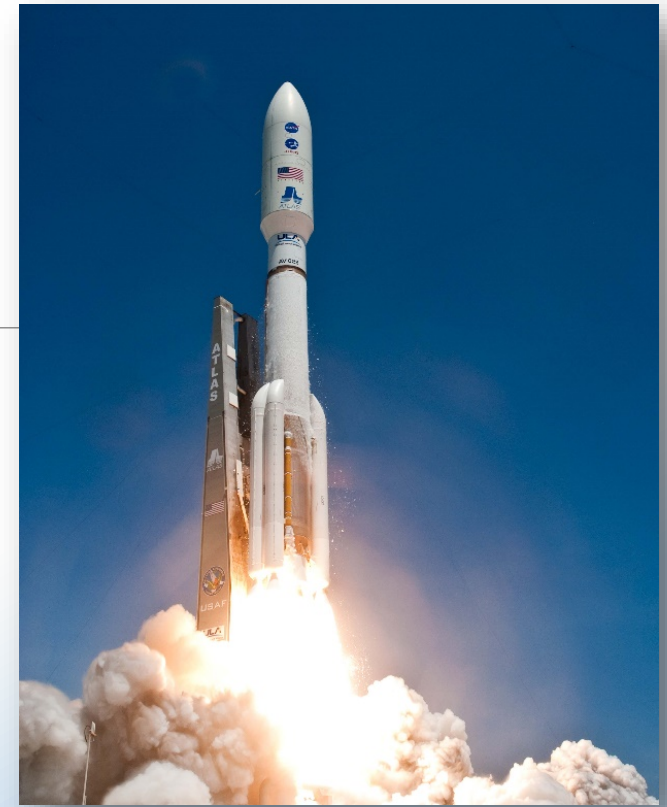




NASA Counterfeit Parts Awareness and Inspection



JERRY MARTINEZ

JET PROPULSION LABORATORY, CALIFORNIA INSTITUTE OF TECHNOLOGY

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology.



Training Course Objectives

This course provides a high-level overview of counterfeit concepts related to government and industry best practices:

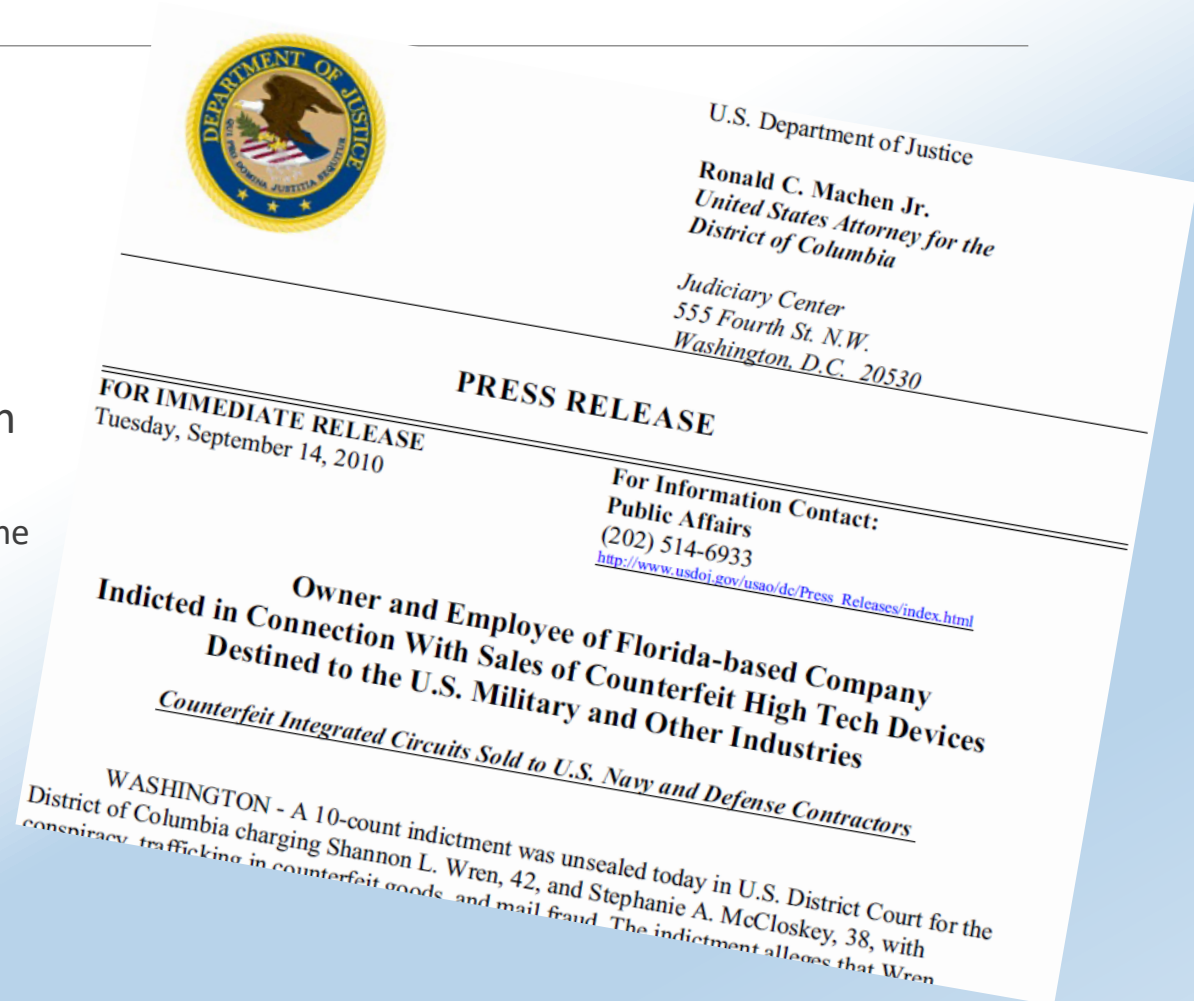
- Gain an understanding of the EEE parts counterfeit problem
- Discuss the problems faced in the supply chain environment
- Develop a familiarity with some of the methods to counterfeit material
- Learn the major steps of a risk mitigation procedure
- What you can do to avoid counterfeits



The Counterfeit Problem

Independent distributor VisionTech Components, caught 2010

- Clearwater, FL
- Nine employees
- Distributor sold ICs for over a five-year period
- Imported 95% of their parts from a single supplier in China through various U.S. ports
 - 3,263 shipments (59k parts) often changing the name of what they were importing
 - 35 shipments were stopped by Customs and Border Protection, analyzed, and determined to be counterfeit
- ICs sold as “military grade” from Germany but were counterfeits from China
- Sold large amount of semiconductor chips to 1,100 customers
 - Sold to every sector, most of devices have not been recovered



Source: Criminal Case 10-245-PLF



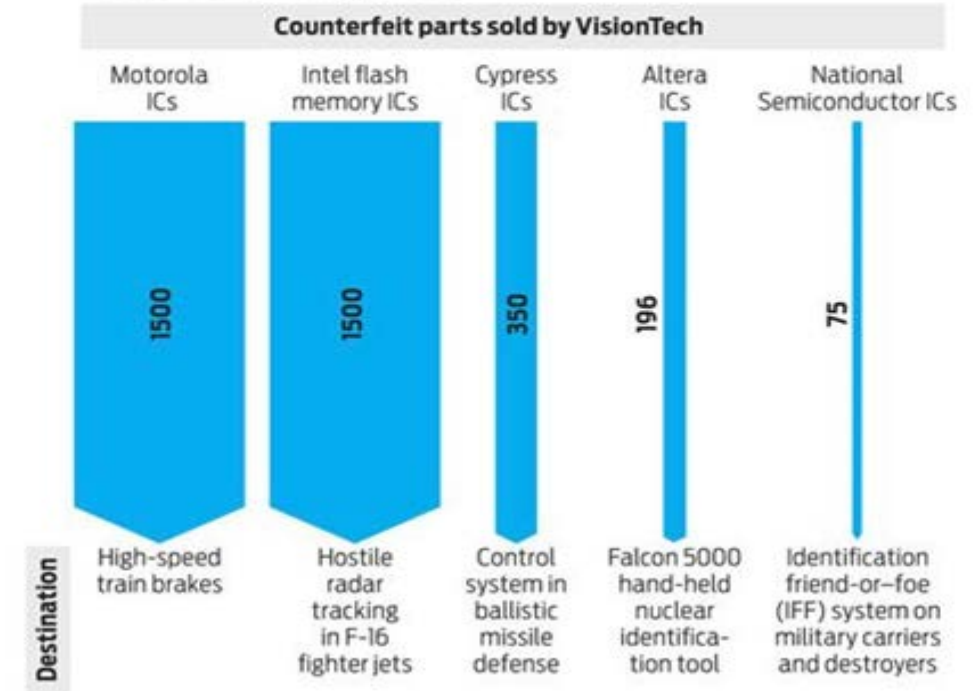
Why is it a problem?

Where did those fake parts end up?

- Hostile radar tracking in F-16 fighter jets
- High-speed train brakes
- Control system in ballistic missile defense
- Falcon hand-held nuclear identification tool
- IFF system on military carriers and destroyers

A Case Study in Fake Chips

In 2010 the United States prosecuted its first case against a counterfeit-chip broker. The company, VisionTech, sold thousands of fake chips, many of which were destined for military products.

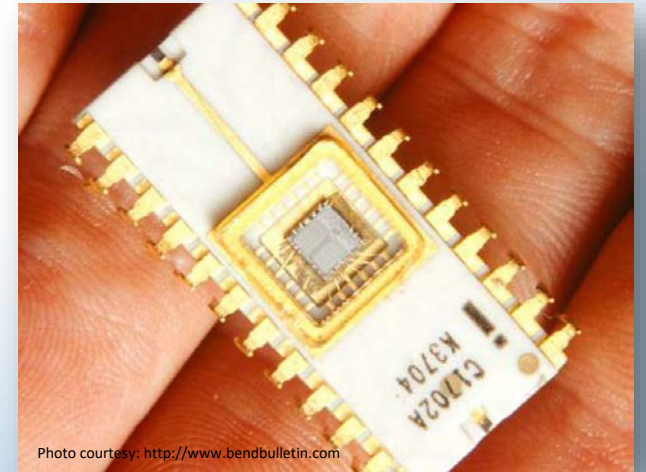


Source: Sentencing memo, *United States of America v. Stephanie A. McCloskey*, filed 7 September 2011



Why is it a problem?

- VisionTech received \$16 million in payments
 - Had spent \$7.5 million for purchase of parts
 - Had spent \$14,742 on testing parts
- Baited and switched good samples for companies to test
 - Good returned chips were provided to another customer
- Devices showed signs of blacktopping, incorrect P/Ns and date codes
 - Used Armor All to make parts appear shiny
 - One VisionTech employee e-mailed a counterfeiter to use “stronger ink” and use acetone to “make sure the ink does not come off” because their customers were “beginning to use acetone on all parts”
 - Forged CofCs
- Employees were both arrested in Florida
 - Police seized luxury vehicles, motorcycles, motor home, beach home, and four other properties





Reality of Counterfeiting

Massachusetts Man Sentenced to 37 Months in Prison for Trafficking Counterfeit Military Goods

<http://www.justice.gov/opa/pr/massachusetts-man-sentenced-37-months-prison-trafficking-counterfeit-military-goods-0>

New Jersey Man Admits Smuggling \$65 Million in Sensitive Electronic Components to Russia's Ministry of Defense

<http://www.justice.gov/opa/pr/new-jersey-man-admits-smuggling-65-million-sensitive-electronic-components-russia-s-ministry>

Texan gets 10 years in U.S. prison for Russian tech export scheme

<http://www.reuters.com/article/us-usa-russia-fishenko-idUSKCN1012ML?il=0>

Counterfeiters Will Become 'Virtual Criminal Underground:' Europol

http://www.ebnonline.com/author.asp?section_id=3788&doc_id=278060

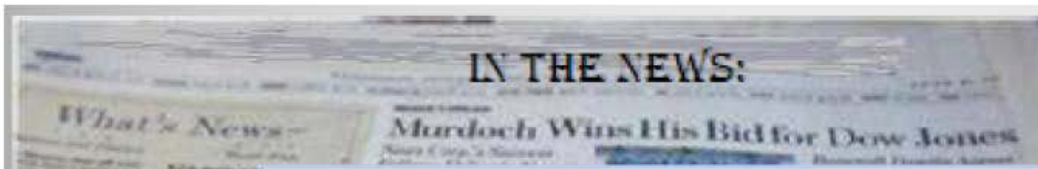
History of Pre-Infected Electronics Will Block China's Bid to Purchase Micron Technology

<http://www.theepochtimes.com/n3/1463955-history-of-pre-infected-electronics-will-block-chinas-bid-to-purchase-micron-technology>

Company news: Amazon Project Zero—Empowering brands to drive counterfeits to zero

<https://blog.aboutamazon.com/company-news/amazon-project-zero>

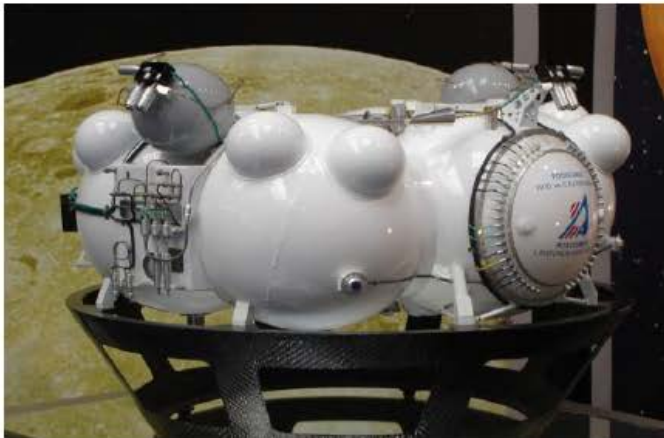




IEEE Spectrum Tech Alert [Did Bad Memory Chips Down Russia's Mars Probe?](#)

IEEE report blames the loss of Russia's ambitious Phobos-Grunt space mission on faulty memory chips ... **report suggests that the chips were counterfeits** that had been intentionally misrepresented as offering higher performance than they were actually capable of.

Report cites malfunctioning WS512K32 chip (a single-package assembly of *static random access memory (SRAM)* chips) suspected to be counterfeit



Mockup of Phobos-Grunt main propulsion unit



Reality of Counterfeiting—How Far Do The Counterfeiters Go

- In 2004, NEC started getting unusual product returns and reports of suspect counterfeit products
- A two-year investigation found over 50 factories, many bearing NEC logos, in China and Taiwan manufacturing fake NEC products—including products the real NEC didn't make
- Employees had NEC business cards and thought they worked for the real NEC
- Apple “Stoers” have also been faked



Photo courtesy of: www.cracked.com



Photo courtesy of: www.nytimes.com



Section 1 – the Landscape of the Counterfeiting Issue



Which term to use?

COUNTERFEIT ELECTRONIC PART

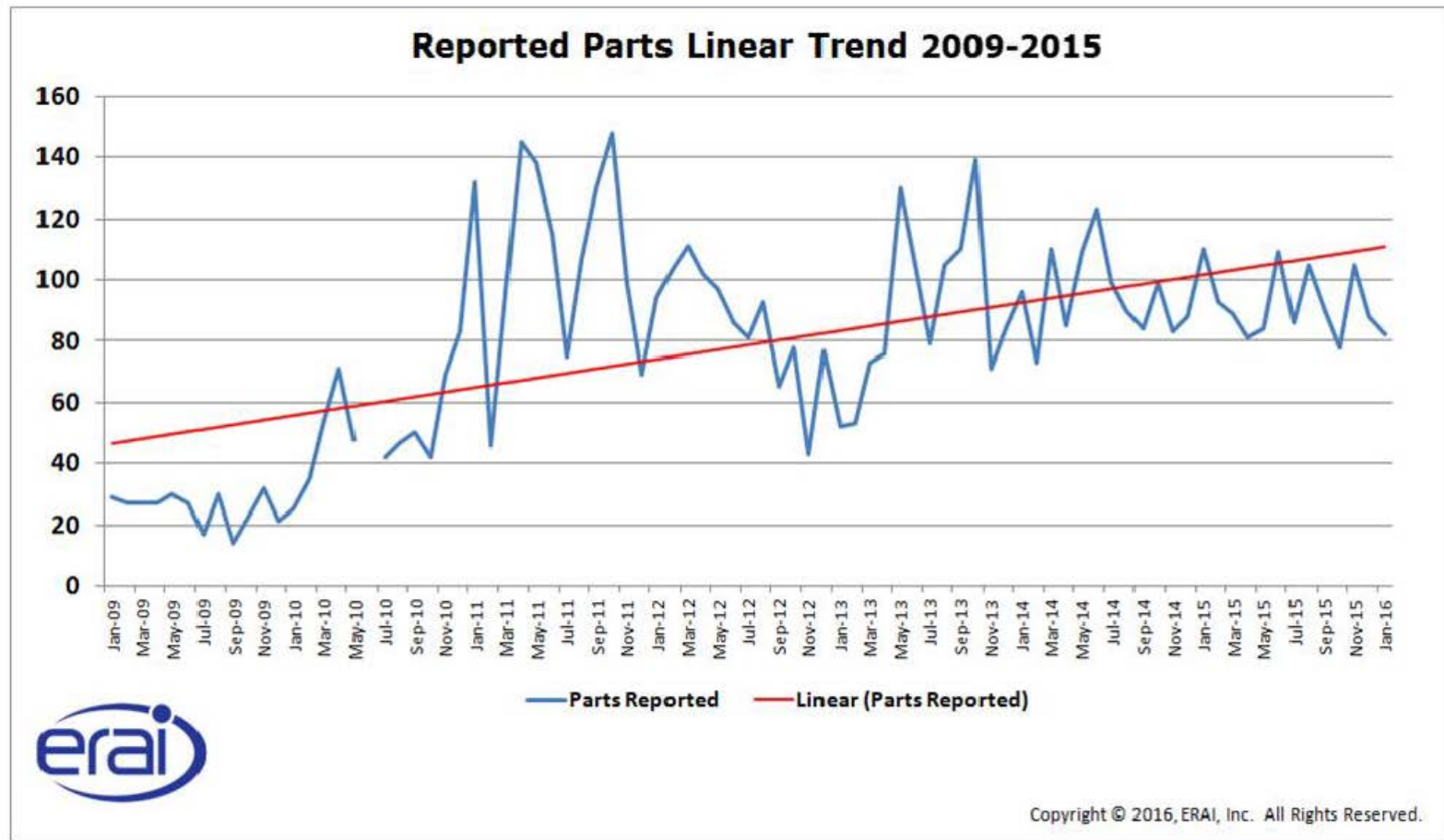
An unlawful or unauthorized reproduction, substitution, or alteration that has been **knowingly** mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer.

SUSPECT COUNTERFEIT ELECTRONIC PART

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.

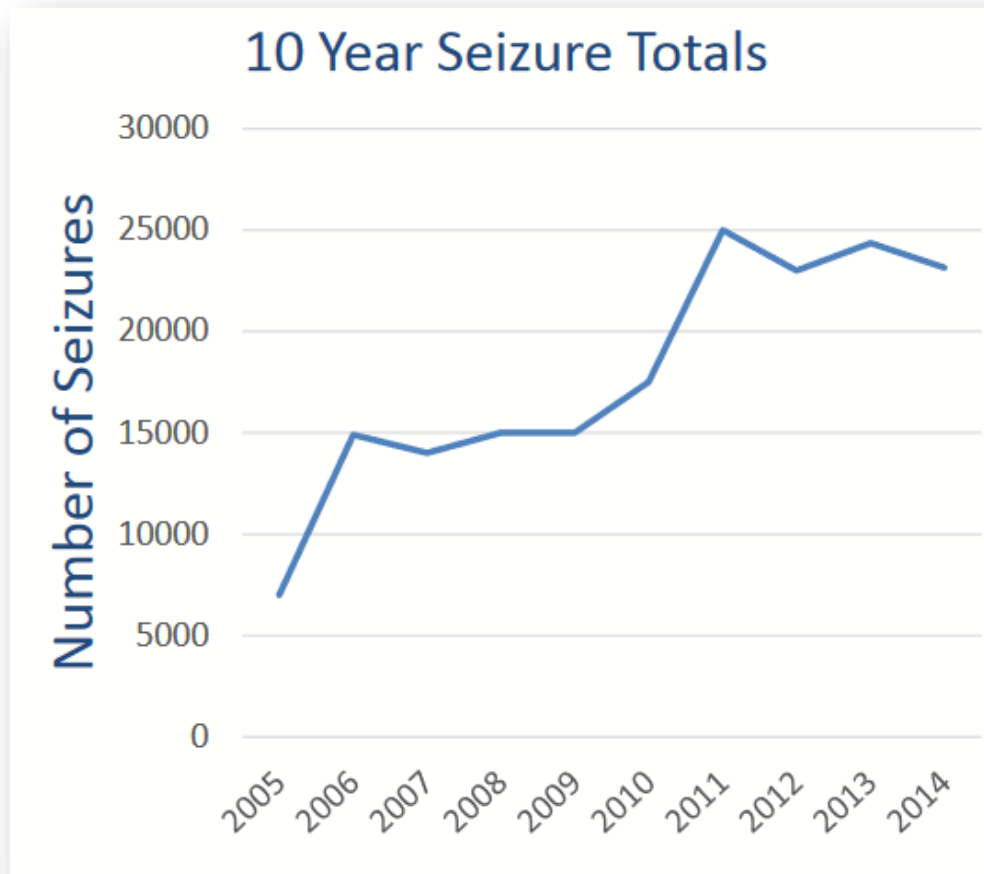


An Increasing Threat





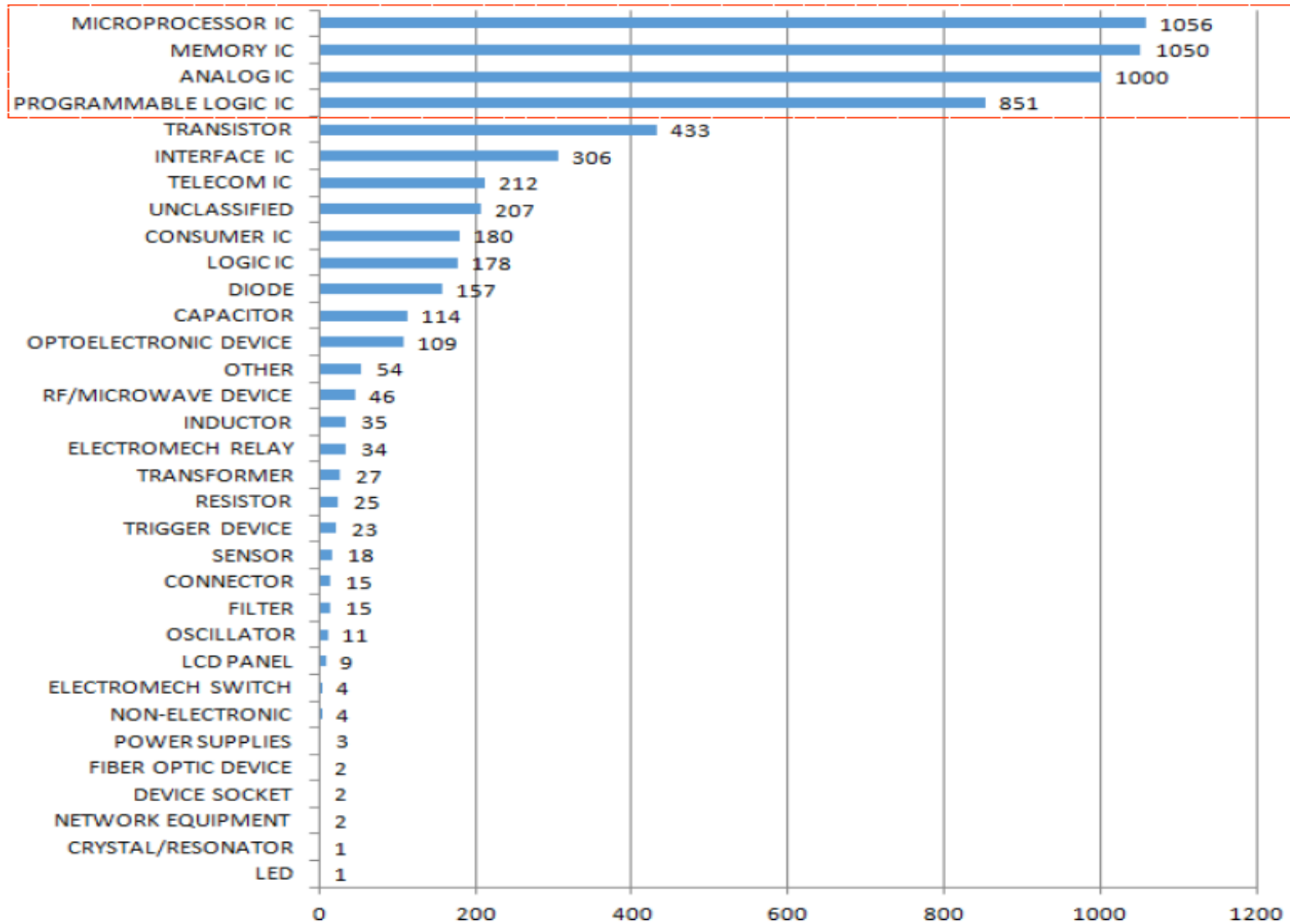
Total # of counterfeit seizures



- Since 2009, counterfeit seizures have increased 40%
- Semiconductor enforcement focus led to 5% increase in seizures
- 23,140 seizures in FY2014
 - seaports, land borders, air, cargo, mail



Types of Parts Reported by ERAI in 2010-2015

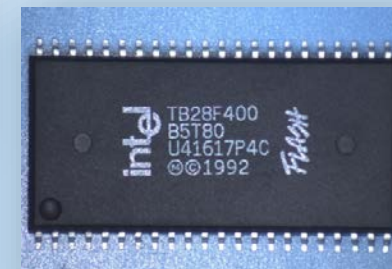


Copyright © 2016, ERAI, Inc. All Rights Reserved



Integrated Circuit (IC)

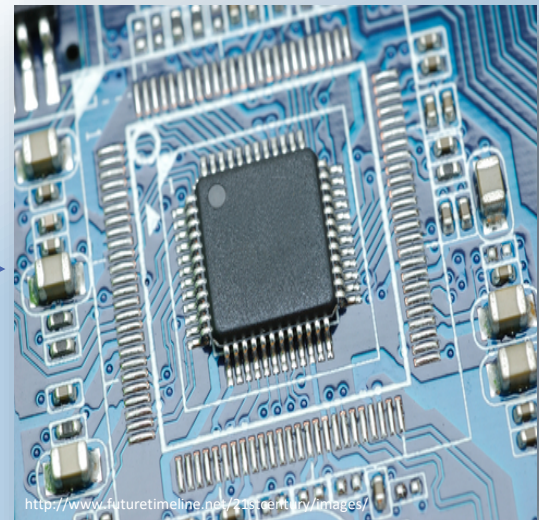
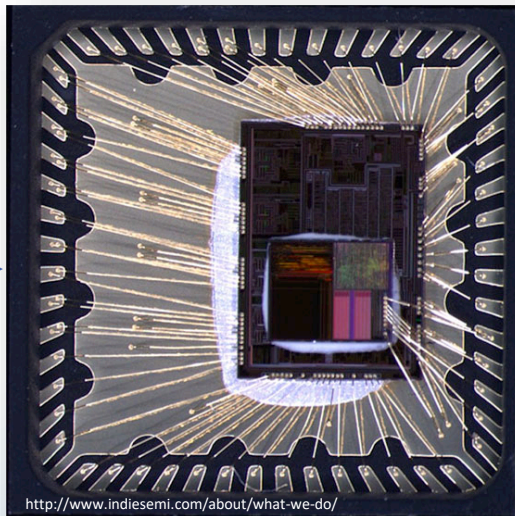
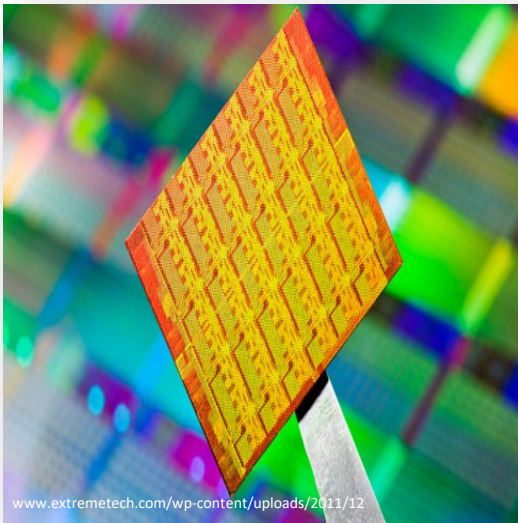
- Complex electronic part that “controls” the flow of electricity
- Basis of all modern electronics
- Used in aerospace, military, industrial, computers, and many other industries
- Also found in numerous consumer electronics
 - Personal computers, phones, home appliances





Integrated Circuit (IC)

- Component packaged in plastic, metal, or ceramic package containing a semiconductor chip
 - Package serves to protect and preserve performance of the chip
- Semiconductor material usually made of silicon and contains many transistors



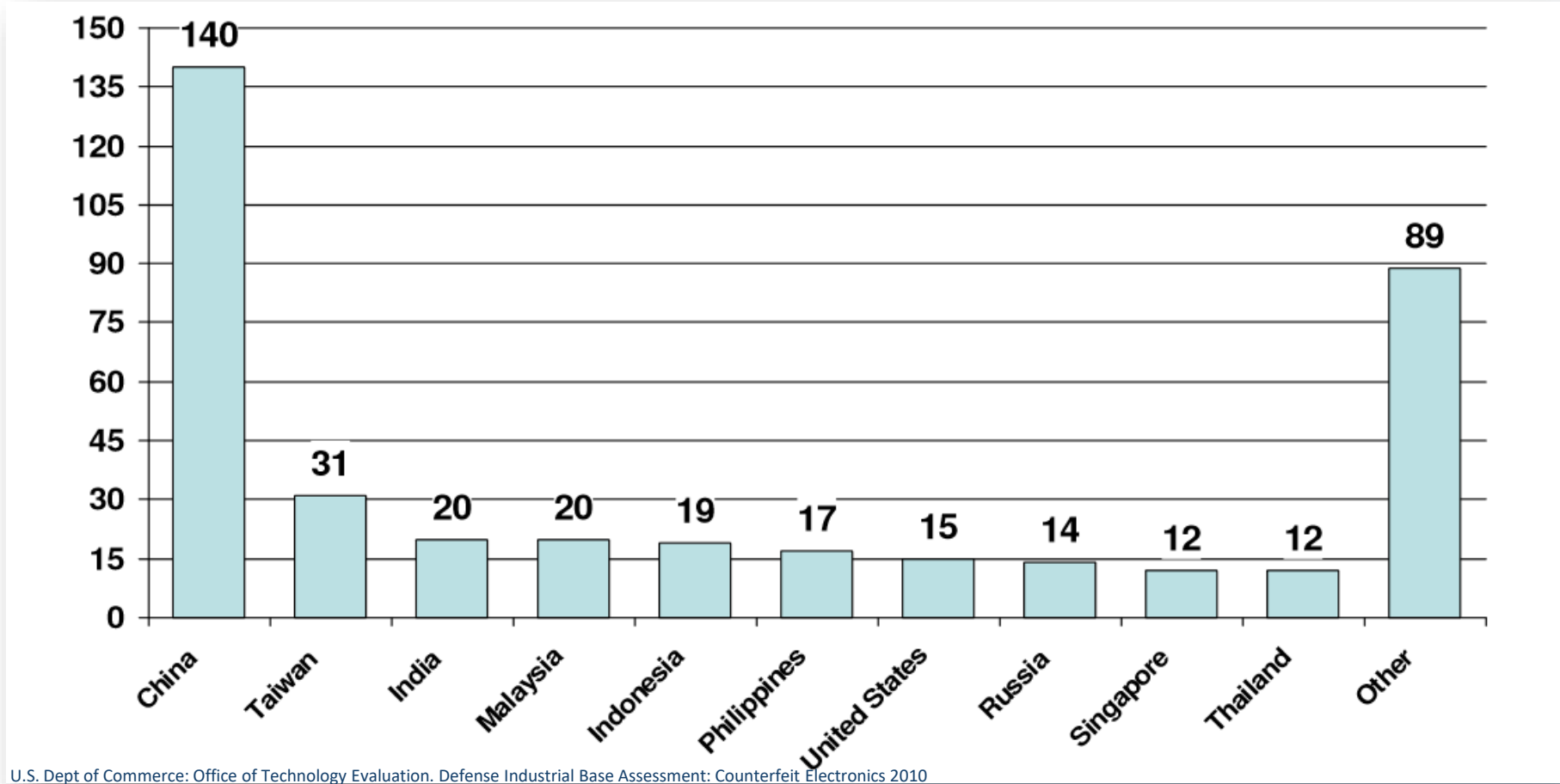


Recent Trends

- One of the main reporting organizations, ERAI, says suspect reports are steady at **~1000 reports/year**; they estimate that only **~10%** of suspect counterfeit parts found are reported
- ICs are still the most reported EEE component by ERAI in 2018 at **57%** (down from **87%** in 2016); **capacitors are up to 16%**, transistors 12%
- According to ERAI, **72% of reported suspect counterfeits are obsolete** parts (reported 2001 – 2013)
- MIL-spec temperature-range parts account for only 1% of the ICs used, but **40% of the ICs reported counterfeited**
- The average gap between purchase time and when suspects are reported to ERAI or GIDEP is **4.6 years**; only 3.7% of suspect counterfeits reported to GIDEP are reported within a year of their date codes
- Bearings, valves, nuts, bolts, and washers are often counterfeited; most counterfeited DoD parts found have been **fasteners and bearings**
- **3D printing** now brings us a host of new risks, from cloned designs to bad raw materials



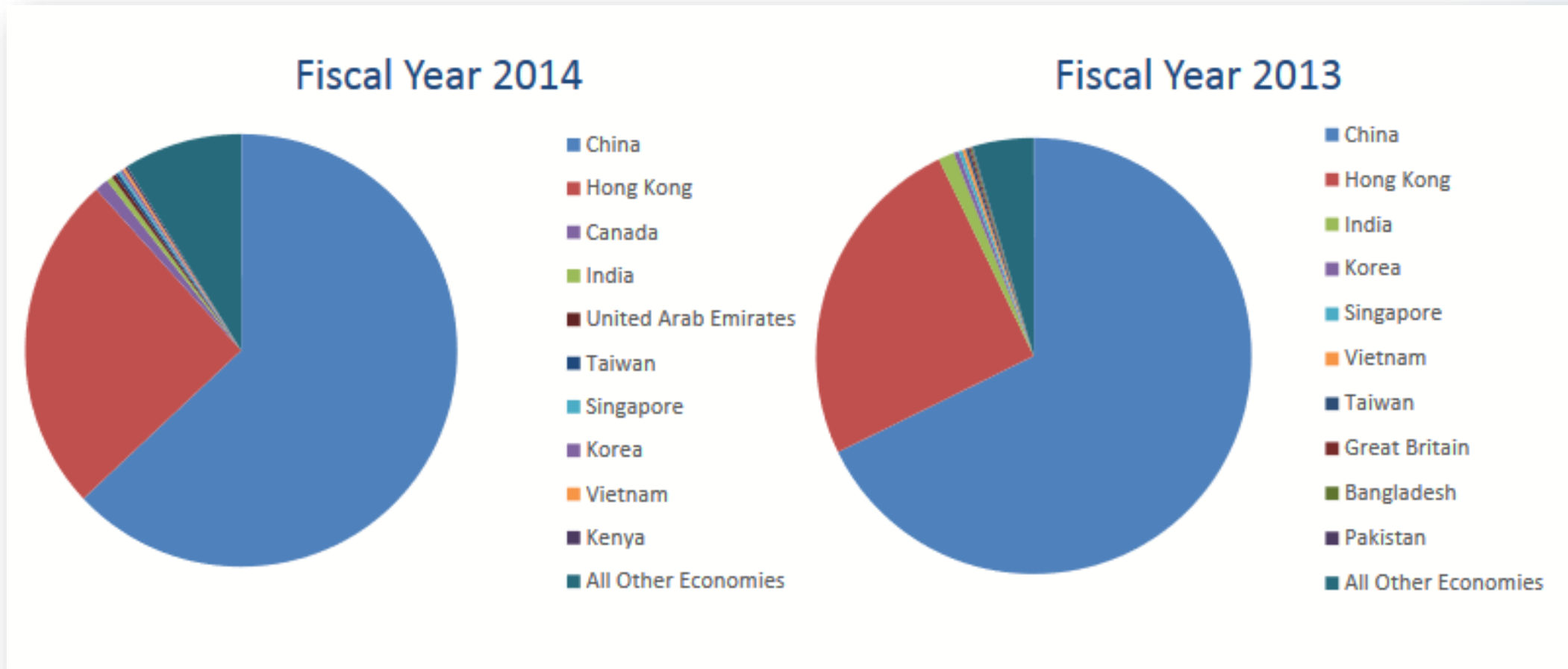
Top countries suspected or confirmed to be sources of counterfeits



U.S. Dept of Commerce: Office of Technology Evaluation. Defense Industrial Base Assessment: Counterfeit Electronics 2010



Top Countries with Homeland Seizures



Courtesy: Homeland Security: IPR Seizures FY 2014



Section 2-Identifying the Problem



Which product is more likely to encounter counterfeit parts?



Copyright: <http://www.boeing.com>

Military—design life of product outlives design of electronic parts. Components in military aircraft have short life times compared to use of aging systems.



Space—different risk profile compared to military, often build only 1 flight model. Projects primarily based on new design



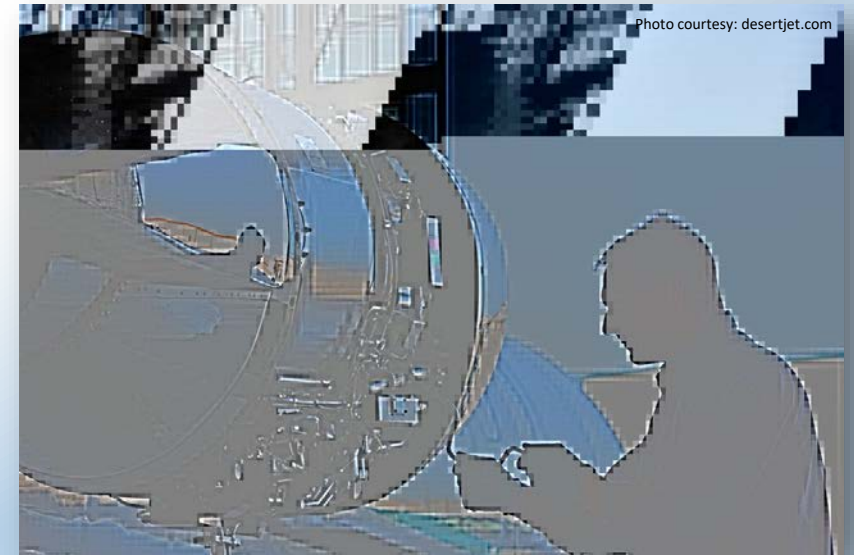
Copyright: <http://www.sony.com>

Commercial—cell phones, computers, video game system products mirror part lifetime.



Part Obsolescence

- Demand for critical systems designs with 20+ year life cycles
 - Systems such as the F-15, which was put into service in 1975 and is scheduled to be in service till 2025, are used far after their original end-of-life projections.
- A component that is no longer manufactured by the Original Component Manufacturer. An obsolete component can no longer be purchased directly from an OCM or authorized distributor but may be sourced from the open market.
- Parts cycle life have become significantly shorter than the life cycle of the product
 - Systems may contain obsolescence problems before product is fielded and during field life
 - Decline in military parts
 - Projected lifecycles of electronic parts and components produced by industry can be as brief as two years.





Do you know where your parts come from?



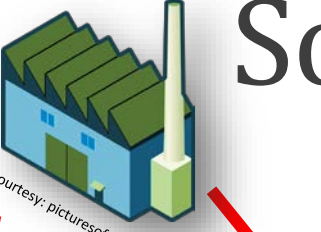


Supply Chain Traceability

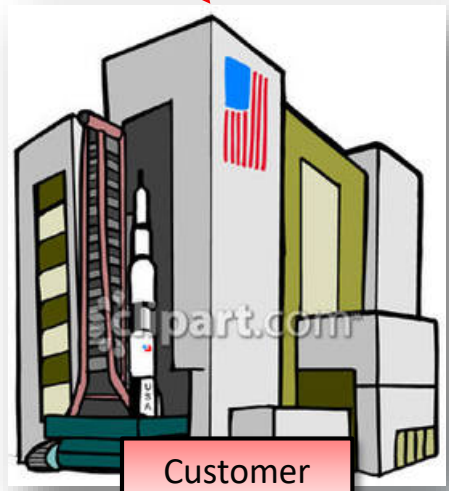
- Documented evidence of a part's supply chain history
 - Supply chain intermediaries and significant handling transactions, such as from OCM to distributor, or from excess inventory to broker to distributor.
- Provides evidence where part was manufactured and who has “touched” the part before it is received into the hands of the customer
 - Longer thread of intermediaries creates more risk
 - Harder to find traceability for >2nd tier subcontractor
 - Open market tends to provide limited traceability

Sources of Supply

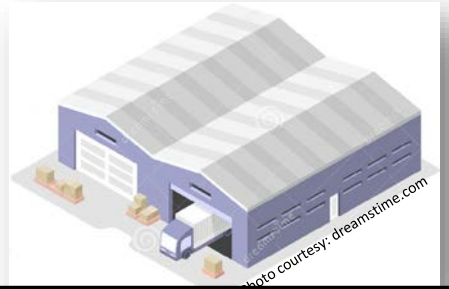
Original Component Manufacturer (OCM)



Original Equipment Manufacturer (OEM)



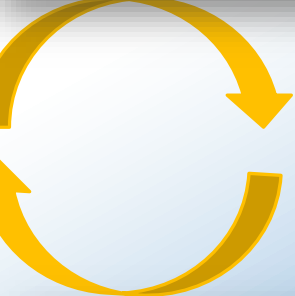
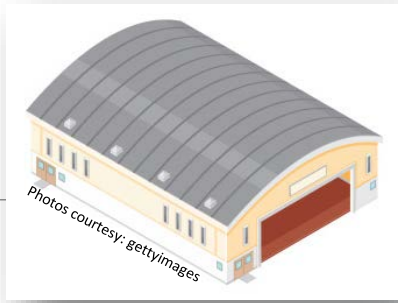
Customer



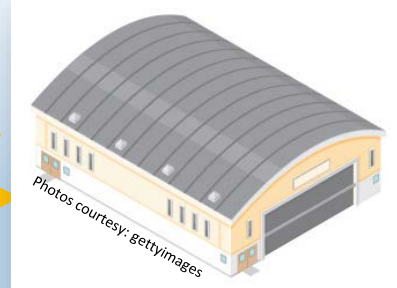
Authorized/Franchised Supplier



Aftermarket Manufacturer



Independent Distributors (Stocking, Non-stocking, Brokers)



Controlled Market

Open Market



Sources of Supply

- **ORIGINAL EQUIPMENT MANUFACTURER (OEM):** A company that manufactures products that it has designed from purchased components and sells those products under the company's brand name.
- **ORIGINAL COMPONENT MANUFACTURER (OCM):** An organization that designs and/or engineers a part and is pursuing or has obtained the intellectual property rights to that part.
 - The part and/or its packaging are typically identified with the OCM's trademark.
 - OCMs may contract out manufacturing and/or distribution of their product.
 - Different OCMs may supply product for the same application or to a common specification.
- **AUTHORIZED/FRANCHISED DISTRIBUTOR:** A distributor with which the OCM has a contractual agreement to buy, stock, re-package, sell and distribute its product lines. When a distributor does not provide products in this manner, then for the purpose of this document, the distributor is considered an independent distributor for those products. Franchised distributors normally offer the product for sale with full manufacturer flow-through warranty. Franchising contracts may include clauses that provide for the OCM's marketing and technical support inclusive of, but not limited to, failure analysis and corrective action, exclusivity of inventory, and competitive limiters.
- **AFTERMARKET MANUFACTURER:** Authorized by the OCM to produce and sell replacements parts, due to discontinuation of production of a part. Produces parts through emulation, reverse-engineering, or redesign, that match the OCM's specifications and satisfy customer needs without violating the OCM's intellectual property and intellectual property rights.

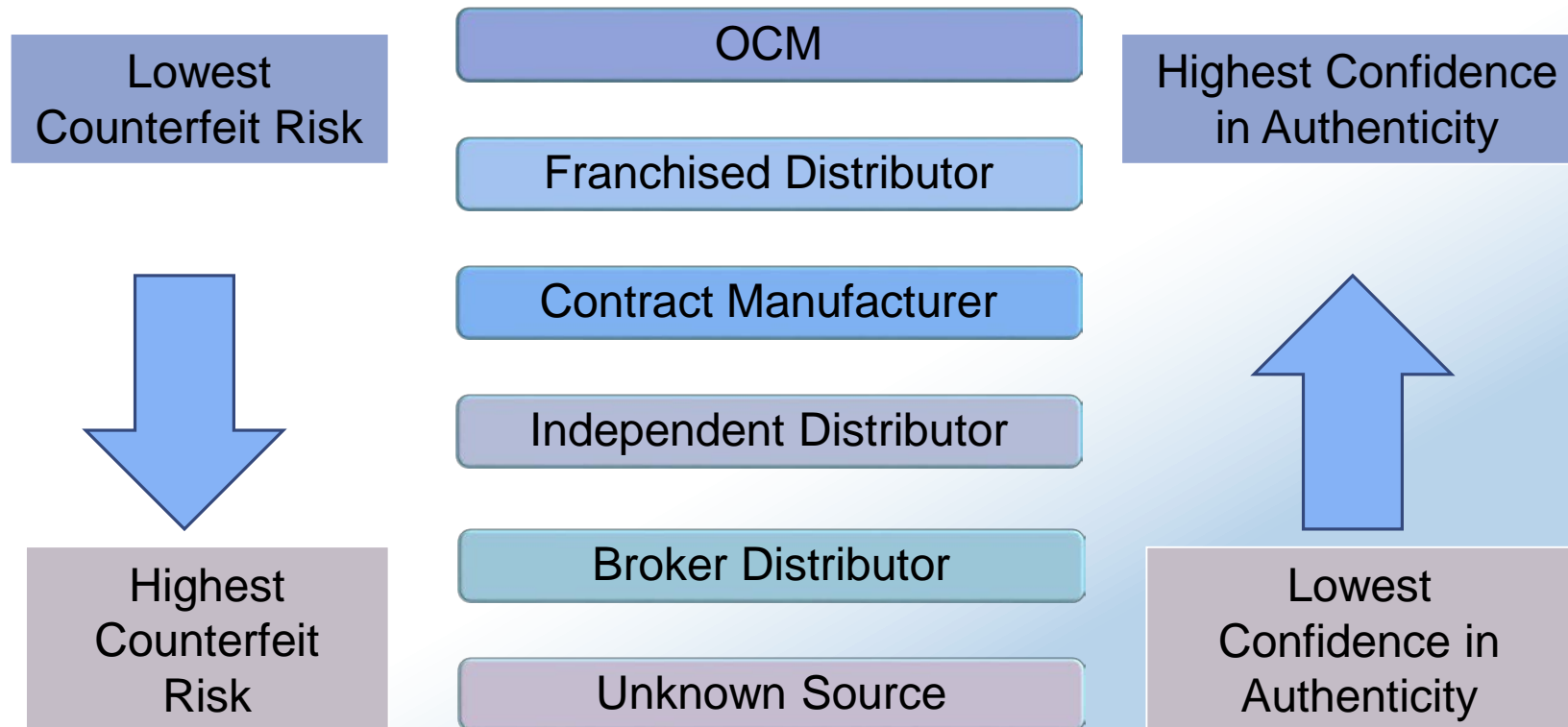


Sources of Supply

- **OPEN MARKET:** The trading market that buys or consigns primarily OEM and Contract Manufacturer's **excess** inventories of new electronic parts and subsequently utilizes these inventories to fulfill supply needs of other OEMs and contract manufacturers, often due to urgent or obsolete part demands.
- **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.
- **STOCKING DISTRIBUTOR:** A type of Independent Distributor that stocks large inventories typically purchased from OEMs and Contract Manufacturers. The handling, chain of custody, and environmental conditions for parts procured from Stocking Distributors are generally better known than for product bought and supplied by Broker Distributors.
- **BROKER DISTRIBUTOR:** A type of Independent Distributor that works in a "Just in Time" (JIT) environment. Customers contact the Broker Distributor with requirements identifying the part number, quantity, target price, and date required. The Broker Distributor searches the industry and locates parts that meet the target price and other Customer requirements.



The “Procurement Decision”





Senate Armed Services Committee Investigation

- 2012 investigation into counterfeit electronic parts in the DoD supply chain, 2009-2010
- Led by Senators John McCain (R-AZ) and Carl Levin (D-MI)
- Many of the investigators pointed to China as a source for counterfeit electronics
- SASC staff were refused access to China
- Many of these parts came from resale points in the U.S., U.K., and Canada



Analysis performed	DAAG	DAAG	B90T	MLL1	MLL1	YCCT	YCCT
Visual Inspection	Fail	Fail	Fail	Fail	Fail	Fail	Fail
Resistance to Solvents (RFS) and Solder Test	N/A	N/A	Fail	N/A	N/A	Pass	Pass
Package Configuration and Dimensions	Pass	Pass	Pass	Pass	Pass	Pass	Fail
X-Ray Fluorescence Spectroscopic Analysis	Fail	Fail	Pass	Fail	Fail	Pass	Pass
High-Temp X-ray Analysis	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Scanning Electron Microscopy (SEM) Analysis	Fail	Fail	Pass	Pass	Pass	Fail	Fail
Solderability Test	Pass	Pass	Pass	Pass	Pass	Pass	Pass
Dimensional Test	N/A	N/A	Fail	N/A	N/A	N/A	Fail



SASC Investigation

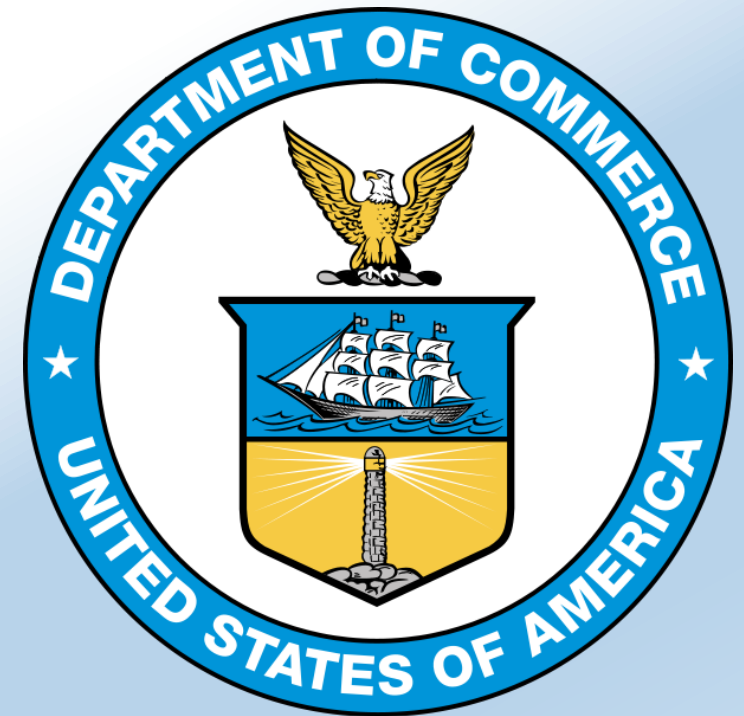
- Investigation uncovered suspected counterfeit parts on mission computers for MDA missile, thermal weapons sights delivered to the Army and on military planes including C-17, C-130J, C-27J, and P-8A as well as on AH-64, SH-60B, and CH-46 helicopters.
- Identified 1,800 cases of counterfeiting
 - >1 million total suspected parts
 - Obsolete part numbers
 - Cost for replacement?
 - Parts sold by US companies originally from China!
- [Video: SASC Hearing](#)





U.S. Department of Commerce Findings

- All orgs in supply chain have been directly impacted
- Record-keeping on counterfeit findings is limited
- Incorrect assumption at others in supply chain are testing parts
- Most DoD orgs do not have counterfeit mitigation policies
- Lack of traceability is common
- Stricter testing and quality controls are required





Section 3 – the Extent of the Problem



The problem of E-waste

- E-waste is electronic products nearing the end of their "useful life."
 - Computers, televisions, VCRs, stereos, copiers, and fax machines are common electronic products.
 - Many of these products can be reused, refurbished, or recycled.
- Loopholes created in "loose" regulating policies and E-waste is shipped to other countries for cheap processing
- Electronics Recycling is now the fastest growing solid waste stream in the world
 - EPA estimated 2012 E-waste at 3.4 million tons
 - Only 29.2% is recycled



Photo courtesy of: <http://discardstudies.files.wordpress.com/2012/03/ewaste-destinations.jpg>

Source: EPA 530-R-11-002



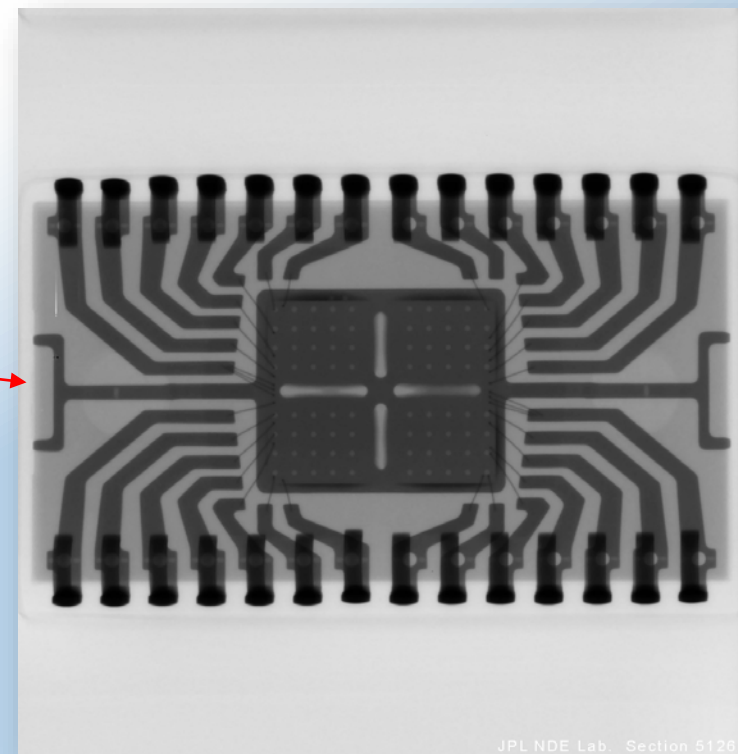
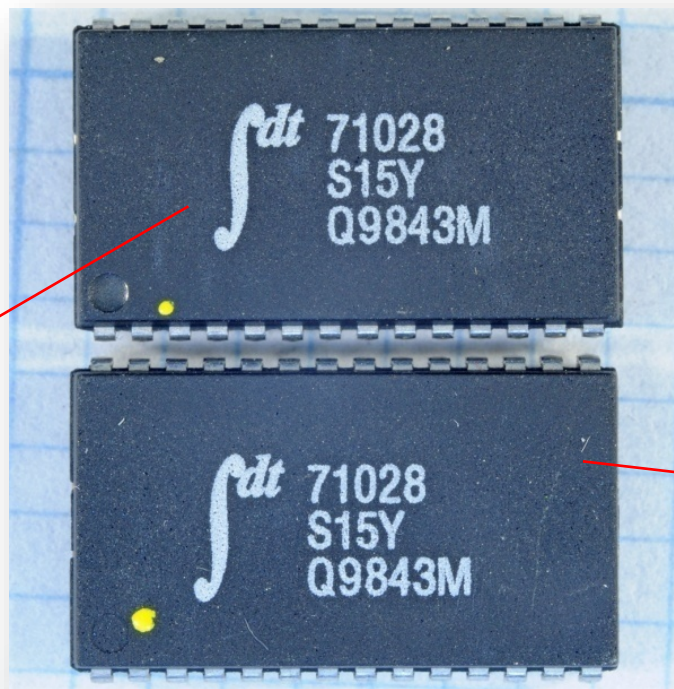
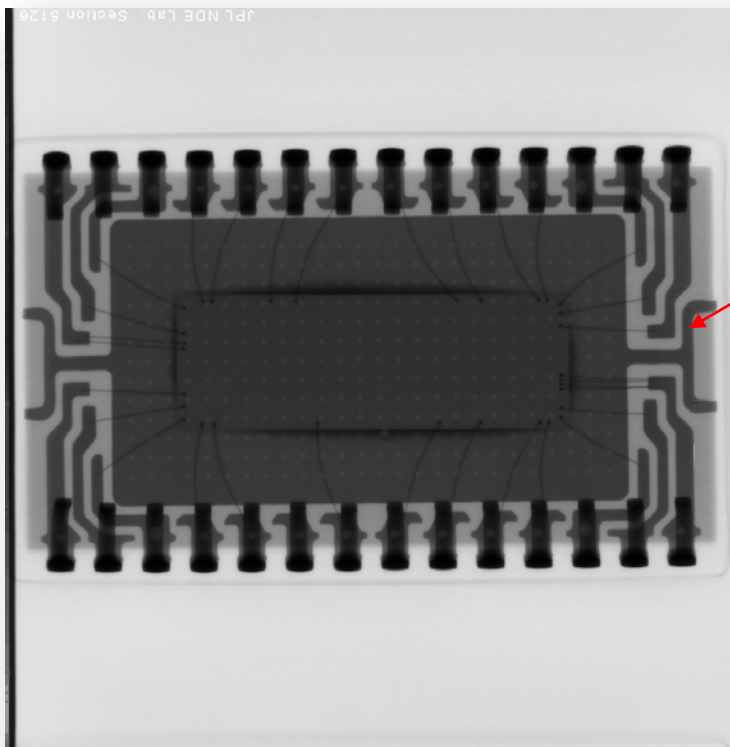
The problem of E-waste

- E-waste has “turned into an abundance of discrete electronic components and microcircuits for counterfeit parts” (Department of Commerce)
- Refinished parts are slipped back into the supply chains which we have then procured
- Video: The “Digital Dumping Ground”
<http://www.pbs.org/frontlineworld/stories/ghana804/>



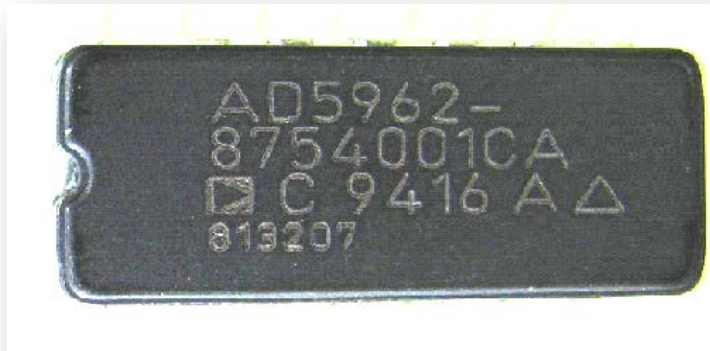


What's in the box?

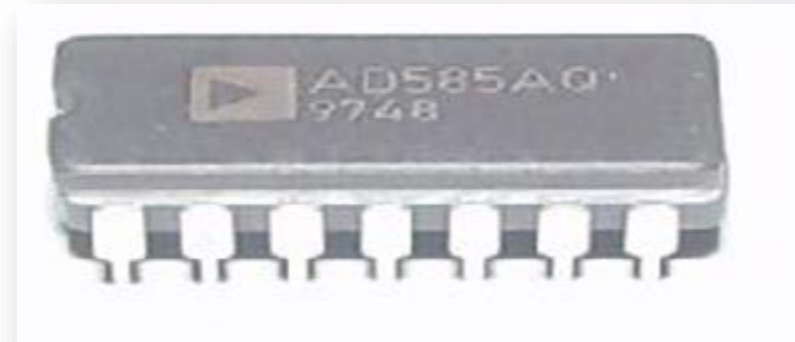




False Advertising – Mil or Commercial



- Meets Requirements of DSCC specification 5962-87540
- Military Grade Quality Assurance Level
- Rated over a wider temperature range than commercial or industrial parts
- Costs more than industrial grade



- Industrial Grade IC
- Smaller temperature range
- Cost less money than the military grade

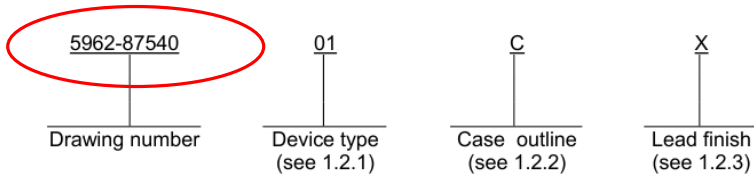


False Advertising – Mil or Commercial

1. SCOPE

1.1 Scope. This drawing describes device requirements for MIL-STD-883 compliant, non-JAN class level B microcircuits in accordance with MIL-PRF-38535, appendix A.

1.2 Part or Identifying Number (PIN). The complete PIN is as shown in the following example:



1.2.1 Device type(s). The device type(s) identify the circuit function as follows:

Device type	Generic number	Circuit function
01	AD585	High speed, sample and hold amplifier

1.2.2 Case outline(s). The case outline(s) are as designated in MIL-STD-1835 and as follows:

Outline letter	Descriptive designator	Terminals	Package style
C	GDIP1-T14 or CDIP2-T14	14	Dual in line
2	CQCC1-N20	20	Square leadless chip carrier

1.2.3 Lead finish. The lead finish is as specified in MIL-PRF-38535, appendix A.

1.3 Absolute maximum ratings.

1.4 Recommended operating conditions.

Positive supply voltage (+V _S)	+5 V dc to +18 V dc
Negative supply voltage (-V _S)	-12 V dc to -18 V dc
Ambient operating temperature range (T _A)	-55°C to +125°C

ANALOG INPUT CHARACTERISTICS											
Offset Voltage	5		2		2				mV		
Offset Voltage, T _{MIN} to T _{MAX}	6		3		3				mV		
Bias Current	2		2		2				nA		
Bias Current, T _{MIN} to T _{MAX}	5		5		50 ²		20		nA		
Input Capacitance, f = 1 MHz	10		10		10				pF		
Input Resistance, Sample or Hold	10 ¹²		10 ¹²		10 ¹²						
20 V p-p Input, A = +1											
DIGITAL INPUT CHARACTERISTICS											
TTL Reference Output	1.2	1.4	1.6	1.2	1.4	1.6	1.2	1.4	1.6	V	
Logic Input High Voltage	2.0		2.0		2.0				V		
Logic Input Low Voltage			0.8		0.8		0.7		V		
Logic Input Current (Either Input)			50		50		50		μA		
POWER SUPPLY CHARACTERISTICS											
Operating Voltage Range	+5, -10.8		±18		+5, -10.8		±18		V		
Supply Current, R _L = ∞	6		10		6		10		mA		
Power Supply Rejection, Sample Mode	70		70		70		70		dB		
TEMPERATURE RANGE											
Specified Performance	0		+70		-25		+85		-55	+125	°C
PACKAGE OPTIONS ^{3,4}											
Cerdip (Q-14)					AD585AQ		AD585SQ		AD585SE		
LCC (E-20A)											
PLCC (P-20A)	AD585JP										

NOTES

¹Maximum input signal is the minimum supply minus a headroom voltage of 2.5 V.

²Not tested at -55°C.

³E = Leadless Ceramic Chip Carrier; P = Plastic Leaded Chip Carrier; Q = Cerdip.

⁴For AD585/883B specifications, refer to Analog Devices Military Products Databook.

Specifications subject to change without notice.

Specifications shown in **boldface** are tested on all production units at final electrical test. Results from those tests are used to calculate outgoing quality levels.

All min and max specifications are guaranteed, although only those shown in **boldface** are tested on all production units.



False Advertising – Mil or Commercial

- Pricing through Analog Devices site:
 - Military Grade >\$60 more expensive
- Counterfeiters will falsify documents saying you are purchasing a military grade when it is actually commercial grade

SAMPLES & PURCHASE | PACKAGING

AD585 Model Options

Model	Status	Package	Pins	Temp. Range	Price* (100-499)	Price* (1000 pcs.)	Packing / Qty
5962-87540012A	Prodn	20 Id LCC	20	Mil	\$79.75	\$72.08	Tube, 54
5962-8754001CA	Prodn	14 Id CerDIP	14	Mil	\$84.32	\$76.21	Tube, 25
AD585ACHIPS	Prodn	CHIPS OR DIE	-	Ind	\$10.30	\$10.30	Tray, 100
AD585AQ	Not Rec**	14 Id CerDIP	14	Ind	\$22.43	\$20.30	Tube, 25
AD585JP	Not Rec**	20 Id PLCC	20	Comm.	\$20.53	\$18.55	Tube, 49
AD585JP-REEL	Not Rec**	20 Id PLCC	20	Comm.	-	\$18.55	Reel, 1000
AD585JP-REEL7	Contact ADI	20 Id PLCC	20		-	-	Reel, 250
AD585JPZ	Not Rec**	20 Id PLCC	20	Comm.	\$18.70	\$16.91	Tube, 49
AD585JPZ-REEL7	Not Rec**	20 Id PLCC	20	Comm.	-	\$16.91	Reel, 250
AD585SCHIPS	Prodn	CHIPS OR DIE	-	Mil	\$36.77	\$36.77	Tray, 100
AD585SE	Prodn	20 Id LCC	20	Mil	\$59.81	\$54.04	Tube, 54
AD585SE/883B	Prodn	20 Id LCC	20	Mil	\$80.68	\$72.92	Tube, 54
AD585SQ	Prodn	14 Id CerDIP	14	Mil	\$62.04	\$56.10	Tube, 25
AD585SQ/883B	Prodn	14 Id CerDIP	14	Mil	\$80.65	\$72.91	Tube, 25



Other Examples of Counterfeit Parts

- Parts which do not contain the proper **internal construction** (die, manufacturer, wire bonding, etc.) consistent with the ordered part.
- Parts which have been **used, refurbished or reclaimed**, but represented as new product.
- Parts which have **different package style or surface plating/finish** than the ordered parts.
- Parts which have not successfully completed the Original Component Manufacturer's (OCM's) full **production and test flow**, but are represented as completed product.
- Parts sold as upscreened parts, which have **not successfully completed upscreening**.
- Parts sold with **modified labeling or markings** intended to misrepresent the part's form, fit, function, or grade.

Parts which have been refinished, upscreened, or uprated and have been identified as such are not considered counterfeit



Returns

Authentic



- Properly marked
- Similar vintage and configuration as the fake part

Counterfeit



- Counterfeit logo
- Incorrect fonts & format
- Wrong ink

- At any moment parts leave hands, this creates risk
- Must have procedures in place, to verify you are receiving the same product back into stock
- Manufacturers and authorized distributors have unwittingly sold counterfeits of their own products
- Some suppliers are no longer selling previously returned items to aerospace and space flight industries



Returns



Authentic

Counterfeit


- Bottom markings in black validate configuration, serial number, and date code

- Bottom markings removed



Returns

- Supplier unknowingly returned bad parts switched out by customer.
- Parts then sent to new customers who caught the discrepancies
- Some suppliers are no longer selling previously returned items to aerospace/ space flight industry

 GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM PROBLEM ADVISORY		
1. TITLE (Class, Function, Type, etc.)		2. DOCUMENT NUMBER
Suspect Counterfeit, Microcircuit, +5V CMOS, RS-232 100KBPS, Transceiver with 2 Drivers/Receivers		3. DATE (DD-MMM-YY)
4. MANUFACTURER AND ADDRESS	5. PART NUMBER	6. NATIONAL STOCK NUMBER
	ADM232LARZ	Not Available
	7. SPECIFICATION	8. GOVERNMENT PART NUMBER
	Not Available	Not Available
	9. LOT DATE CODE START	10. LOT DATE CODE END
	1108	1108
11. MANUFACTURER'S POINT OF CONTACT	12. CAGE	13. MANUFACTURER'S FAX
14. MFR. POC PHONE	15. MANUFACTURER'S E-MAIL	
16. SUPPLIER	17. SUPPLIER ADDRESS	18. SUPPLIER CAGE
	San Diego, CA !	
19. PROBLEM DESCRIPTION / DISCUSSION / EFFECT		
<p>Supplier is an authorized distributor of OCMs products which were originally shipped to Customer. Supplier shipped ADM232LARZ parts acquired directly from OCMs to Customer. Based on this shipment and upon Customer request, Supplier later issued a Return Material Authorization (RMA) to Customer. Customer shipped 200 pieces of part number ADM232LARZ to Supplier on an RMA. These parts were received into inventory and subsequently re-shipped to two customers: 94 pieces to Customer A and 106 pieces to Customer B. Customer B advised Supplier that they had received non-conforming ADM232LARZ parts and sent a photo of the non-conforming parts. Customer B also contacted OCMs and submitted a photo for review and requested product change notices for the non-conforming parts. Supplier also contacted OCMs and in response to Supplier request, OCMs advised Supplier that the date code on the non-conforming parts indicated that these parts had never been shipped by OCMs to Supplier.</p>		

Courtesy: GIDEP



Clones

Cloned Part: The complete manufacture of a reverse engineered device to have the same form, fit, and function as the original. Devices are produced on low end equipment and will not meet the original reliability requirements. Devices are branded and sold as Original Component Manufacturer (OCM) parts.



Courtesy: iNEMI, "Development of a Methodology to Determine Risk of Counterfeit Use" by Mark Schaffer



Clones

- Cloned counterfeit electronic parts **visually look authentic** and pass the requirements of form and fit.
- The additional danger is that clones **will actually power up and function** just like the authentic devices, essentially looking and acting just like the originals.
- The hidden danger is the **reliability concerns**. These components are not meant to meet the reliability requirements and could fail at anytime.
- One way to reveal a clone is **more stringent electrical testing** which can be costly and time-consuming.
- The best way to reveal a clone is by **comparison with a known genuine part**.
- This is a new but **growing threat**: In 2018, over 150 different part numbers were cloned.



A New Threat: Counterfeit Test Equipment

- Vulnerability identified in 2018 in a GIDEP Alert
- Northrop Grumman had bought a noise figure analyzer, allegedly made by Keysight Technologies of Englewood, CO, sold by Valuetronics International of Elgin, IL, that turned out to be a Chinese clone
- Keysight had to disassemble the analyzer to determine that it was a clone
- Equipment purchases are generally not controlled as carefully as purchases of flight parts





Value-added processes

- Any value added process sent out to another company creates risk
 - Such as further part-level testing
 - Manufacturing processes
- Some test houses are soliciting cheaper test houses to do their contracted testing without notifying the customer
- Falsified Test Reports
 - 19% of companies contracting test houses had problems with counterfeit testing



Photo courtesy: engineerredtaxsolutions



Commercial off the Shelf (COTS) items

- Goods and services bought and used under a federal contract available from the commercial marketplace
- Benefits of using COTS:
 - Reduced development time and delivery schedule
 - Reduction of cost, low-cost alternative to full mil-spec parts
 - Alternative to custom-built parts
 - New generation of leading COTS IC technologies introduced every 3 years

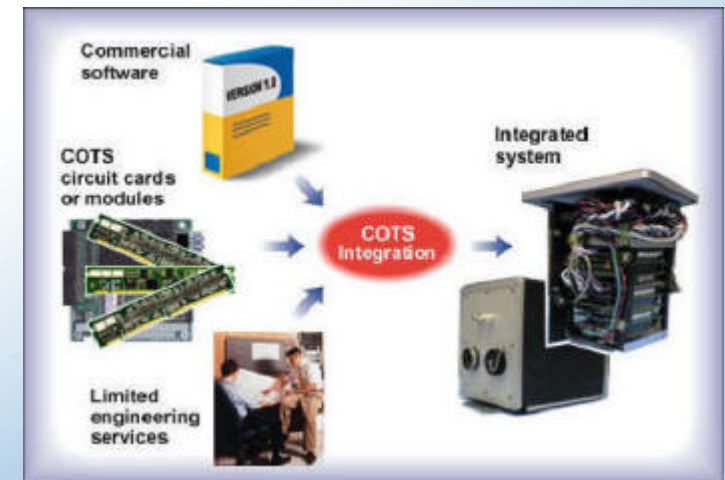


Photo courtesy: swri.org



Commercial off the Shelf (COTS) items

- Risks of costs
 - Security vulnerabilities
 - Traceability may not exist
 - Vendor's business practices
 - Vendor may reject customers procurement requirements
 - At the mercy of commercial suppliers economic decisions
 - Little technical data provided
 - Not held to military specs
 - Not been designed or qualified for military market
 - Cannot upgrade to mil temperature range
 - Supplier selection can be risky
 - Obsolescence (military vs. space)



Photo courtesy: ginaabudi.com



Section 4 – Supplier and Part Availability Management



NPD 8730.2: NASA Parts Policy

Policy to control risk and enhance reliability in NASA flight and critical ground support test systems by managing selection, acquisition, traceability, testing, handling, packaging, and storage of EEE and mechanical parts and materials

- Responsibility:

- **Develop, document, and implement a counterfeit EEE parts control plan** for the avoidance, detection, mitigation, disposition, control, and reporting of counterfeit EEE parts (Requirement).
- **Perform surveys, audits, product inspections, qualification testing, risk assessments, and/or production line certifications** to verify the capability and qualification of supply sources (Requirement). The results of surveys, audits, and product inspections performed by other Centers, other Government agencies, accredited third-party organizations, or the private sector may be utilized on a risk-informed basis as a supplement to, or a substitute for, direct surveillance.
- **Report nonconforming, defective, and/or suspected counterfeit parts** in accordance with **NPR 8735.1**, and for all cases involving counterfeit parts or other potential fraud, to the NASA Office of Inspector General and the NASA Director, Acquisition Integrity Program (AIP)(Requirement).
- Ensure that **effective processes and controls** are in place for parts and materials within NASA programs and projects and at NASA Centers (Requirement). Assurance methods include auditing, conducting program reviews, and establishing and tracking performance parameters



NPD 8730.2: NASA Parts Policy

- Attachment C: Counterfeit Parts Control Plan

- 1) Parts Availability Process:

- a. Maximize availability of **authentic**, originally designed, and qualified parts throughout the product's life cycle, including, for example:
 - (1) **Control of parts obsolescence.**
 - (2) **Alternate/multiple sources.**
 - (3) Acceptable product substitutions.
 - (4) System redesign.
 - (5) Inventory control, parts sparing, and/or **lifetime buy practices.**
 - (6) Planning for adequate procurement lead times in support of manufacturing and delivery schedules.



NPD 8730.2: NASA Parts Policy

- 2) Procurement Process:
 - a. **Assess potential sources of supply to determine the risk of receiving non-authentic parts. Original Component Manufacturers (OCM), OCM-authorized suppliers (e.g., franchised distributors), and authorized aftermarket manufacturers are considered to have low risk of supplying non-authentic parts.** Assessment actions include surveys, audits, review of product alerts (e.g., GIDEP, ERAI), and analysis of supplier quality data to determine past performance. (Note: GIDEP and ERAI product alerts are accessible through NASA's Supplier Assessment System (<http://sas.nasa.gov>).)
 - b. Mitigate risks of procuring counterfeit parts from sources other than OCMs or authorized suppliers.
 - c. Factor risk of receiving nonauthentic parts into the source selection process.
 - d. Ensure that approved/ongoing sources of supply are maintaining effective processes for mitigating the risks of supplying counterfeit EEE parts.
 - e. **Include applicable contract or purchase order quality requirements related to counterfeit parts prevention.** Examples of quality requirements are provided in AS5553, including
 - (1) Certificate of Conformance
 - (2) Mandatory product tests and inspections
 - (3) Supply chain traceability
 - (4) Federal penalties associated with fraud and falsification
 - f. **Specify contractor flow-down of applicable counterfeit parts prevention requirements to their subcontractors.**



NPR 8735.1: Exchange of Problem Data Using NASA Advisories and GIDEP

Establishes general requirements and procedures for NASA to ensure that information concerning significant problems involving parts, materials, processes, software, and safety problems is exchanged internally and externally

3.4.3 NASA Program Managers shall generate NASA Advisories or GIDEP Notices for items that meet the following criteria:

- a. Counterfeit or suspect counterfeit, or;
- b. Contain a major or critical nonconformance, and:

Note: Incidents of counterfeiting and fraud related to procurement may also be reported to the Office of General Counsel's Acquisition Integrity Program.

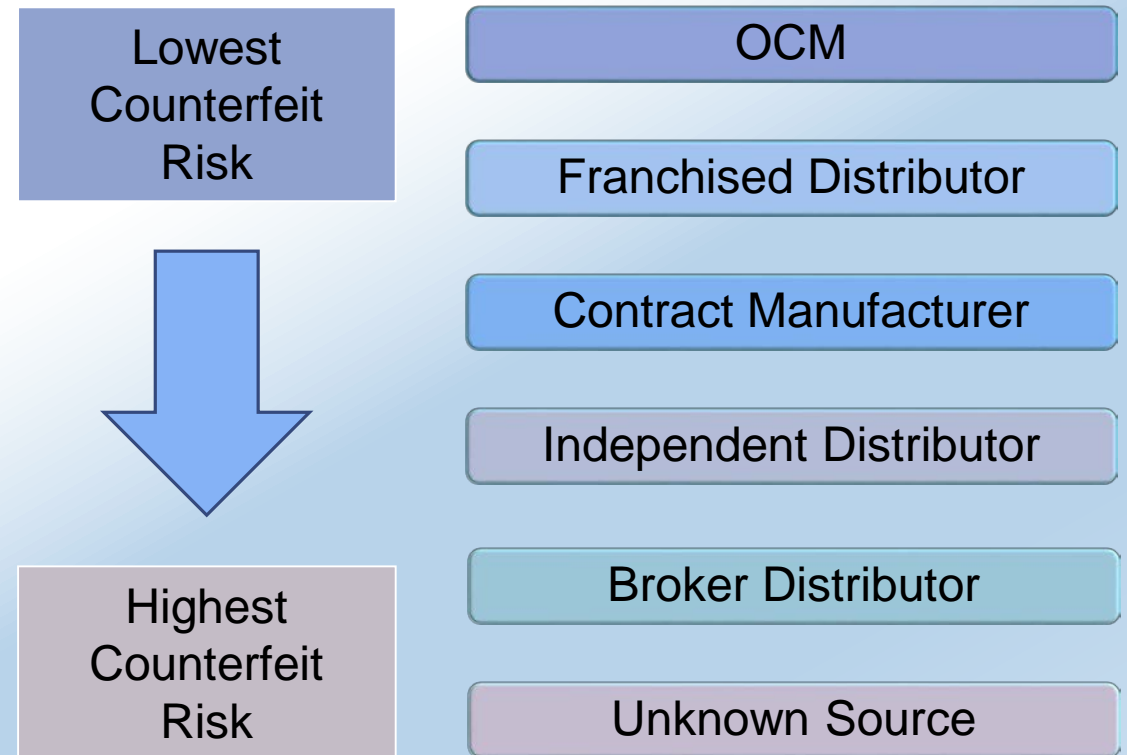
- (1) Are commercially available or common items, or;
- (2) Constitute a quality escape (e.g. a nonconforming item has been released to more than one customer).

Note: NASA Advisories are issued for items described above that are peculiar to NASA applications and/or have not escaped to non-NASA organizations. GIDEP Notices should be issued for other items in work.



Supplier Management

- Assuring our approved suppliers are maintaining effective processes for mitigating the risks of supplying counterfeit electronic parts includes:
 - On-site audits (QMS, counterfeit)
 - Analysis of supplier data and trends
 - Managing your supplier list
- Suppliers must demonstrate quality control, main source documentation history, and possess necessary certifications





Know your Suppliers, and their Suppliers

- Supplier Management can reduce the risk of:
 - Breaking the chain of traceability of parts
 - Returns process
 - Outsourcing of work
 - Weak supplier selection process
 - Procurement of counterfeit parts
 - Failure to detect and inspect counterfeit parts
 - Process in place is nonexistent or inadequate in responding to counterfeit parts
 - Personnel unaware of counterfeit parts issue
- **There is NO alternative to supply chain management and mitigation**
- **This is where counterfeit avoidance STARTS**



American Conspirators

- Supplier A
 - Operated for 3 years
 - Sold to DoD as “Wholesale Electronics Components” business
 - Falsely stated and knowing bought parts that were new and not from Asia, when in fact they were bought from companies located in Asia and were used
- Supplier B
 - Battery distributor sold near \$3 million in fake batteries to DoD
 - For 7 years, sold more than 80k batteries for Navy purposes
 - First case prosecuted under 2011 Defense Authorization Act
 - Affixed counterfeit labels identifying them as originating from approved suppliers, used chemicals to remove “Made in China”, and prepared doctored documents
- Supplier C
 - Sold known Chinese counterfeit semiconductors to DoD contractors for use in nuclear submarines
 - Charged with conspiracy to traffic in counterfeit military goods, trafficking, wire fraud, money laundering
 - Criminal conduct spanned Feb 07-April 12
 - Purchased millions of dollars in counterfeit ICs bearing marks of 35 electronic manufacturers
- Supplier D
 - Illegal incidents occurred during 2005-2008
 - Supplied customers with falsely remarked microprocessor chips manufactured in China
 - Many chips used in US military and commercial helicopters



Useful Industry Standards

- AS5553—Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
 - Provides uniform requirements, practices and methods to mitigate the risks of receiving and installing counterfeit electronic parts for industry
 - AS6081—Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors
 - Identify reliable sources, mitigate distribution risk, control and reporting procedures
 - AS6171—Test Methods Standard; Counterfeit Electronic Parts
 - EVI-SEM techniques for Counterfeit detection
- ARP6328—Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems
- Supplements AS9100, guidance for implementing counterfeit mitigation program



Section 5 – What You Can Do to Avoid Counterfeits



What You Can Do: Counterfeit avoidance team

Set up a counterfeit part avoidance team, committee, or working group:

- Suggested membership would include QA, Acquisition, and Component Engineering
- If your organization doesn't yet have a counterfeit parts control program, start one
- Can focus on only EEE parts, or can encompass hardware, materials, equipment for flight testing—these would require the involvement of different disciplines
- Monitor GIDEP and NASA alerts for reports of suspect counterfeits that might involve parts or suppliers your organization has dealt with
- Meet periodically and as needed to keep up with changes, continually review and update your counterfeit prevention program, monitor the industry for new threats and mitigations, address vulnerabilities as they are discovered, provide training



What You Can Do: Navy guidebook

- Download the **Department of the Navy’s free Counterfeit Materiel Process Guidebook**, which includes indicators and examples of counterfeit electronic and mechanical parts and materials, a suggested authentication process flow, detailed sample statement of work wording for contracts

<http://www.secnv.navy.mil/rda/Policy/2017%20Policy%20Memoranda/DON%20Counterfeit%20Materiel%20Process%20Guidebook.pdf>



COUNTERFEIT MATERIEL PROCESS GUIDEBOOK

*Guidelines for Mitigating the Risk
Of Counterfeit Materiel in the Supply Chain*

Published by the Office of the Assistant Secretary of the Navy
(Research, Development & Acquisition) Acquisition and Business Management

June 2017
NAVSO P-7000

Appendix H: Indicators of Counterfeit Mechanical Parts and Materials

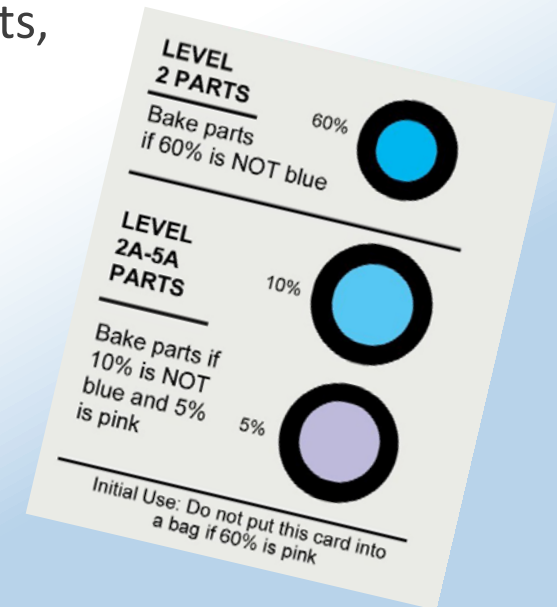
Test/Materiel Type	Counterfeit Indicator	Strength of Indicator
Packaging Indicators	Inconsistent vendor name on the item and on the shipping container, or no name on the container	Moderate
	Shipping boxes contain mixed batch numbers, expiration dates, and UPC codes	Minor
	Unusual packaging and boxing of items	Moderate
	Inconsistent with the manufacturer’s normal packaging or documentation requirements	Major
	Questionable or meaningless numbers on the item(s) or packaging	Moderate
	Obviously changed labeling (crossed out or erased)	Moderate
	Erroneous OM Logo on external packaging	Major
	Appear to have been altered, photocopied, or painted over	Major



What You Can Do: Receiving Inspection

Promote additional Receiving Inspection protocol for riskier procurements, specifically for counterfeit parts prevention:

- Packaging—shipping boxes, ESD and humidity protection
- Packing—fitting trays, reels, tubes with correct part info
- Part traceability—part numbers, mixed lots, CoC, authenticity of documents and logos, misspellings
- 100% visual inspection—pin arrangement and style, P/N markings, logo or CAGE code, country of origin, marking inconsistencies, marking quality, top and bottom markings match, used or refurbished leads, markings indicating previous screening or programming, blacktopping, sanding marks, ghost markings, damage



Train your part inspectors on counterfeit awareness so they are always on the lookout



What You Can Do: Learn more

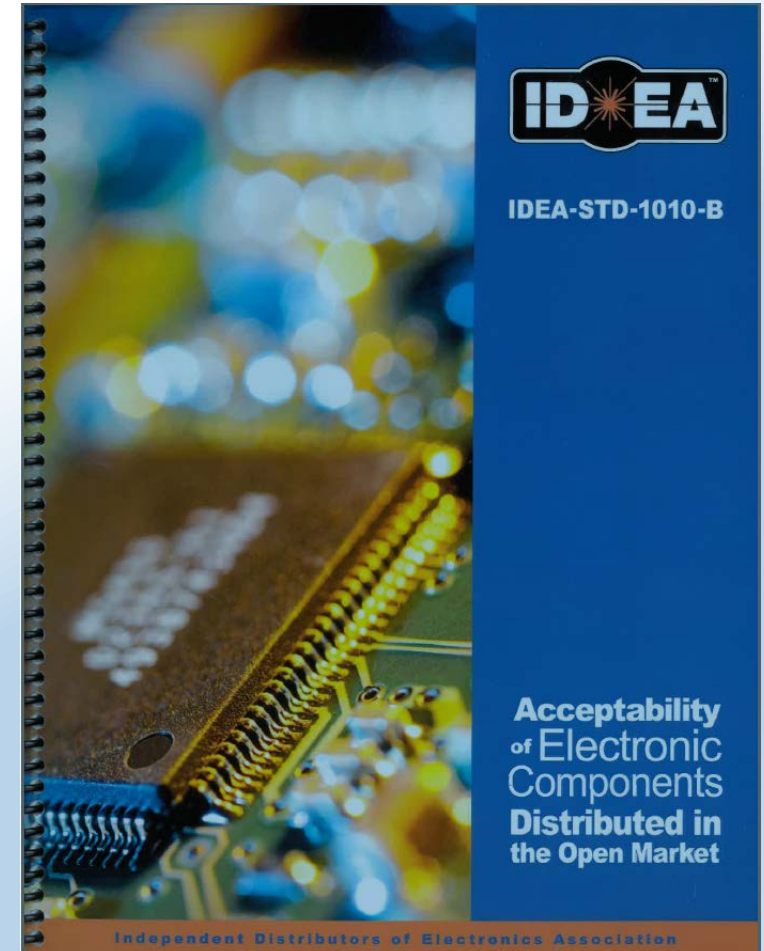
- Learn more: keep up with news by subscribing to ERAI's quarterly newsletter, [https://www.eraf.com/Subscribe to Newsletter](https://www.eraf.com/Subscribe%20to%20Newsletter)
- Learn more: attend the annual SMTA/CALCE Symposium on Counterfeit Parts and Materials at the University of Maryland in June of every year
- Learn more and become involved: SAE Technical Committee G-19, Counterfeit Electronic Parts, chartered to address aspects of preventing, detecting, responding to and counteracting the threat of counterfeit electronic components; publishes AS5553, AS6171 and its slash sheets for different test techniques
- Learn more: take additional training and certify your inspectors
 - IDEA
 - ERAI and InterCEPT
 - Components Technology Institute (CTI) – CCAP-101



What You Can Do: IDEA-STD-1010

IDEA-STD-1010: Acceptability of Electronic Components Distributed in the Open Market

- Gives detailed guidelines for counterfeit analysis of suspect electronic components by documentation check, packing material checks, visual examination, x-ray, chemical checks for re-marking or resurfacing, internal examination
- Compiled by the Independent Distributors of Electronics Association, a nonprofit consortium, idofea.org
- IDEA accepts as members independent distributors who meet a consensus set of requirements to ensure that their supply chains are clean
- IDEA offers training to the standard (1-day or 2-day)
- IDEA offers inspector certification via the IDEA-ICE-3000 Professional Inspector Certification Exam





What You Can Do

- Procurements: For nonflight parts, be vigilant yourself as there are likely no safeguards against your buying counterfeit products—and we don't want them *anywhere*
- Procurements: Be wary of CAGE-hopping, in which unscrupulous suppliers periodically change names and get new CAGE code numbers (it's easy to do) in order to appear legitimate
- For CubeSat or other “high-risk” missions, be vigilant yourself, as many safeguards are bypassed
- Make sure that distributors you're using are authorized for the product lines or part numbers you're buying—most distributors are authorized only for selected products from manufacturers
 - Check manufacturer website for authorized distributors or www.eciaauthorized.com
- For people interfacing with designers, encourage the use of ASL suppliers even for nonflight and EM parts to avoid sourcing problems later
- Use an Approved Supplier List for flight parts—and if you can't, flag the procurement for a counterfeit check
- If you need a suspect counterfeit analysis performed on a purchased lot, try to select a lab that has access to a known-good part, or a Destructive Physical Analysis (DPA) report on a genuine part for comparison

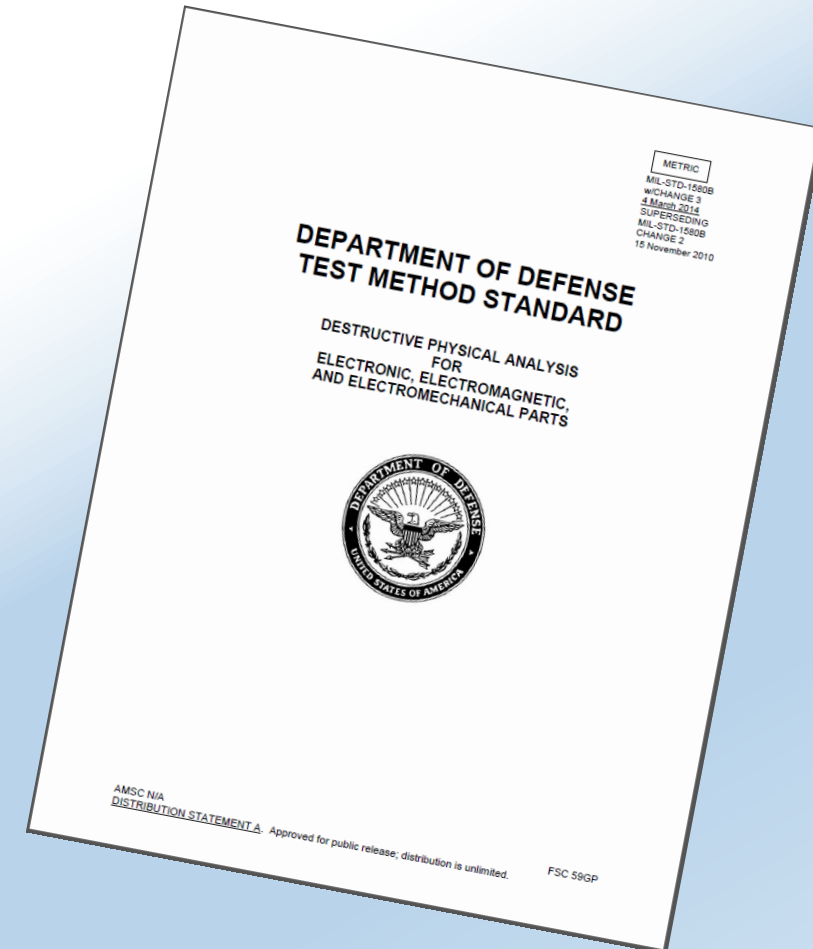


What You Can Do: DPA

What is a DPA?

A destructive physical analysis (DPA) is an “assessment of part lot quality based on the destructive examination of samples randomly selected from each production lot,” typically in accordance with MIL-STD-1580 or some tailored variation of it. A DPA is a series of specific nondestructive and increasingly destructive analytical steps defined by part type and construction that will provide as much information as possible about a lot’s quality.

A failure analysis is not a DPA, though it will often contain some of the same information



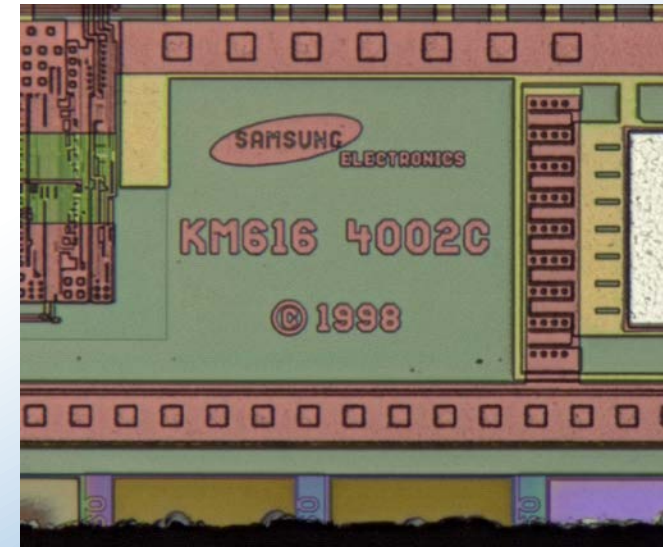


What You Can Do: DPA

What does a DPA include?

Depends on the part type:

- Overall photo, including markings
- X-rays—typically three 90° views
- Internal photos, including overall die photos
- Cross sections
- For diodes—basic electrical parameters
- Residual gas analysis (RGA or IGA)
- Particle impact noise detection (PIND), hermeticity, bond pull, die shear, solderability, scanning electron microscope (SEM) metallization examination



Ideally, you want golden part info on the same part family, from nearly the same date code, or date codes bracketing your samples



What You Can Do

- Train all parts procurement people, component engineers, and failure analysis, test, and DPA lab staff in counterfeit part awareness—and everyone who directly handles flight components
- Follow approved policies, procedures, and practices—and if something doesn't make sense, raise a flag
- For procurements or data review, insist on no gaps in the supply chain to the OCM—and if you can't, flag the procurement for a counterfeit check
- If a procurement, supplier, shipment, document, part—anything—doesn't seem right, question it until you are satisfied, or raise a flag to management or a counterfeit team member
- Look for sneak paths—for instance,
 - Do you have separate purchase processes for flight and nonflight parts?
 - Can nonflight parts be upgraded to flight parts?
 - Does your upgrade process include a counterfeit check
- If you notice a vulnerability, raise a flag so it can be addressed
 - Subcontractor suppliers, often not divulged to prime contractors

You know your job best, and you can best bullet-proof your organization against counterfeiters



Additional References

- SAE Aerospace Standard AS5553: Counterfeit EEE Components; Avoidance, Detection, Mitigation, and Disposition
- SAE Aerospace Standard AS6174: Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel
- SMT Corp. – Miscellaneous charts and images on sample counterfeit parts
- IDEA-STD-1010-B: Acceptability of Electronic Components Distributed in the Open Market
- “Addressing Obsolescence – The Uprating Option.” M. Pecht, D. Humphrey, IEEE Transactions on Components and Packaging Technologies, V31, No. 3, September 2008
- <http://counterfeitparts.wordpress.com>
- <http://www.acq.osd.mil/dpap/index.html>
- <http://www.integra-tech.com/>
- “Reliability Concerns for COTS Microelectronics in Space & Military Applications.” M. Sandor & S. Agarwal, EEE Parts Microelectronics Reliability and Qualification Workshop, 1998