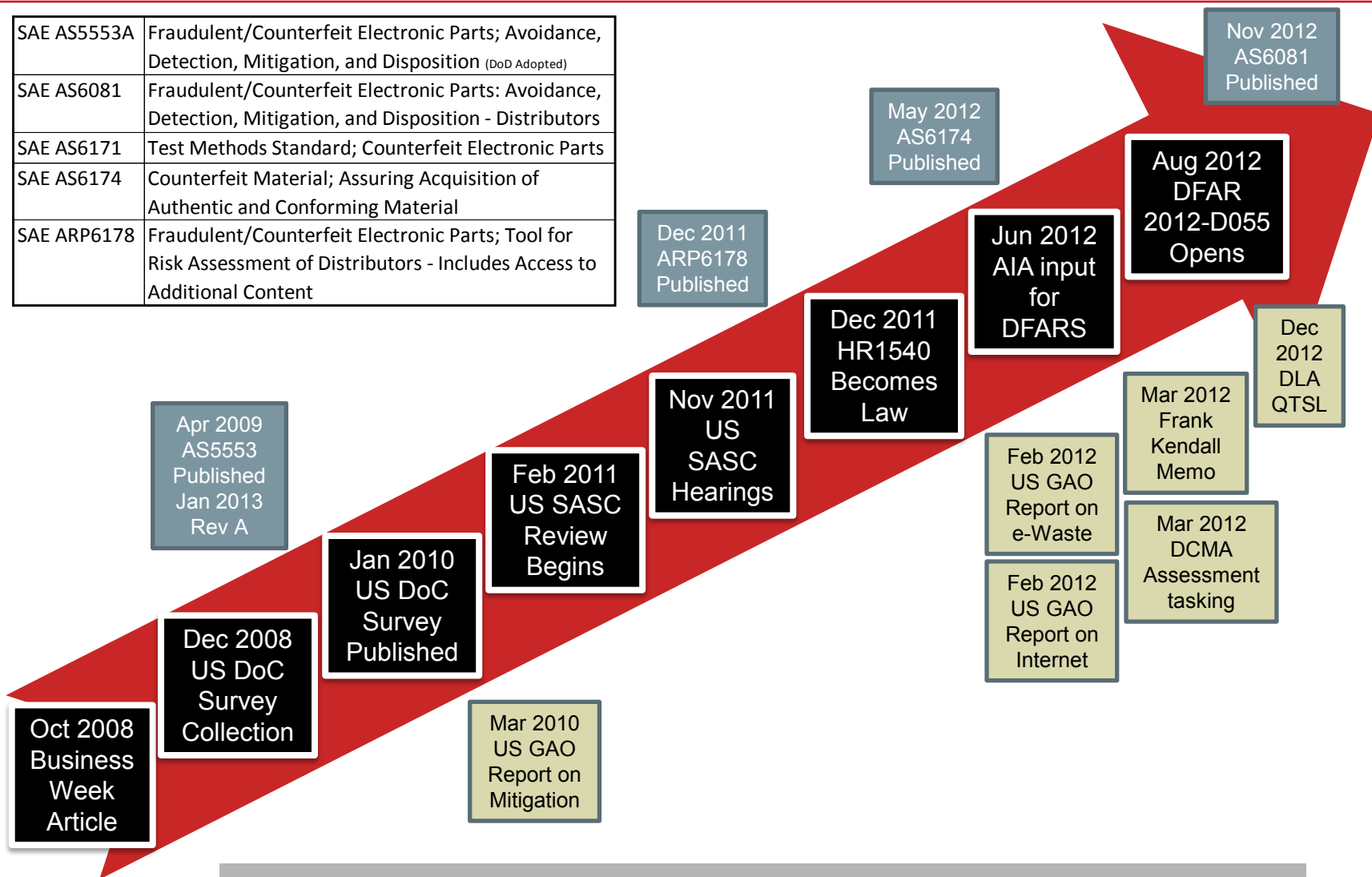
- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



Example of welded lead replacements

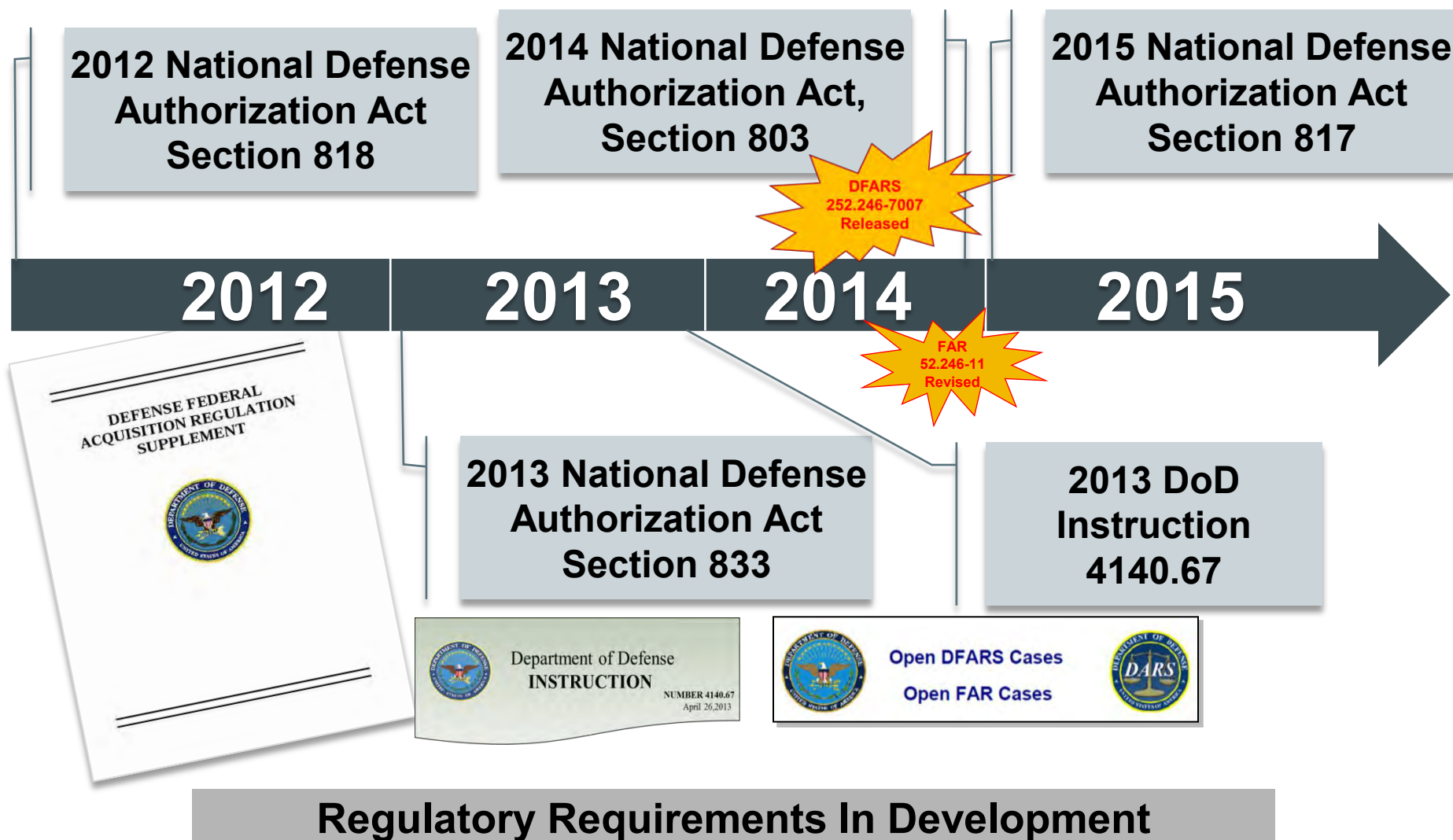
US Government & Standards Activity

SAE AS5553A	Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (DoD Adopted)
SAE AS6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors
SAE AS6171	Test Methods Standard; Counterfeit Electronic Parts
SAE AS6174	Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
SAE ARP6178	Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors - Includes Access to Additional Content



Build up to US Procurement Regulations

US Regulatory Activity



DFARS/FAR Cases of Interest

DFARS Case 2012-D055: Detection and Avoidance of Counterfeit Parts

- **Counterfeit avoidance becomes part of contractor purchasing system**



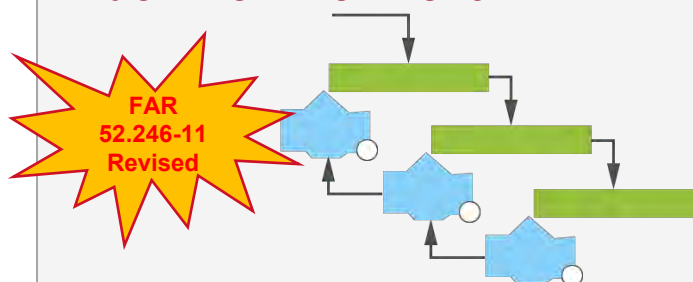
DFARS Case 2014-D005: Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation

- **Anticipated regulations for smaller businesses and non CAS covered contractors**



FAR Case 2012-032: Higher Level Contract Quality Requirements

- **Revised the Quality Management flow down environment**



FAR Case 2013-002: Expanded Reporting of Nonconforming Supplies

- **May significantly increase reporting requirements for non-conforming material**



DFARS 252.246-7007 Summary

- DFARS 252.246-7007 for Counterfeits released 05/06/14
- Partial implementation of 2012 & 2013 NDAA requirements
- Effective 05/06/14
- First of four planned regulations (DFARS and FARs)
- “risk based provides for flexibility on how contractors interpret and implement the 12 system criteria.
- Government Agencies (DCMA, DPAP, etc.) have not yet given further definitive guidance on what will be acceptable.

DFARS for Counterfeit Electronic Parts

DFARS 252.246-7007 12 System Criteria (partial text)

- 1) The **training** of personnel.
- 2) The **inspection and testing of electronic parts**, including criteria for acceptance and rejection.
- 3) **Processes to abolish** counterfeit parts proliferation.
- 4) **Processes for maintaining electronic part traceability** (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies....
- 5) **Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer** or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria.
- 6) **Reporting and quarantining of counterfeit electronic parts** and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer **and** to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of....
- 7) **Methodologies to identify** suspect counterfeit parts **and to rapidly determine** if a suspect counterfeit part is, in fact, counterfeit.

DFARS 252.246-7007 12 System Criteria (partial text)

- 8) **Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts** and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.
- 9) **Flow down of counterfeit detection and avoidance requirements**, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.
- 10) **Process for keeping continually informed** of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes.
- 11) **Process for screening GIDEP reports** and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.
- 12) **Control of obsolete electronic parts** in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle.

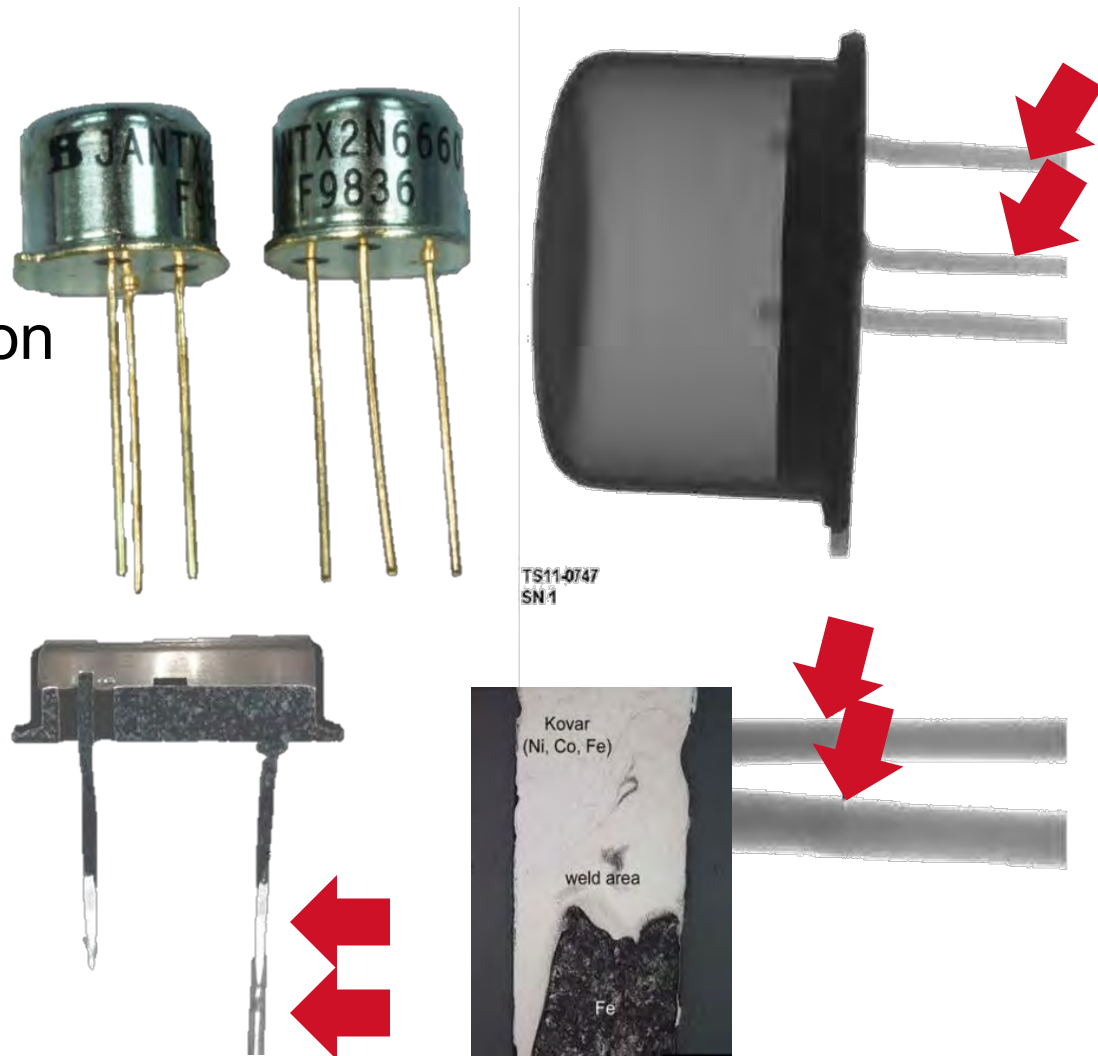
Challenges

- Electronic Part includes embedded software and firmware
- Unallowable costs, with little opportunity to make allowable
- Counterfeit detection and avoidance systems now in CPSR
- Commercial items and COTS are in scope
- Traceability in supplier base of piece part and parts in assemblies
- No grandfather clause for inventory in supply base
- GIDEP reporting and screening within global supply base
- Impact to small businesses

DFARS Present Challenges Throughout Supply Chain

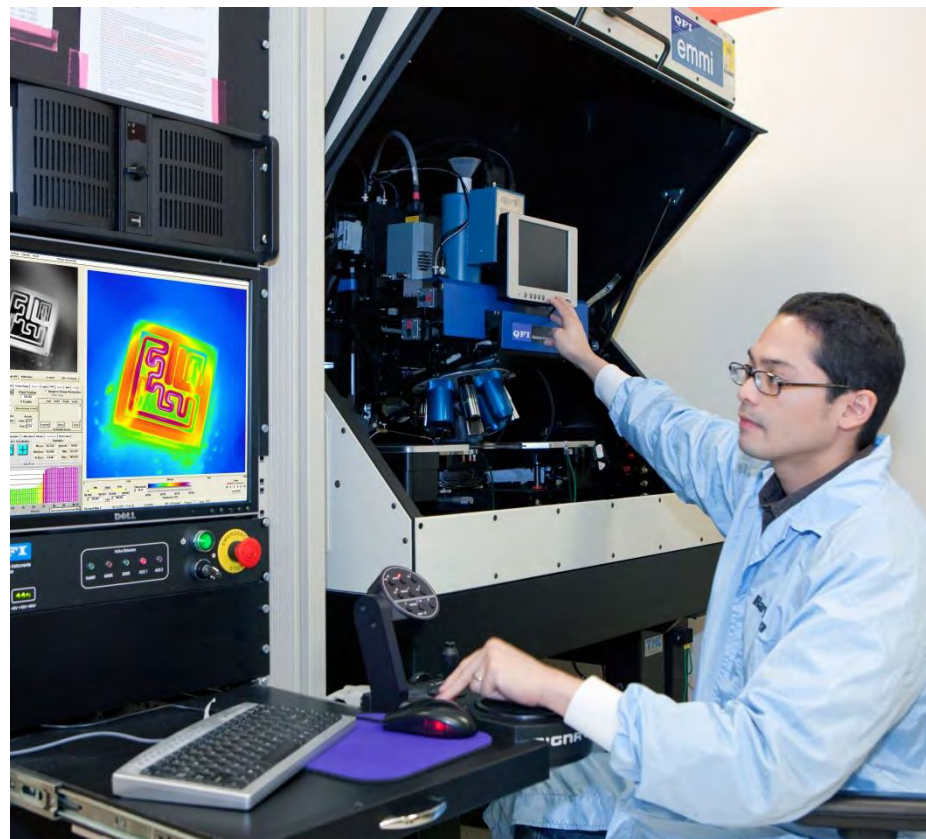
Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- **Counterfeit Risk Mitigation**
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



Raytheon Company Approach

- Raytheon utilizes a standardized, risk based approach
- Prevention focus: electronics, materials, mechanical, assemblies and test equipment
- Obsolescence management is key
- OEM preferred; Five brokers with testing
- Supply Base:
 - Optimization
 - Awareness
 - Requirement Flow Down
 - Assessment
- GIDEP reporting on all incidents
- Suspect material does not return to Supply Chain



Lower Risk through Robust Process and Tools

Raytheon Company Approach

Example of Raytheon Counterfeit Risk Mitigation Requirement

Hard Copy Uncontrolled
Compare Date to On-Line Version

Raytheon Quality Note

GP

Revision - Date

7 – 10/10/2013

ELECTRONIC PART COUNTERFEIT RISK MITIGATION

- Identifies specific tests & inspection
- Defines sample requirements
- Requires data review by Raytheon

Inspection/Test	Requirement	Sample Size
Packaging Inspection and OEM/OCM history investigation	Verification that package marking is consistent with the OEM marking and that the date / lot code is not later than the last production date. For Qualified Parts List (QPL) parts, verify that the manufacturer identified on the package was a QPL source for the time period represented by the part date / lot code.	3 parts from each date code 1/
External Visual Inspection	IDEA-STD-1010, 20 X magnification minimum, 50 X or greater may be used to detect counterfeiting	100% up to 45 pieces and minimum 45 piece sample for lots greater than 45 pieces
Mechanical Inspection	IDEA-STD-1010 paragraph 10.3.3	20 parts from each date code
Marking Permanency	Using the following in the order specified: 1) 3 parts Mineral Spirits, 1 part Isopropyl Alcohol mixture, 2) Acetone	3 parts from each date code 1/
Blacktop Testing	1) 1-Methyl 2- Pyrrolidone (AS6081), 2) Dynasolve 750 solution (AS6081), 3) Scrape Test (IDEA 1010.3.2.3)	3 parts from each date code 2/ 1/
Delid / Decapsulation	Component Decap (cavity devices only) and die photograph to compare die marking to external part marking, OEM/OCM die maps or datasheet or known good die, if available	3 parts from each date code 1/
Lead Cross-Section	For metal can, through hole packages such as TO-99, TO-100, TO-8, etc. All device leads must be cross-sectioned in order to determine if leads have been extended by welding	3 parts from each date code, all leads (may be performed on the Delid / Decapsulation sample) 1/
Solderability	per IPC/EIA-J-STD-002	3 parts from each date code 1/
X-Ray Fluorescence	Termination finish composition	3 parts from each date code 1/
Electrical	Test in accordance with commodity matrix in Appendix A herein	100%
Radiographic Inspection	Radiographic Inspection of the die and internal construction of the product	100%

Raytheon Approach

Organizational Resources

Tools, Training, Communication

COUNTERFEIT MATERIAL AVOIDANCE		
OVERALL RESULTS OF PPV FOR THIS PROCESS	Response	DETAILS
Is Process in control and effective?		
If there is a contractual flowdown, is the supplier meeting that requirement?		
Has Raytheon identified this as a key process as relates to KPC Management?		
If there is controlled documentation that outlines elements of this process, is it readily available?		
Is there a method the supplier uses to monitor effectiveness of process?		
Was hardware reviewed?		
Was hardware reviewed acceptable?		
Were the supplier's inspection documentation reviewed in preparation for this PPV?		
EVALUATION AREAS		

Customer Success is Our Mission

Raytheon Home | Directory | Search | Newsroom | Collaboration | Help

RCPT Home Search Supplier Info Request SME Login Support Logout

Raytheon Counterfeit Parts Tool Return to CIMS Home

The Raytheon Counterfeit Parts Tool (RCPT) captures and documents counterfeit part incidents and provides access to search Industry Standard datasets for counterfeit issues.

Search

Supplier Info

Create RCPT Incident Report

Team Login

Support

1.1 PROCUREMENT POLICY AND Intent: Review identified process documented on Action Status Tab.

1.1.1 Does the company procure materials?

Materials

Mechanical Subsystems Directorate

Raytheon

Materials & Mechanical LESSONS LEARNED!

Counterfeit Electronics- What's Inside?

May 7, 2013 Issue 119

ABSTRACT

Counterfeiting is an international industry that profits from reproductions or imitations of manufactured goods, such as electronic components, medications, etc. A counterfeit electronic part is one whose identity has been deliberately misrepresented by the supplier. Recently, there has been a dramatic increase in the occurrence of counterfeit electronics in the military/aerospace industry, including RMS.

Figure 1: Left: Counterfeit device discovered at RSN with...

EDGEworks

Counterfeit Parts

Engineering Area: Design and Implementation

243-RP Distributors material, military program counterfeit parts counterfeit authentication 015-013 technology obsolescence inventory mission assurance investigation 004-019

Recently, a Raytheon production program had to issue a recall due to a malfunctioning system. Failure analysis indicated the root cause of the problem to be counterfeit parts used on a circuit card. The program replaced the parts and returned the system to the field; however, the cost impacted Raytheon's profit margin and the customer's confidence in our system.

In November of 2011, Arizona Senator John McCain stated, "Counterfeit parts pose an increasing risk to our national security, to the reliability of our weapons systems, and to the safety of our men and women in uniform."

Description

Raytheon has invested significantly into the development of a Counterfeit Product Risk Mitigation and Prevention strategy. This page describes how programs can implement that strategy to minimize the risk of counterfeit parts in delivered systems.

Purpose

- Facilitate program implementation using single location of counterfeit parts plan templates, policies, best practices and procedures.
- Communicate Raytheon policy changes to minimize the risk of counterfeit parts.
- Provide awareness information to emphasize the importance of the threat to Raytheon.

Raytheon

Customer Success is Our Mission

Raytheon Home | Directory | Search | Newsroom | Collaboration | Help

CTN Home RSP & RSS PEMS/Non-Mil Libraries & Teams Obsolescence Management Counterfeit Parts International & Regional Tools

Counterfeit Parts

Current Events and Updates

New Updates added 02/28/2013

ERAI Executive Conference April 18 & 19 Orlando, FL [+]

SMTA /CALCE Counterfeit Symposium East, June 25-27, College Park, MD [+]

External Webinar: Eliminating Counterfeits at NASA Dryden [+]

NCS Edgeworks, Execution+ Counterfeit Parts [+]

2012 DMSMS conference has been rescheduled and will be November 26-29 in Orlando, FL [+]

Raytheon's Technology Today - Responding to the Counterfeit Threat [+]

2012 ERAI Conference Presentations Posted [+]

Counterfeit Parts Navigation

Home

Counterfeit Parts

Resources

Resources: Home Page

Resources: Raytheon Papers and Presentations

Resources: Industry Presentations

Incident Database (US only)

Raytheon Counterfeit Parts Tool

Previous Updates

Technology Today

HIGHLIGHTING RAYTHEON'S TECHNOLOGY

2012 Issue 1

Home

Message From Mark

Features

Raytheon Leaders

Eye on Technology

People

Resources

Events

Patent Recognition

Interact

Archive

Responding to the Counterfeit Threat

When counterfeit electronic components, materials and mechanical parts enter the supply chain, they can jeopardize product quality and reliability, threatening overall mission success.

In the broadest sense, counterfeiting is the deliberate misrepresentation of an item with the intent to deceive a customer or an end user. Counterfeiters have found discarded commercial electrical and electronic products to be a good source of raw material for their...

Enterprise Resources

Raytheon Requirement Documents

Supplier Connections

www.raytheon.com/connections/supplier/index.html

Raytheon is committed to providing our suppliers and partners with the most advanced electronic tools and processes, and best-in-class SCM systems to enable fast, secure and efficient ways to improve the information flow to our supply chain including:

- Transmitting critical information
- Performing business transactions
- Collaborating with partners

This commitment supports our strategic efforts to align company resources and processes with our suppliers' capabilities, by welcoming diversity and by supporting our partners' efforts to provide superior performance and quality.

Connections to:

[Supplier Registration](#)

[Electronic Commerce at Raytheon](#)

[Raytheon Terms and Conditions](#)

[Conflict Minerals Resources](#)

[Quality Notes](#)

[Raytheon Carrier Guide](#)

[Raytheon Supplier Diversity](#)

Counterfeit Specific Quality Notes

GP: Counterfeit Electronic Part Risk Mitigation
 WE: Counterfeit Material Avoidance Process Requirements
 WK: Metal Procurement Certification and Traceability Requirements
 WL: Counterfeit Risk Mitigation, Chemical, Gas, Non-Metallic, Raw Material
 WM: Counterfeit Risk Mitigation, Mechanical Part
 WN: Counterfeit Risk Mitigation, Fab, Molded, Plastic and Rubber Parts

[TC-004 International General Terms and Conditions](#)

[TC-009 Fixed Price Level of Effort Subcontracts](#)

[TC-013 Purchase Order Attachment- Warranty for Goods Obtained From Brokers](#)

[TC-020 Fixed Price Incentive Purchase Orders](#)

[TC-DEAR General Terms and Conditions of Purchase Supplement](#)
 It will be used when a purchase order is placed with a U.S. Government Department of Energy contract or higher-tier subcontract

[TC-HARDCODE Standard Hard-Coded Purchase Order Terms and Conditions](#)

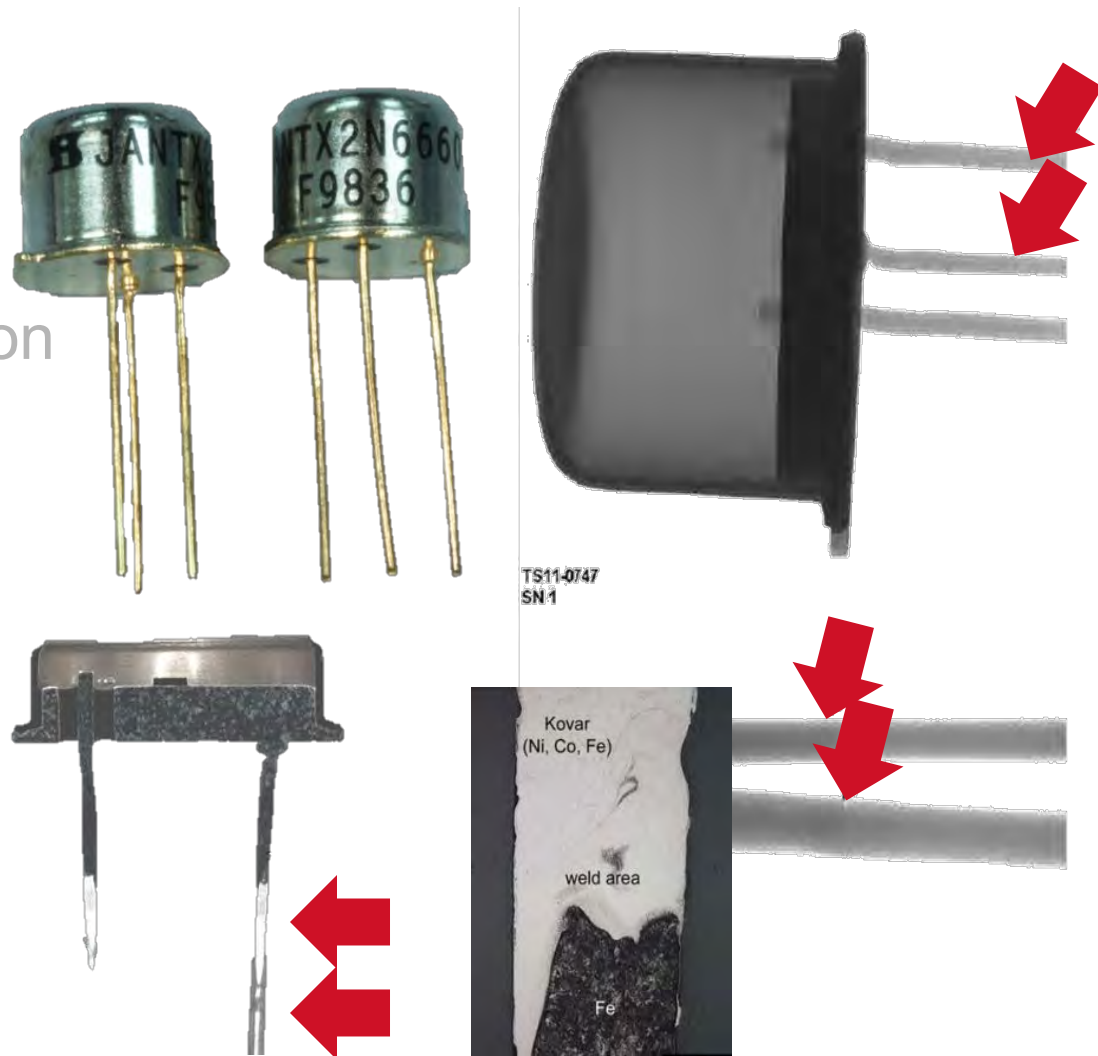
Key Counterfeit Avoidance Requirements

- **TC-001 General Terms and Conditions of Purchase (04/13) 13(b)**
- **TC-004 International General Terms and Conditions of Purchase (04/13) 13(b)**
 - Goods are and only contain material from OM or OM Authorized source
 - Not be or contain Counterfeit items
 - Definition for Counterfeit Goods
 - DFARS 252.246-7007
- **TC Hardcode (12/13) (10)**
 - Notification and authorization if materials cannot be obtained from OM or OM Authorized Source
 - Flow down of counterfeit risk mitigation requirement to sub tiers
- **TC013 (12/11) Warranty For Goods Obtained From Brokers**
 - When used replaces Section 13 of TC-001 or TC-004
- **Quality Note WE**
 - Counterfeit Risk Mitigation using SAE AS5553 as a guide. (supplier & supplier sub tiers)
 - GIDEP participation monitor & acting on alerts
 - Communication details if procurement from other than OM or OM Authorized Source is required
 - Flow down of requirements

Ensure Requirements are Understood & Definitions Align

Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- **Supplier Engagement**
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



Example of welded lead replacements

Raytheon Expectations

- Establish a counterfeit prevention, detection and risk mitigation policy aligned with Industry and DoD requirements
- Robust, active obsolescence management
- Procure from OEM/OCM or their authorized resellers
- Use non-OEM/authorized sources ONLY for obsolete items
- Implement training and maintain counterfeit avoidance and detection competencies
- Robust supplier assessment and minimum quantity of independent distributors
- Specify and confirm counterfeit detection test and analysis requirements
- Monitor and report to GIDEP or regional equivalent
- Keep suspect counterfeit material out of the Supply Chain
- Measure, communicate and report
- Accept and meet DFARS 252.246-7007



**Counterfeit
Dust Cover**

Preferred Sources, Robust Counterfeit Prevention

Raytheon Enterprise Supplier Assessment (RESA)

\rē-să\ n 1. Enterprise process for assessing supplier capabilities, promoting educated and informed

decisions. 2. Assessments are a collaboration of Raytheon Supply Chain, Mission Assurance, Program Management and Engineering, along with our valued suppliers in an effort to mitigate risk and maximize performance.

Includes Eight Assessment Checklists

RESA Process and Tools

- ✓ Chapter 0: Quality Management Systems Audit
- ✓ Chapter 1: New Supplier Capability Assessment
- ✓ Chapter 2: Existing Supplier Capability Assessment
- ✓ Chapter 3: Supplier Total Business Assessment
- ✓ Chapter 4: Pre-work Authorization Review
- ✓ Chapter 5: Post-award Review
- ✓ Chapter 6: Periodic Total Business Assessment
- ✓ Chapter 7: Product and Process Verification
- ✓ **Chapter 8: Counterfeit Avoidance & Risk Mitigation**

Chapter 8, Counterfeit Avoidance & Risk Mitigation Focuses on:

- Industry Standards
- Raytheon & Regulatory Requirements
- Lessons Learned

Lessons Learned from Recent RESA Engagements

- OM / authorized sources
- Customer notification
- Awareness, training and expertise
- Due diligence
- Industry alerts
- Sub tier supplier assessment



Process Details and Sub Tier Assessment Are Key

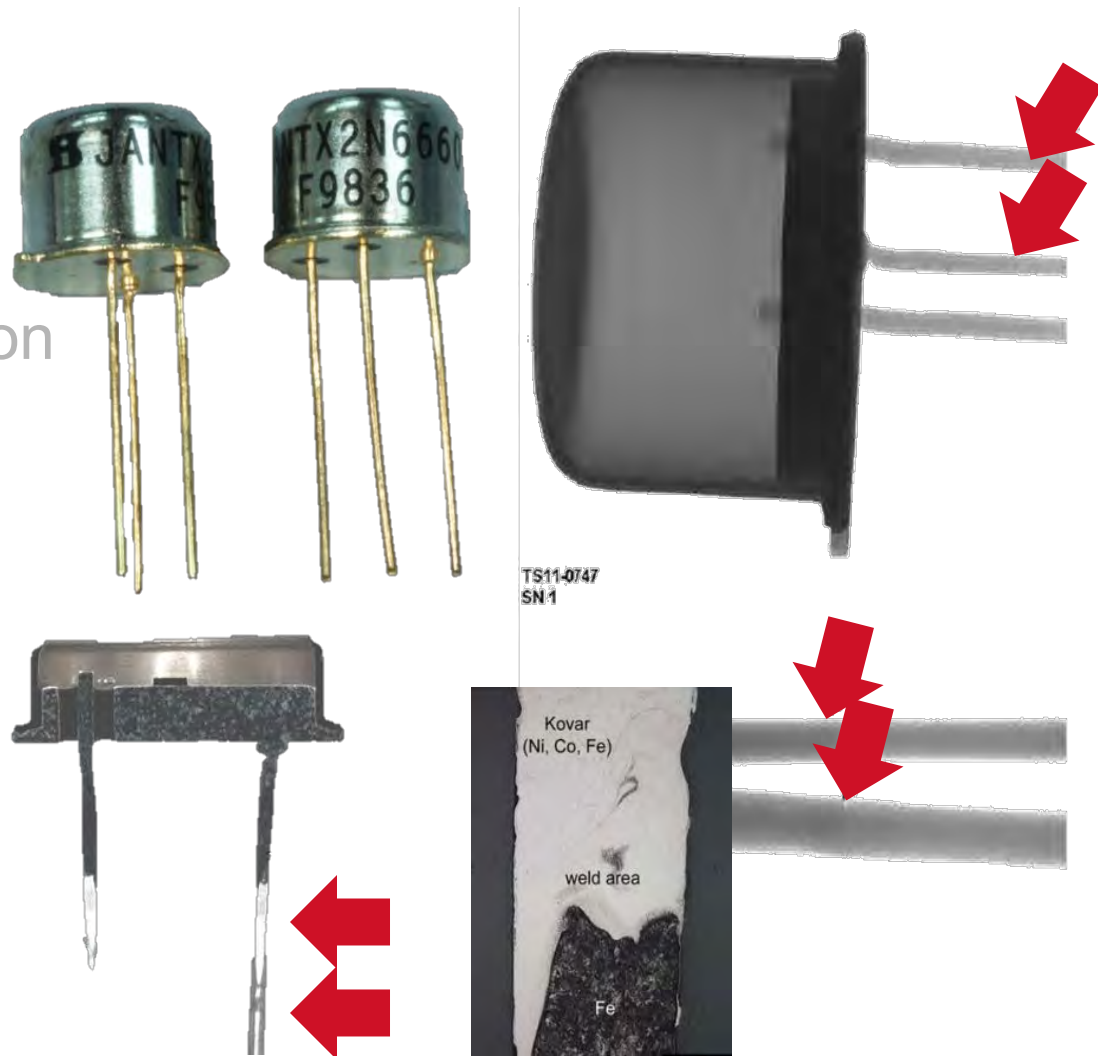
Supplier Assessment Resources

- SAE ARP 6178 Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors (2011)
 - Pre Assessment Information
 - Quality System and Processes
 - Supplier Qualification & Purchasing Process
 - Training & Certifications
 - Nonconforming Material
 - 160 Questions
 - Recommended Rating Criteria & MS Excel template allows for custom weighting
- Technical Operating Report 2014-02200 Counterfeit Parts Prevention Strategies Guide (2014) (Appendix G)
 - General Information
 - Parts Inspection, Verification & Handling
 - Nonconforming Material
 - Document Control & Record Retention
 - Liability & Disposition
 - 67 Questions
 - Guidance provided for each question
- Pre Assessment Information
- Warranty & Insurance
- Handling & Facilities
- Inspection & Test



Counterfeit Avoidance & Risk Mitigation

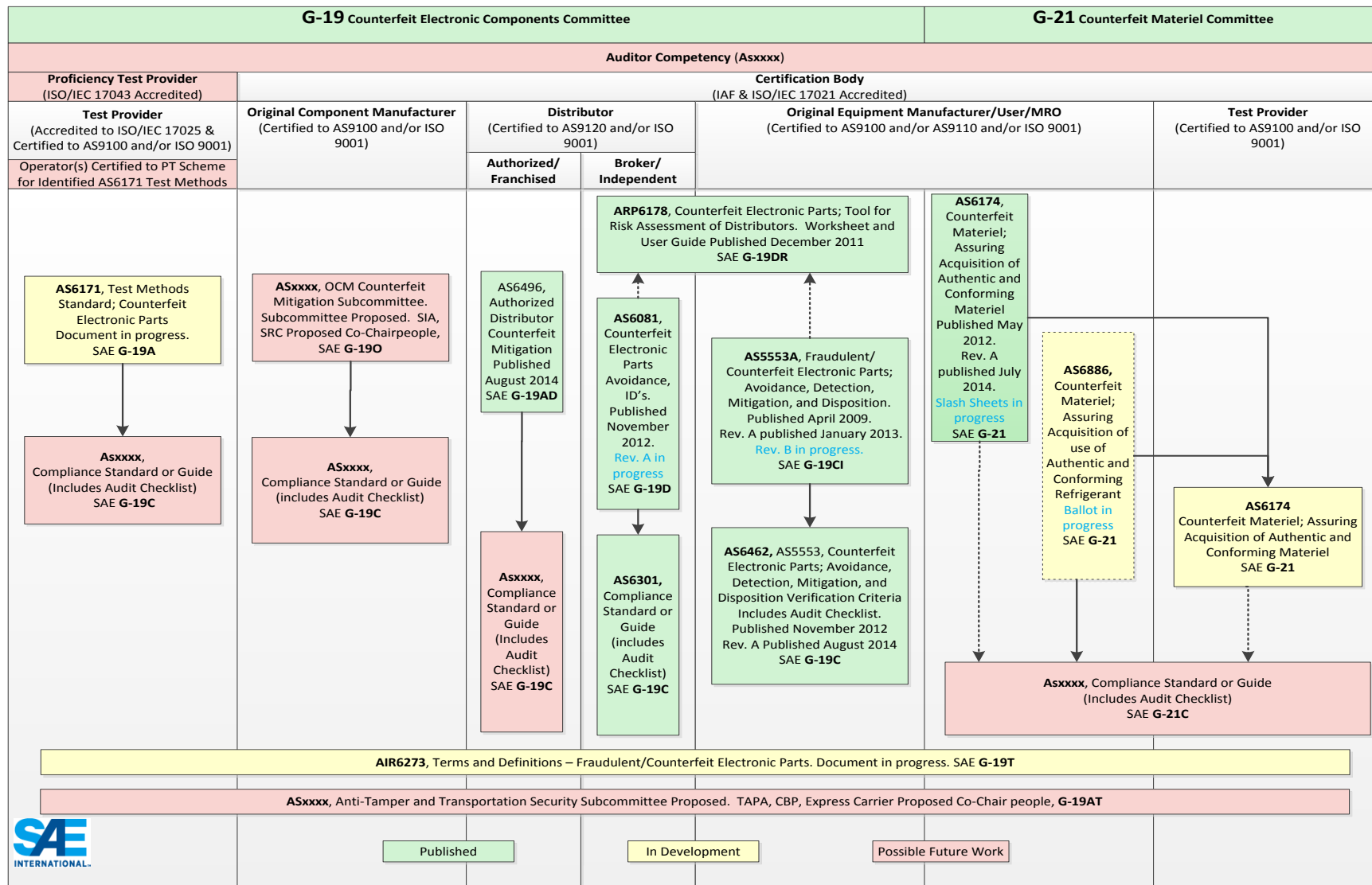
- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- **Standards & Resources**
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion



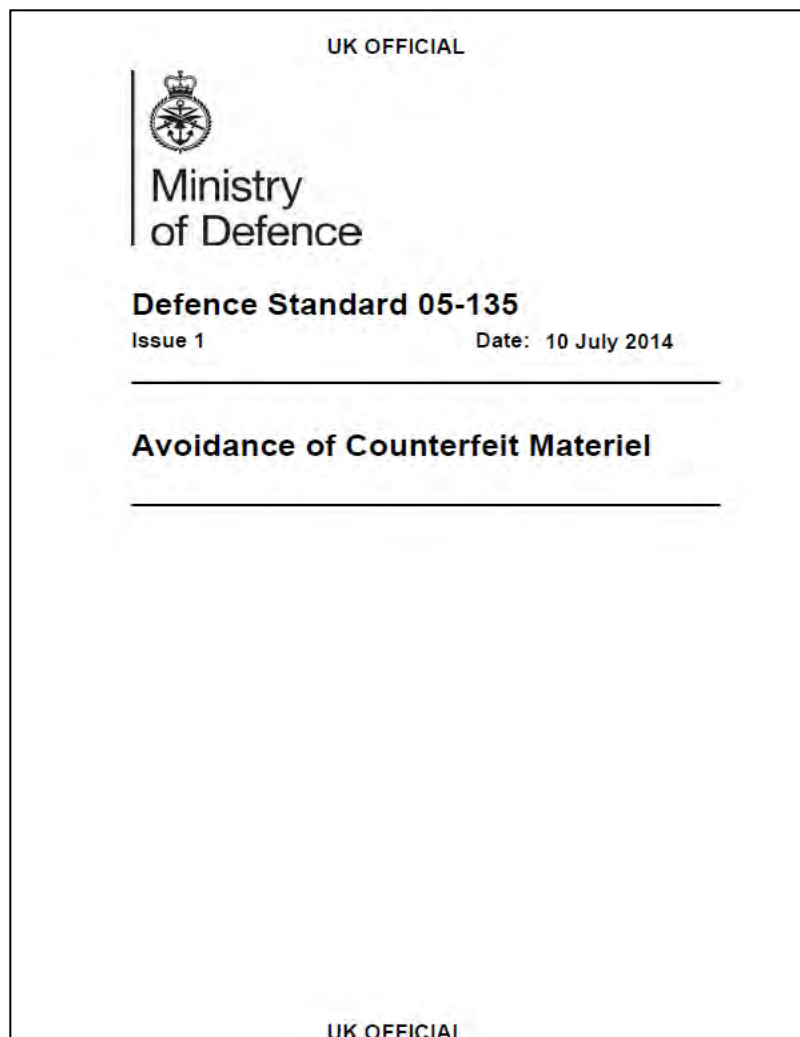
Example of welded lead replacements

SAE Standards Activity

SAE G-19 & G-21 Committee Products



UK Activity & Resources



Electronic Systems Community (ESCO) Anti-Counterfeiting Forum

- Potential Solution Providers
- Best Practices
- Suspect / Alleged Counterfeits
- Other Resources
- Push Mail

www.anticounterfeitingforum.org.uk

Additional Standards, Handbooks and Reports

NASA: MSFC-STD-3619 (2012)

- Electronics & Electromechanical
- Risk Assignment & Mitigation
- Test & Analysis, Photos

<https://standards.nasa.gov/documents/detail/3315823>

Electric Power Research Institute (EPRI)(2014)

Counterfeit and Fraudulent Items-Mitigating the Increasing Risk

- Power Generation Perspective
- Non Electronics Examples

www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=00000000001019163

Aerospace Industry Association Special Report (2011)

- Aerospace & Defense Focus

www.aia-aerospace.org/assets/counterfeit-web11.pdf

Technical Operating Report TOR-2014-02200 (2014)

- Space & Defense Aerospace Focus

library.mailbox@aero.org



Web Resources

SAE Aerospace Counterfeit Parts Portal



counterfeitparts.sae.org

International Aerospace Quality Group Supply Chain Management Handbook (SCMH) April 2014

- Industry Overview
- Definitions
- Risk Mitigation Strategies
- Key Control Processes for Mitigating Risk
- Training
- Obsolescence
- Procurement
- Product Verification
- Investigations
- Reporting

www.iaqg.org.scmh

Authorized Distributor Identification Resources

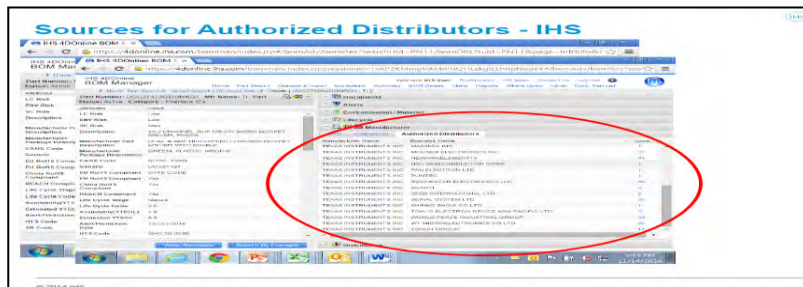
Web Services



<http://www.eciaauthorized.com/>

<http://www.sourceesb.com/>

Subscription Services



Siliconexpert Technologies

Product, Company, & Authorized Distributor Information

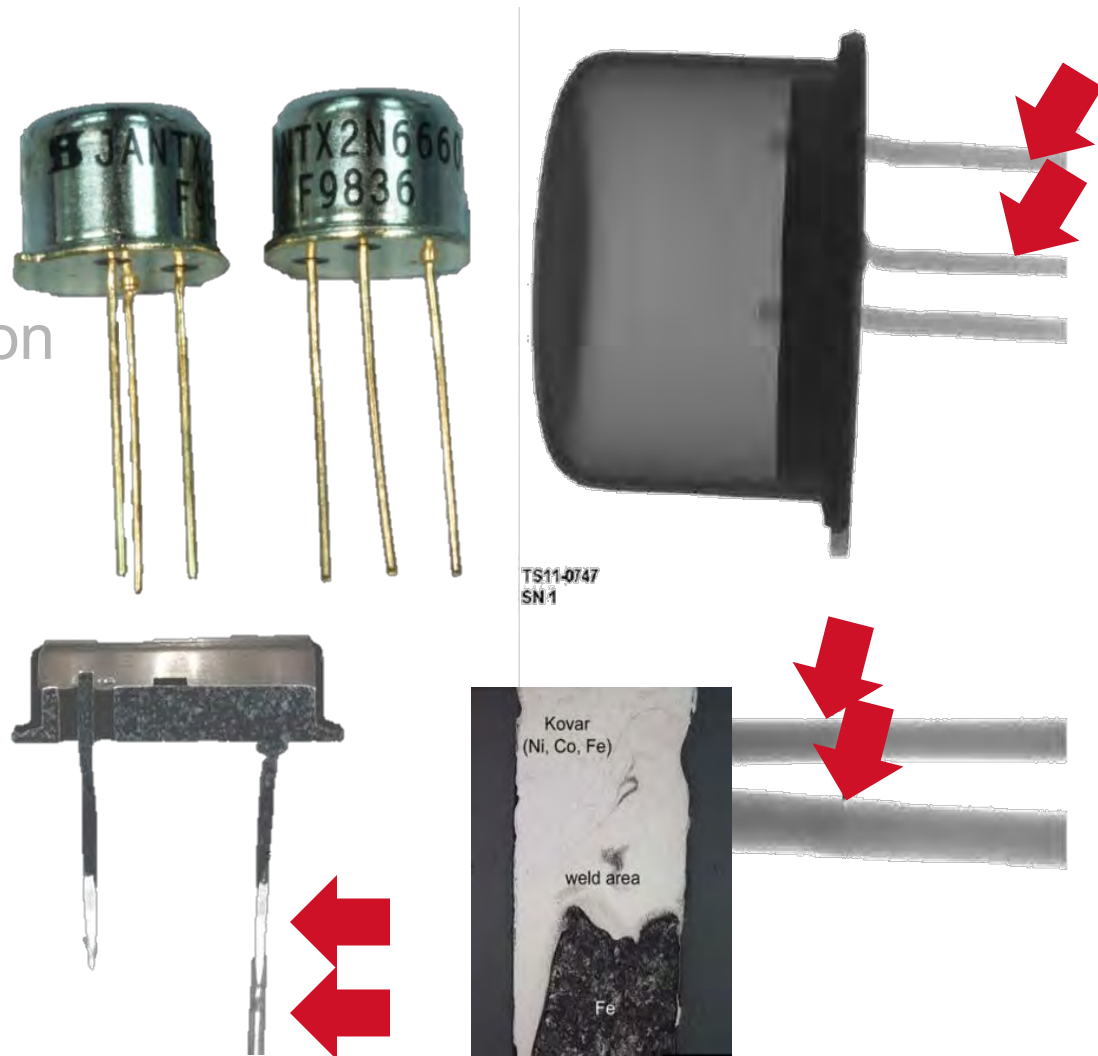
Counterfeit Risk Analysis

<https://www.ihs.com/products/caps-electronic-components.html>

<http://www.siliconexpert.com/>

Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- **Staying Informed**
- Training Resources
- Emerging Detection
- Conclusion



Example of welded lead replacements

Workshops and Symposiums

The screenshot shows the ERAI website's event overview page. At the top left is the ERAI logo. To the right are social media icons for Facebook, Twitter, LinkedIn, and Google+, along with a 'Sign In' button and a lock icon. Below the navigation bar is a blue banner with the text 'Conference 2015 Event Overview'. A left sidebar contains a list of links: 'Register Now', 'Event Overview', 'Conference Schedule', 'Speakers & Instructors', 'Downloads', 'Corporate Sponsors', 'Exhibitors', 'Testimonials', 'Hotel/Travel', 'Abstracts', 'Sponsorship Opportunities', and 'Exhibitor Opportunities'. The main content area is titled '2015 ERAI Executive Conference - Event Overview' and features a large banner for 'SUPPLY CHAIN SECURITY: A MOVING TARGET'. The banner includes the dates 'APRIL 22-23, 2015', the event name 'ERAI Executive Conference', and the location 'Bayfront Hilton, San Diego, CA'. Below the banner, there is a paragraph of text about the conference's focus on supply chain security, followed by a link to download the 2015 ERAI Executive Conference Brochure and a section titled 'How do you hit a moving target?' with a brief explanation of the concept.

erai

Home

Conference 2015 Event Overview

ERAI Executive Conference 2015

- Register Now
- Event Overview
- Conference Schedule
- Speakers & Instructors
- Downloads
- Corporate Sponsors
- Exhibitors
- Testimonials
- Hotel/Travel
- Abstracts
- Sponsorship Opportunities
- Exhibitor Opportunities

2015 ERAI Executive Conference - Event Overview

SUPPLY CHAIN SECURITY: A MOVING TARGET
Succeeding in the Age of Counterfeits, Cyber Attacks, Seized Shipments & Diminishing Resources

APRIL 22-23, 2015
ERAI Executive Conference
Bayfront Hilton, San Diego, CA

The ERAI Executive Conference is the premier gathering for individuals and organizations involved in the purchase, sale or use of electronic parts and/or assemblies.

Product seizures, tight budgets, reporting and other contractual obligations imposed by new and impending regulations have organizations of all types scrambling to meet ever-expanding customer expectations. Using this year's theme, "Supply Chain Security: A Moving Target", as our backdrop, ERAI has set the stage to cumulatively measure our industry's progress in the fight against counterfeit electronic parts while taking a deeper dive into the lesser-traveled territory of cyber attacks, talk of eliminating all surplus inventories from the open market and other security vulnerabilities.

[Click here to download the 2015 ERAI Executive Conference Brochure](#)

How do you hit a moving target?
Supply chain security is not static: it is a constantly moving and evolving target. To hit a moving target, you don't aim at where it is now; you

www.erai.com/conference_2015_event_overview

Workshops and Symposiums



Symposium on Counterfeit Parts and Materials
 June 23-25, 2015
 College Park Marriott Hotel and Conference Center
 College Park, MD

[Home](#) | [Call for Abstracts](#) | [Exhibitor Info](#) | [Hotel/Travel](#) | [Registration](#)

Organized by **SMTA** and **calce**

Event Sponsor:
AERI

Media Sponsors:
CIRCUITS ASSEMBLY
SMT

Technical Symposium: June 23-25, 2015
Workshops: June 25, 2015
Expo: June 23-24, 2015
 University of Maryland, College Park, MD

SMTA and CALCE @ University of Maryland are pleased to announce the east coast venue for the Symposium on Counterfeit Parts and Materials. The program will be held June 23-25 at the Marriott Inn & Conference Center next to the University of Maryland. Don't miss this opportunity to learn from and share your insights with government, industry and academia who are addressing the counterfeit problem.

Changes in electronic supply chain had been fast and furious in the last decades and its impact on the practices of companies is still evolving. It is well understood that, the scourge of counterfeit electronic parts is related to the changes in supply chain but it is only one of the many impacts. This symposium will provide a forum to cover all aspects of changes in the electronic parts supply chain on how an organization performs part selection and management through whole life cycle of the parts.

Going beyond anecdotes and examples of counterfeit parts, this symposium focuses on the solutions that are available and are under development by all sectors of the industry.

Topics will include:

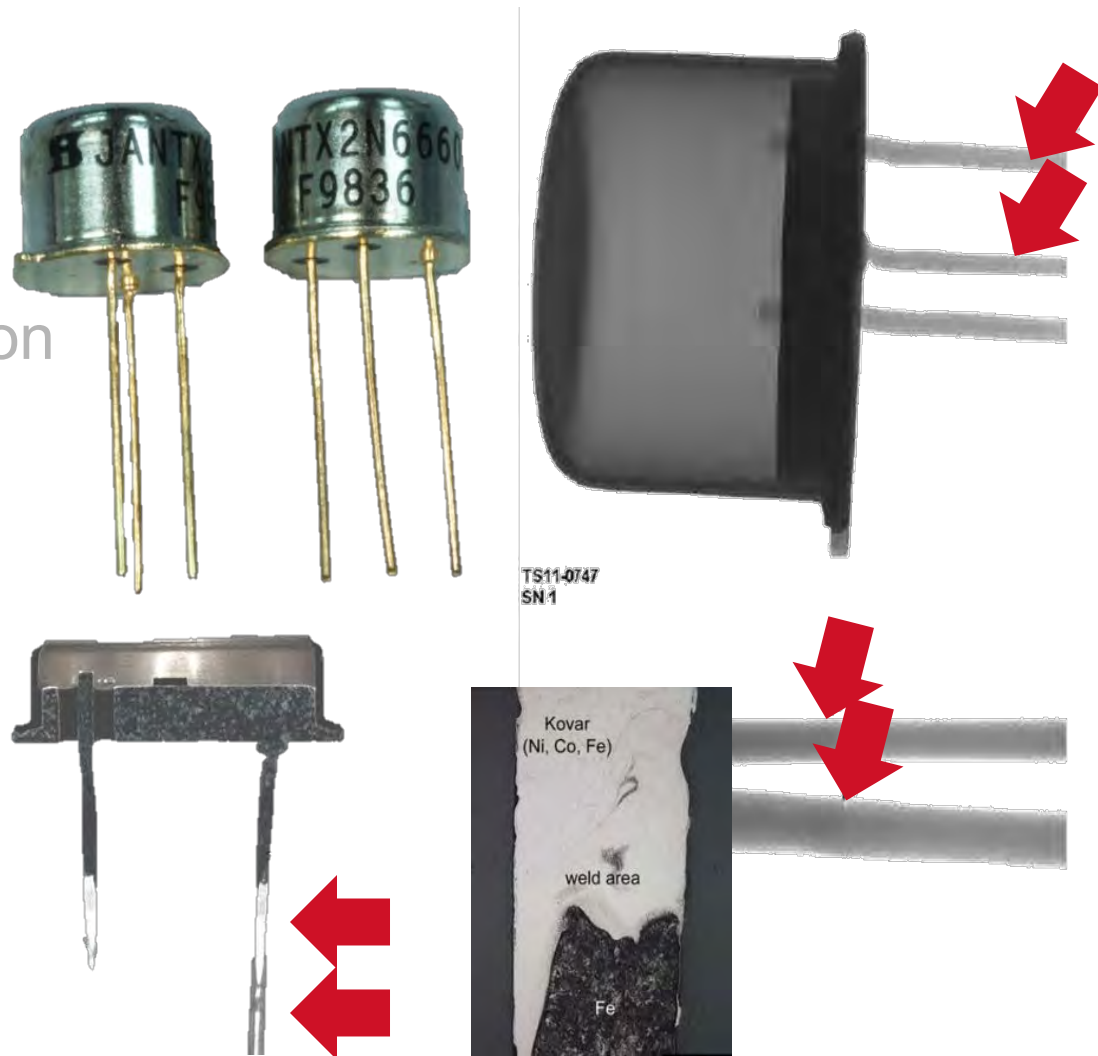
- Impact of supply chain changes on the component management practices: quality, reliability, manufacturability
- Electronic parts distribution: current stage and evolution
- Authentication techniques for securing electronic part supply chain
- Federal procurement practices and its impact on electronic supply chain
- Inspections tools and techniques for detecting counterfeit parts
- New areas of counterfeit concerns: materials, energy storage
- Industry and international working groups and standards on electronic part supply chain and counterfeit electronic parts

The symposium is organized by SMTA in conjunction with Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland, College Park, MD, USA. This symposium will be valuable to quality and reliability manager, supply chain managers, brand protection specialists, inspectors, marketing and procurement policy makers, contracts and legal management, security specialists and government agencies. Our focus is to provide relevant information to the professionals that can be used for solving problems today while planning for a different business and technology environment in the future.

www.smta.org/counterfeit

Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- **Training Resources**
- Emerging Detection
- Conclusion



Example of welded lead replacements

Training Resources

- Counterfeit Products Overview
 - Available on Raytheon Web Site under Supplier Connections



- Course Objectives

- Define counterfeit products and describe why they are a threat to Raytheon and our end users.
- List the most common ways counterfeit products are introduced into the product's lifecycle.
- Identify the proper mitigation strategies to reduce risks associated with counterfeit parts
- Define the roles and responsibilities associated with counterfeit risk mitigation and prevention.



Overview and Awareness Training

• <http://www.raytheon.com/media/modules/corpcou0012/sclist.htm>

Training Resources

- Defense Acquisition University
 - ❑ CLL 032 Preventing Counterfeit Electronic Parts from Entering the DoD Supply System (March 2014)
 - Types of Non Conforming & Suspect Counterfeit Items
 - How Counterfeits enter the supply chain
 - Economic Impact
 - Skills for identifying Counterfeits
 - Risk mitigation
 - Reporting
 - ❑ CLL 062 Counterfeit Prevention Awareness (March 2014)
 - Issues of Counterfeit Material
 - Impact on DoD programs
 - Means to Identify Counterfeits
 - Reporting and Disposition



Training Resources

■ Counterfeit Products Overview

- Materials available on NASA JPL Web Site
- Three Courses
 - Counterfeit Parts Awareness Basic
 - Counterfeit Parts Awareness Intermediate
 - Counterfeit Parts Inspection Training



Counterfeit Parts Awareness - Basic

Description:

The spread of counterfeit electronic components continues to grow within the global supply chain and has penetrated various governmental agencies, including NASA and the US Department of Defense. The risk of counterfeit electronics being used in military equipment prompted an i Services Committee and aggressive legislation Authorization Act. NASA is responding to the iss Act S.3729, authorizing NASA to plan, develop a detect, track, catalog and reduce the number of NASA supply chain.

This is an introductory awareness class. Objecti

- gain a basic understanding of the electron
- gain basic knowledge of the supply chain
- gain familiarity with some of the methods
- examine risk mitigation steps
- Review verification and inspection proces parts

This course uses IDEA-STD-1010-B, AS5553 St Parts; Avoidance, Detection, Mitigation, and Dis Parts Policy and the JPL Counterfeit Electronic P Rules #78395 as references.

Prerequisite: None

Length: Approximately 4 hours

Here is the link to the training material: [COUNTERFEIT PARTS AWARENESS TRAINING_Basic.pptx](#)

Counterfeit Parts Awareness - Intermediate

Description:

This is a follow-on course to the Objectives include the following:

- Explore concepts regarding inspection (concepts introduc
- Present guidance for supp
- Examine the concept of pa parts risk
- Overview of pertinent Unit

Prerequisite: Counterfeit Par

Length: Approximately 4 hou

Here is the link to the training m [TRAINING_Intermediate.pptx](#)

Counterfeit Parts Inspection Training

Description:

This is a follow up class to the JPL Counterfeit Parts Awareness Class. Objectives include the following:

- Gain in-depth knowledge of inspection tools and equipment used for part authentication
- Gain hands-on experience inspecting actual electronic components

Attendees will inspect actual parts and gain equipment knowledge through videos and actual demonstrations.


Prerequisite: Counterfeit Parts Awareness - Basic

Length: approximately 4 hours


Here is the link to the training material: [COUNTERFEIT PARTS AWARENESS TRAINING_Inspection.pptx](#)

Training Resources

- Counterfeit Parts Definitions & Origins
- MDA Documents & Supplier Definitions
- MDA Experience with Counterfeits
- DoD Requirements






Training Objectives



- **Become aware of the counterfeit parts risk.**
- **Learn about MDA requirements, and the impact of counterfeit parts to MDA.**
- **Understand the mission impact from counterfeit parts or equipment.**
- **Realize the need for rigorous parts control and procurement vigilance against these threats.**
- **Learn about counterfeit part types, and how to detect and report them.**
- **Learn what MDA and the Department of Defense (DoD) are doing about the problem.**

Note: This document contains both DoD-specific and commercial data.

MDA COUNTERFEIT PART TRAINING

AVOIDANCE, DETECTION, CONTAINMENT, AND REPORTING

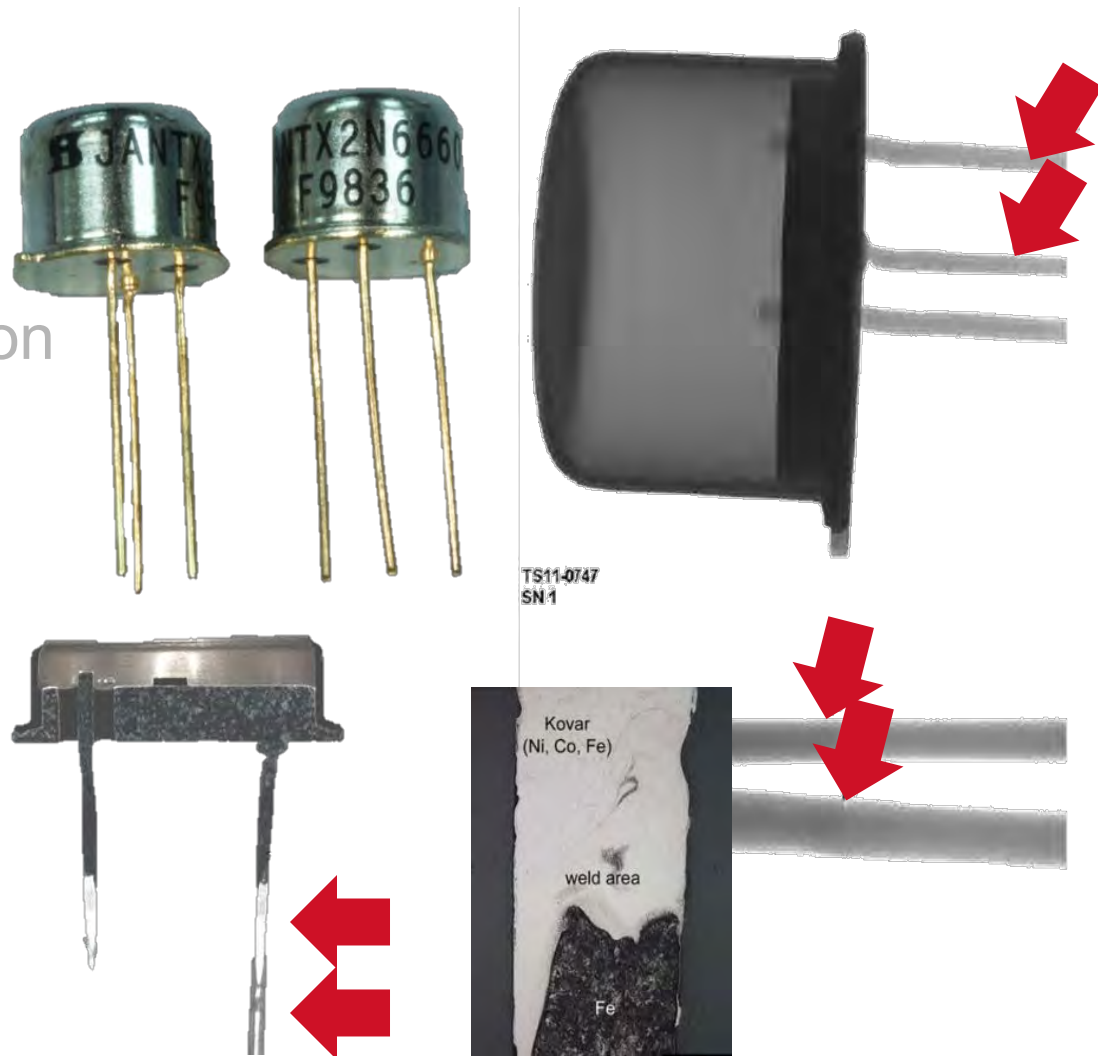
Approved for Public Release
13-MDA-7645 (11 December 13)
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

December 11, 2013

- MDA Requirements & Recommendations
- Counterfeit Part & Material Examples
- MDA Contractor Audits
- Included as Appendix A of TOR 2014-02200

Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- **Emerging Detection**
- Conclusion



Example of welded lead replacements

DARPA Shield

- SHIELD aims to develop tiny components, known as dielets, that could be added to electronics parts during manufacturing or in another trusted setting. The dielets won't have an electronic connection to the parts—and thus wouldn't affect their functionality—but they would have an encryption engine and sensors that would detect tampering, such as revealing an exposure to light if the device had been opened up at some point between manufacture and delivery
- With the SHIELD program, DARPA wants to develop dependable but inexpensive hardware dielets—costing less than a penny each—that could be scanned from a handheld device or larger device for large shipments. Following a scan, a handheld device such as a smartphone would communicate with the dielet, which would then send an encrypted message with information from its sensors. That response would show if any tampering occurred
- Over \$24M in Phase 1 contracts awarded between December 2014 and February 2015
- As of Feb 2015
 - Charles Stark Draper Laboratory \$4.0M (12/2014)
 - University of Illinois \$0.5M (01/2015)
 - Northrop Grumman \$12.2 + (01/2015)
 - SRI International \$6.8M + (01/2015)
 - University of California Berkley \$0.7M (01/2015)
- See DARPA Broad Agency Announcement DARPA-BAA-14-16 for additional details

	Phase 1 18 Months Fundamental Tech Developmt	Phase 2 18 Months Design Integ. HW Build	Phase 3 12 Months Demo, Test, Evaluation
Tech Area 1 Technology	X		
Tech Area 2 Design & Integr	X	X	
Tech Area 3 Deployment	X	X	X

DNA Marking



applieddnasciences

our company ♦ investor information ♦ products ♦ applications ♦ make an appointment

Or call our general information line

Our technology support staff will direct you to a person who can help with all your questions and needs.

Get Started

SIGNATURE® DNA

f in **Twitter** **Email** **RSS** **fr**

SigNature®
the ultimate reality check

SigNature® DNA markers provide a unique and powerful means to authenticate originality, verify provenance, and link offenders and stolen items to crime scenes. With essentially infinite variability, individualized custom DNA sequences can be created and embedded into a range of host carriers such as ink, varnish, thread, laminates and metal coatings. Highly secure, robust, durable and cost-effective, SigNature DNA markers can be used as a forensic complement to barcodes, watermarks, holograms, RFIDs, microdots or any other security platform.

Latest News

[Applied DNA Sciences Launches DNA Taggant and On-Site Authentication for Pharmaceuticals](#)
Multiple Trials Demonstrate that SigNature® DNA Inclusion in Drugs Provides Forensic Proof of Authenticity Seamlessly from Supply Chain to Consumer

[Applied DNA Sciences Announces SigNature® DNA Compliance with FDA Guidelines](#)
Regulatory Firm of Covington & Burling Completes Their Review of the Regulatory Status of DNA Taggants


Source **Extraction** **Ligation** **Encryption** **Reassembly** **Replication** **Deployment**

SigNature DNA markers are based on full, double-stranded plant DNA. These engineered marks have not and cannot be broken. The conventional process used to sequence ("decode") native DNA is not possible with the engineered mark. Additional layers of protection and complexity are added to the mark in a proprietary manner. This botanically engineered solution is shielded by a portfolio of 24 patents, 58 patent applications, and other intellectual property protection.

RF Emissions Analysis

NOKOMIS
Supporting America's Advanced Technology

Home About Us Products Services News Employment Contract Vehicles Contact Us



< Products

Advanced Detection of Electronic Counterfeits (ADEC)

ADEC passively captures Electromagnetic (EM) signatures radiated by electronic components in order to automatically detect and identify counterfeit components. The ADEC System counterfeit detection modality is highly autonomous; non-contact and non-invasive; and has a high confidence rate of detection of counterfeits with a low false positive rate. Through early detection and screening of counterfeit parts the ADEC System prevents system failures, significant delays and redesigns and cost escalation. Updates and additions to the ADEC component signature library require a simple software upgrade and are fast and secure.

The Advanced Detection of Electronic Counterfeits (ADEC) System consists of two primary components: The ADEC Sensor and the Integrated Antenna Enclosure (IAE). Key Benefits of the ADEC System include:

- Detects electronic counterfeits and verifies part authenticity
- Detects anomalies in parts
- Enhances military capability by removing substandard electronics from weapon systems
- Prevents system failures, significant delays and redesigns and cost escalation

<http://www.nokomisinc.com/adec.html>

Surface Analysis

QuanTEK



“Tag-less” track and trace solution

Mitigate threats from counterfeit items in your supply chain.

Addresses the six high-risk Federal Supply Groups (FSG's) identified by the US Defense Logistics Agency.

- Electrical and Electronic Components (FSG 59)
- Engine Accessories (FSG 29)
- Pipe, Tubing, Hose, and Fitting (FSG 27)
- Hardware and Abrasives (FSG 53)
- Vehicular Equipment Components (FSG 25)
- Bearings (FSG 31)

BROAD APPLICABILITY



Value Proposition

Based on mature image capturing optical technique

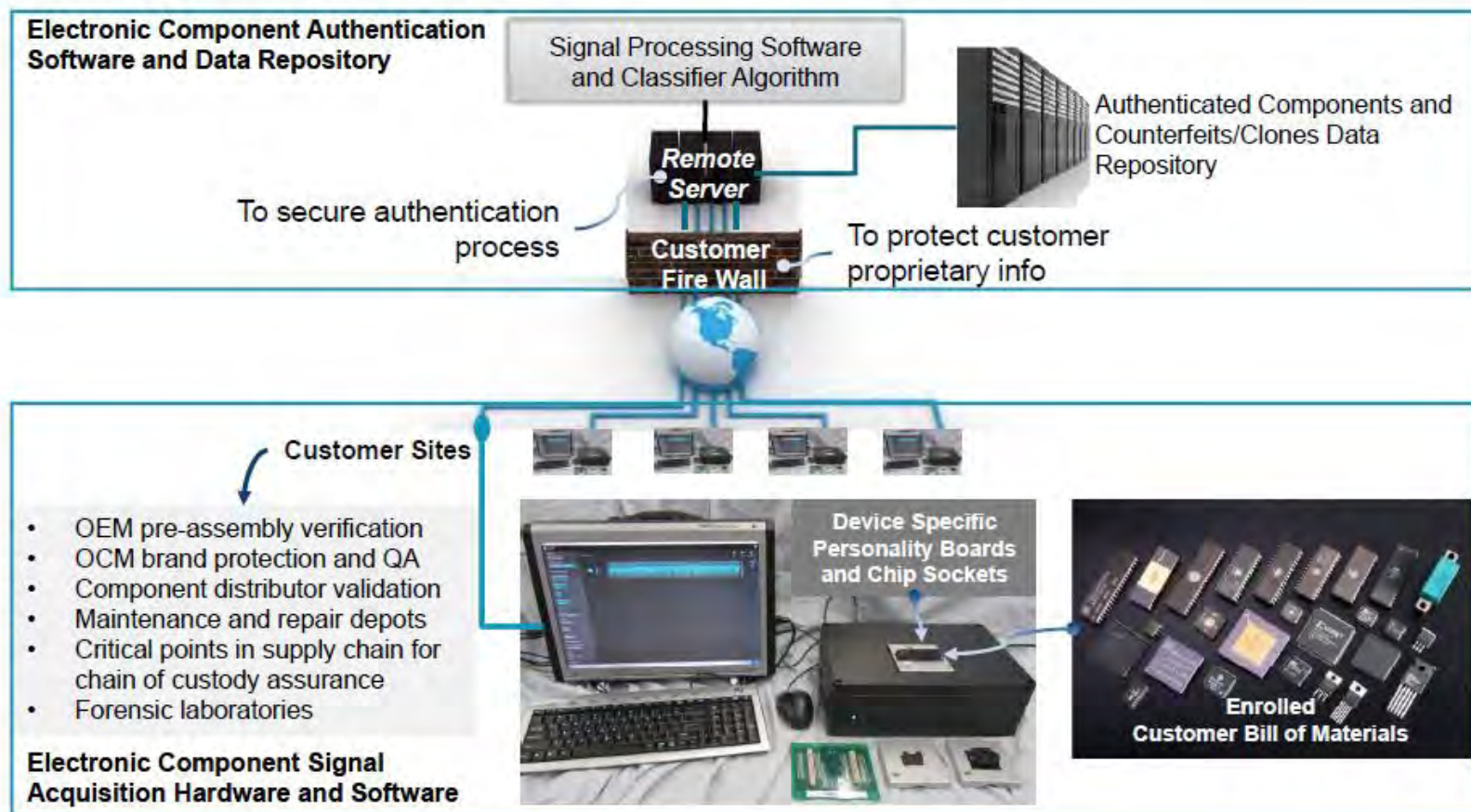
- Non-contact and “tag-less” – avoids handling and warranty issues
- Rapid on-site enrollment/authentication
- Easy to operate; requires minimal training
- Integrate easily with manufacturing workflows (high and low throughput)



COVISUS - A CHROMOLOGIC COMPANY

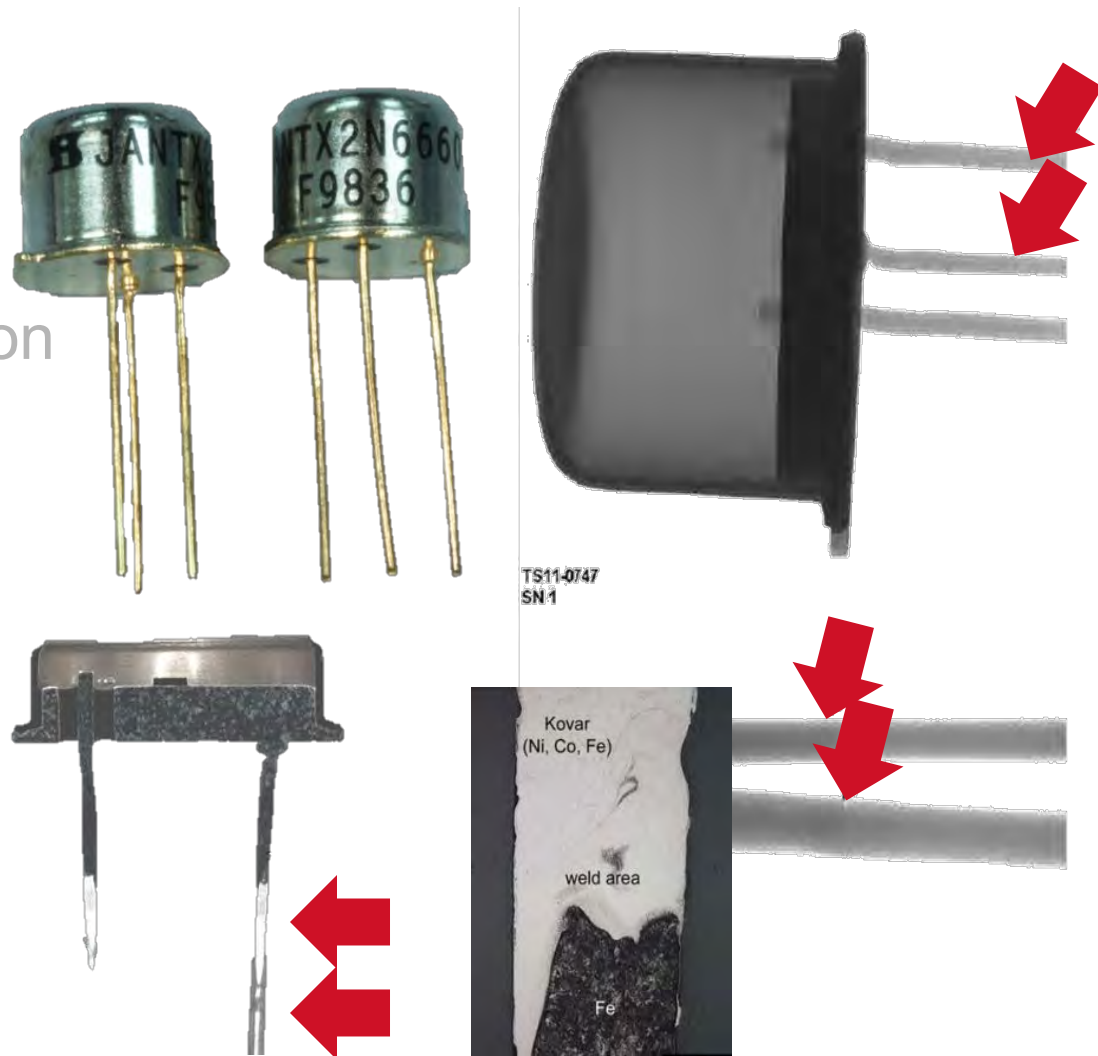
Battelle Memorial Institute - Battelle Barricade™

What is Battelle Barricade™?



Counterfeit Avoidance & Risk Mitigation

- Definition(s)
- The Risk
- U.S. Regulatory Activity
- Counterfeit Risk Mitigation
- Supplier Engagement
- Standards & Resources
- Staying Informed
- Training Resources
- Emerging Detection
- Conclusion




Example of welded lead replacements

Why are Brokers Used?



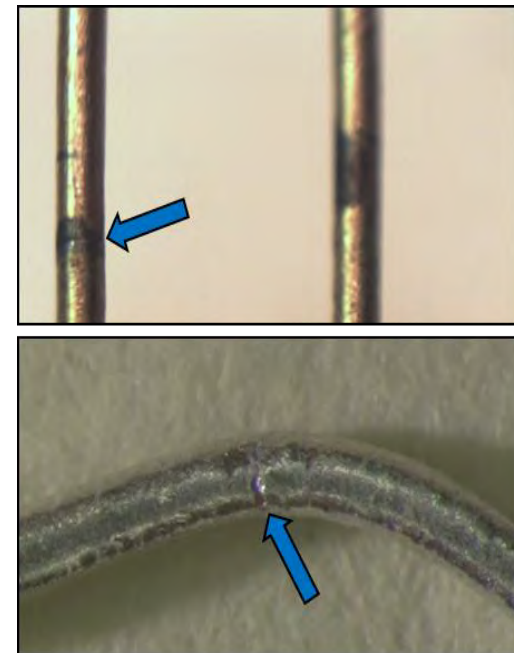
Why is a Broker Used?



The Item is
Obsolete

Main Take Aways

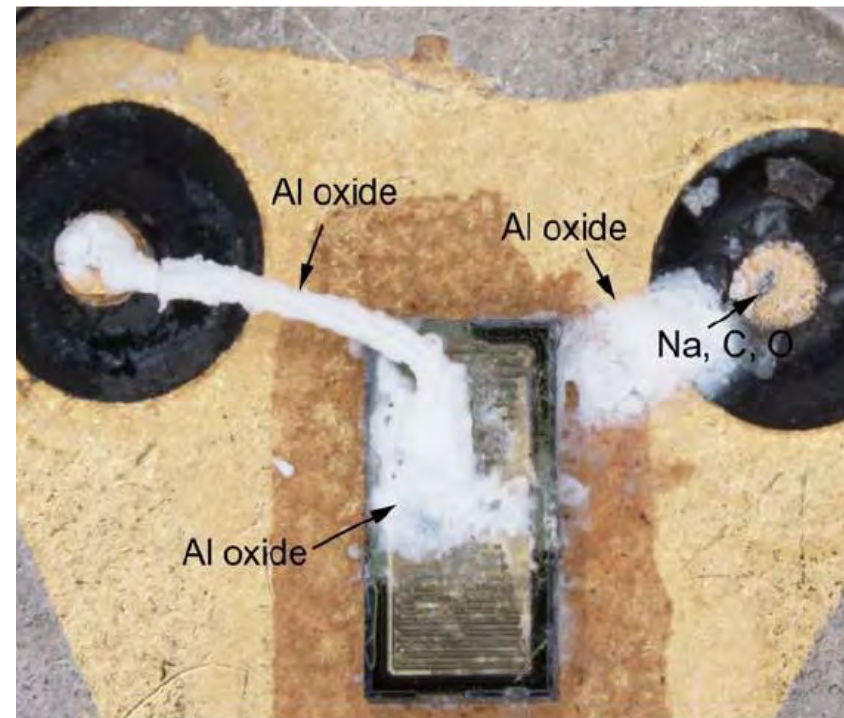
- Awareness & Training
- Obsolescence Management.
- Procure ONLY from OM / OM franchised.
- Sub tier awareness, flow down and process effectiveness.
- Broker procurements ONLY when OM / Franchised no longer support.
- Know if Broker material is going to be used.
- Broker procurements MUST have robust risk mitigation.



Examples of devices with welded lead replacements

Conclusion

- Regulatory environment evolving
- Focus on counterfeit risk avoidance
- Partnering vital to success
- Standardization, processes, reporting
- Companies aligning with regulations
- U.S. DoD, industry working on standards, prevention



Partnering Across Industry for Mutual Success