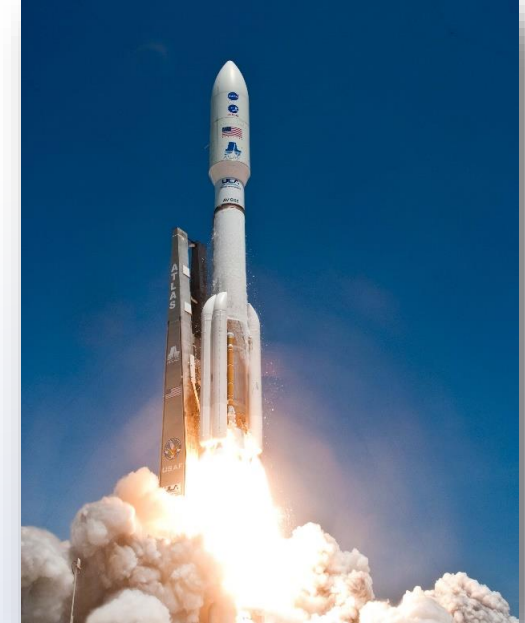


# ***NASA Counterfeit Parts Awareness and Inspection***



---

PRESENTED BY CARLO ABESAMIS & MARK LEBLANC



# Training Course Objectives

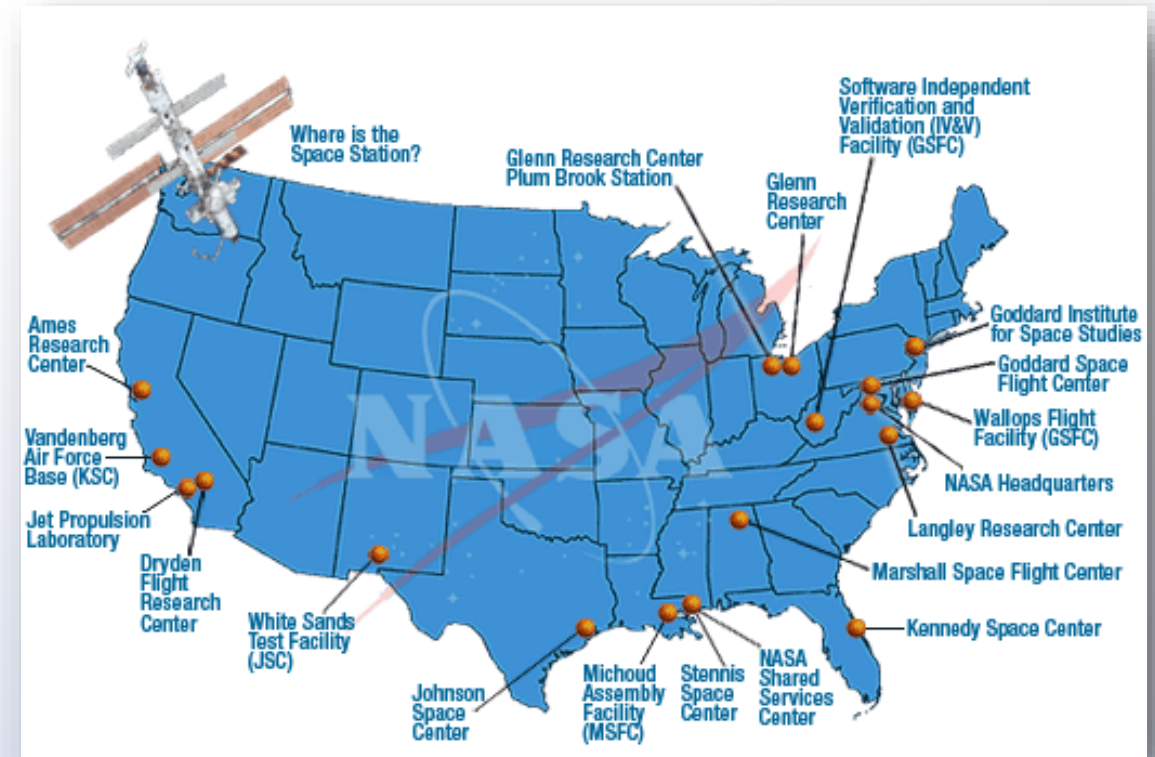
---

- Gain an understanding of the electronics parts counterfeit issue
- Gain knowledge of the supply chain environment for EEE parts
- Develop a familiarity with some of the methods used in counterfeiting
- Learn how to develop risk mitigation steps
- Learn hands-on verification and inspection processes for the detection of suspect parts



# Training Overview

- We Are the Explorers
- Landscape of Counterfeiting
  - Trends/ Definitions/ Origins of the Issue
- The Extent of the Problem
- Risk Mitigation
- Government/ Industry Flow downs
- Counterfeit Part Hands-On Training

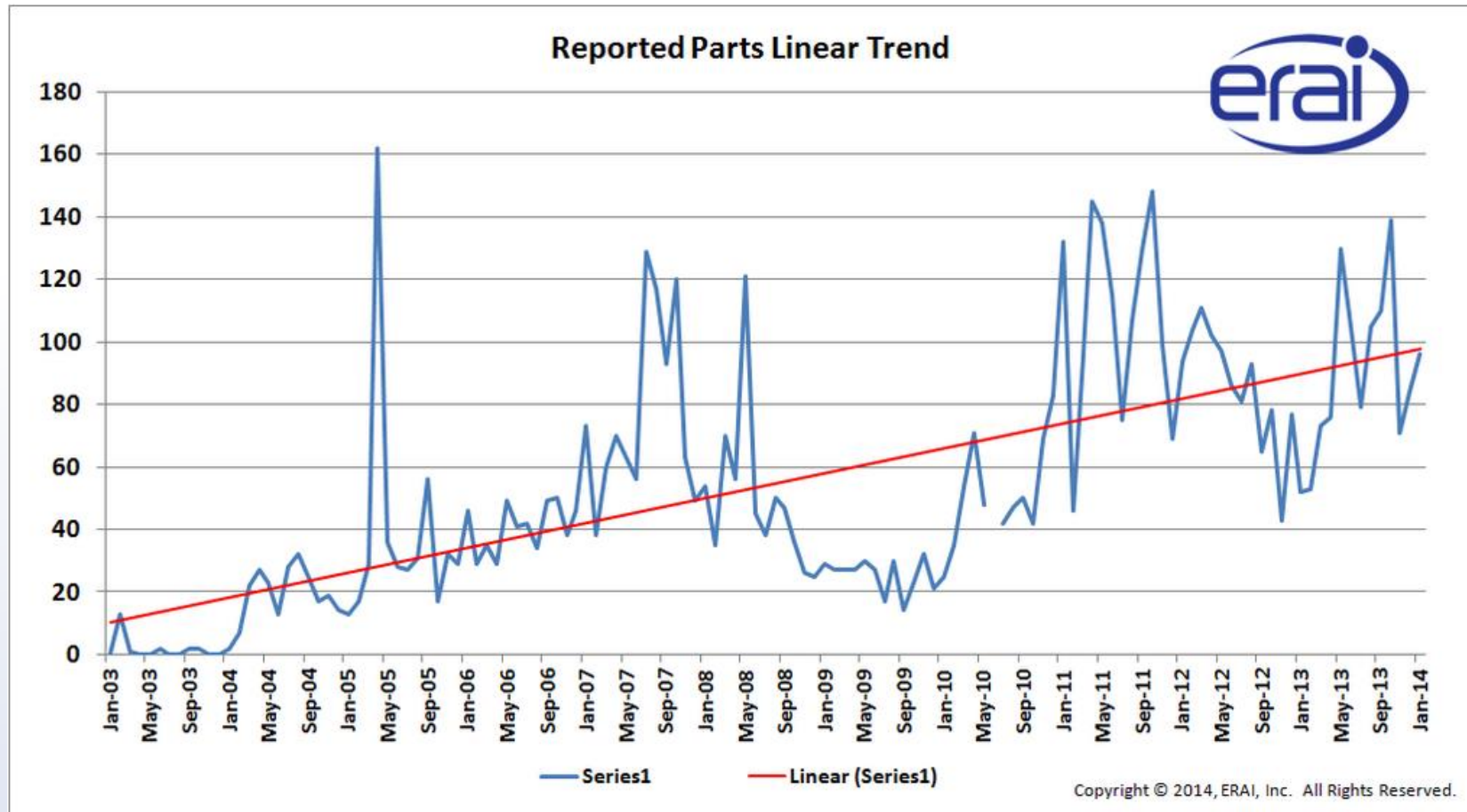


# Section 1 – the Landscape of the Counterfeiting Issue

---

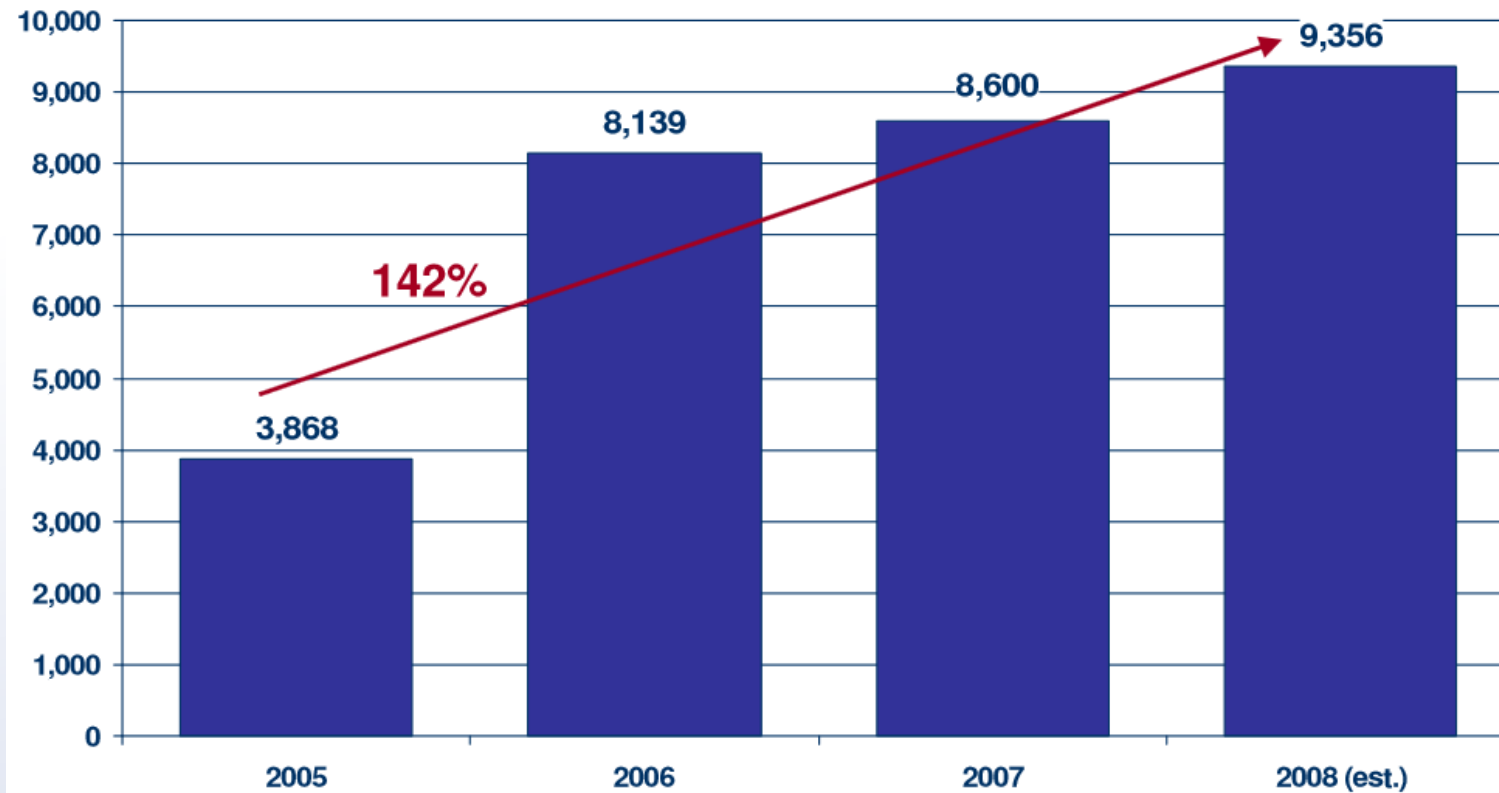


# An Increasing Threat





# Total # of counterfeit incidents

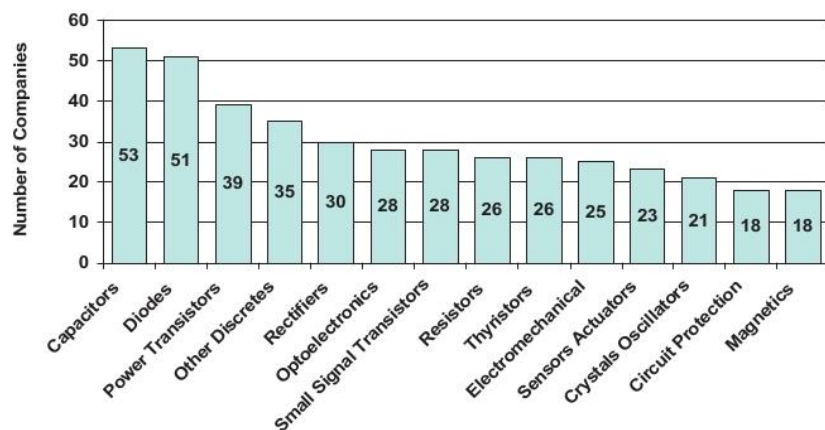


U.S. Dept of Commerce: Office of Technology Evaluation. Defense Industrial Base Assessment: Counterfeit Electronics 2010



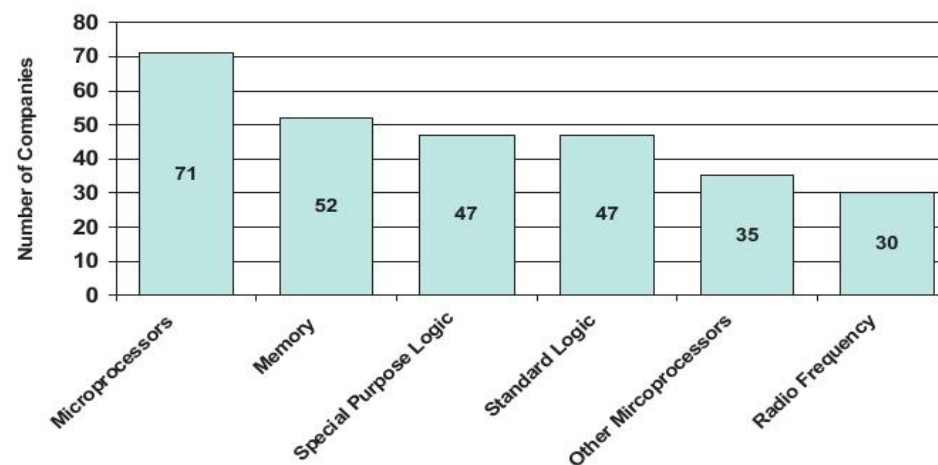
# Commonly counterfeited parts

**Figure VII-3: Types of Parts Suspected/Confirmed to be Counterfeit - Discretes**



Source: U.S. Department of Commerce, Office of Technology Evaluation, Counterfeit Electronics Survey, November 2009.

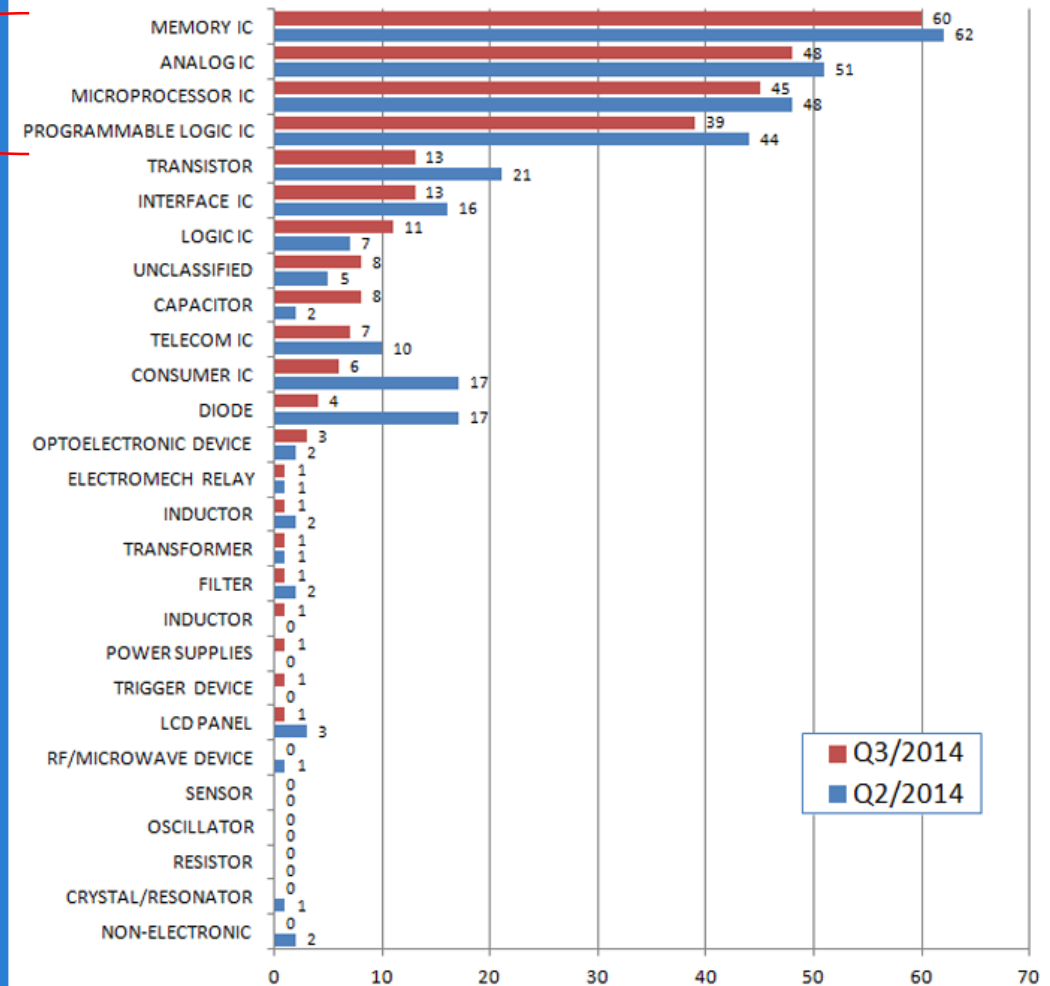
**Figure VII-4: Types of Parts Suspected/Confirmed to be Counterfeit - Microcircuits**



Source: U.S. Department of Commerce, Office of Technology Evaluation, Counterfeit Electronics Survey, November 2009.

ICs still the most commonly parts suspected of counterfeit in 2014, dominate 82% of all reportings.

Types of Components Reported to ERAI in Q2 and Q3 of 2014



Copyright © 2014, ERAI, Inc. All Rights Reserved.





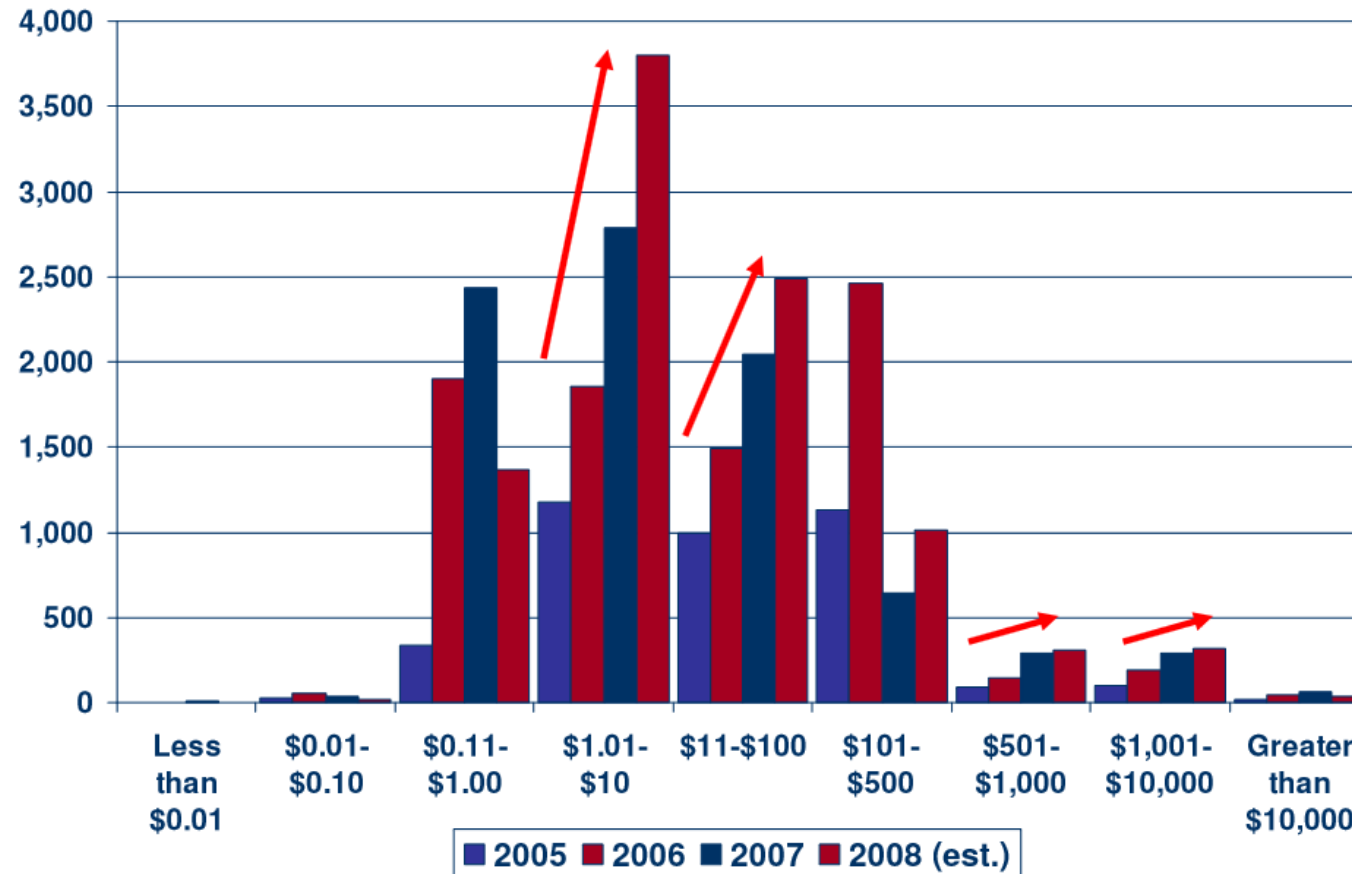
# Types of Counterfeit Incidents

Type of Product	2005	2006	2007	2008 (est.)
Industrial/Commercial	1739	4860	3841	2839
Consumer	154	345	398	531
<b>High Reliability – Industrial</b>	<b>49</b>	<b>81</b>	<b>164</b>	<b>488</b>
<b>Qualified Manufacturers List (QML)</b>	<b>49</b>	<b>77</b>	<b>161</b>	<b>261</b>
<b>Critical Safety</b>	<b>42</b>	<b>63</b>	<b>93</b>	<b>277</b>
<b>Qualified Products List (QPL)</b>	<b>16</b>	<b>39</b>	<b>111</b>	<b>144</b>
High Reliability – Medical	1	24	58	105
ITAR Controlled	15	10	67	19
Commercial Aviation	9	15	17	27
High Reliability – Automotive	2	6	8	25
Generalized Emulation Microcircuits (GEM)	0	0	0	2

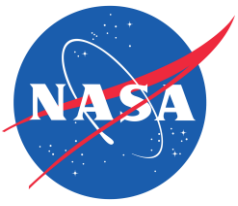
U.S. Dept of Commerce: Office of Technology Evaluation. Defense Industrial Base Assessment: Counterfeit Electronics 2010



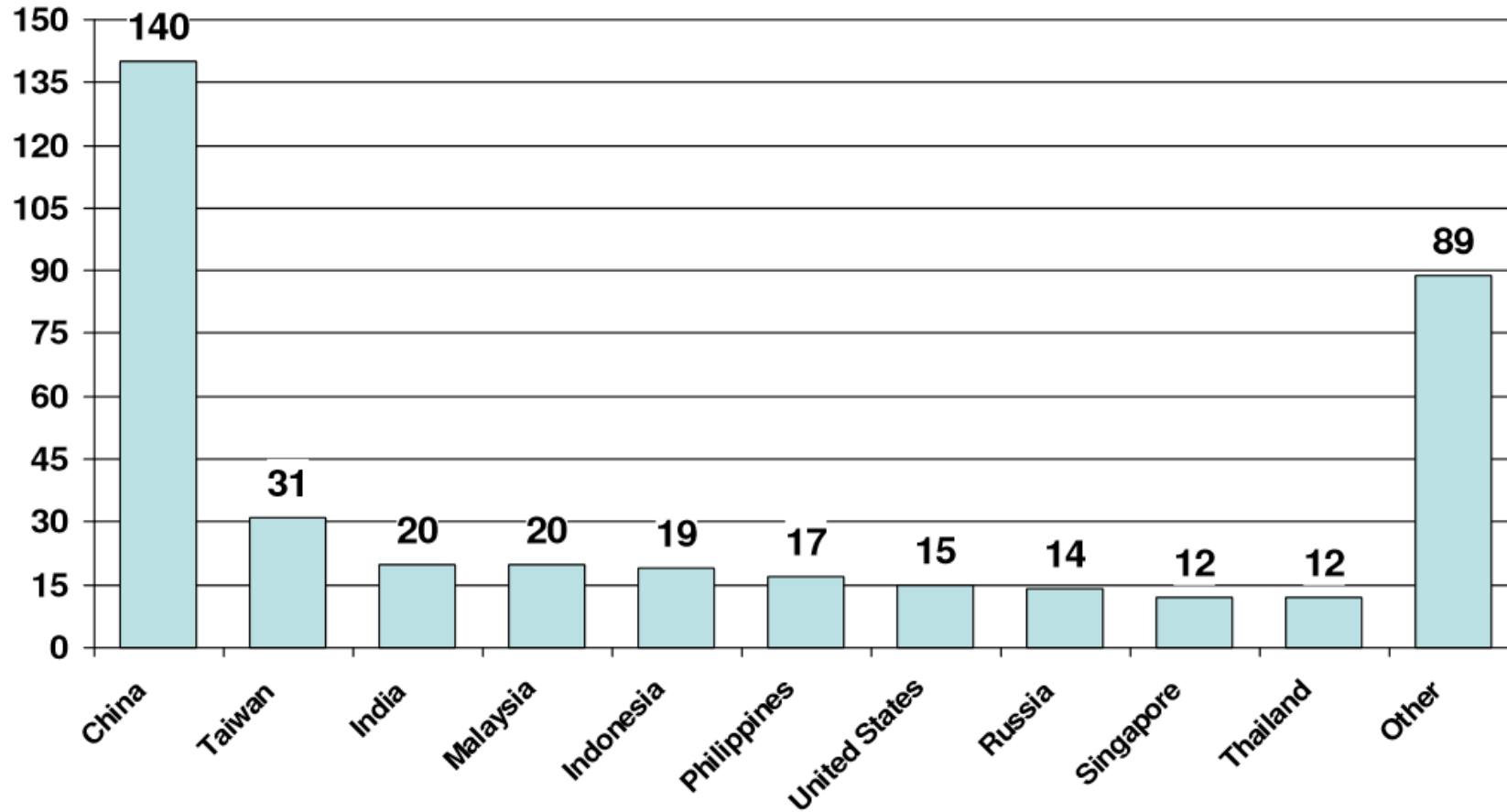
# Incidents by Product Resale Value



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



# Top countries suspected/ confirmed to be Sources of Counterfeits



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



# What is the largest problem area?

---

- Integrated circuits
  - 82% of all reportings
- High reliability and critical safety at risk
- \$0.10-\$100
- Parts largely procured or imported from the east Asia.



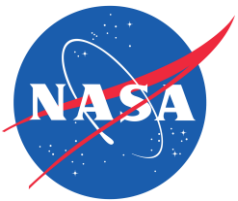
# Counterfeit Electronic Part (AS5553)

---

- **COUNTERFEIT PART:** A suspect part that is a copy or substitute without legal right or authority to do so or one whose material, performance, or characteristics are knowingly misrepresented by a supplier in the supply chain.

Examples of counterfeit parts include, but are not limited to:

- 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.



# Counterfeit Electronic Part (DFARS)

---

**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.

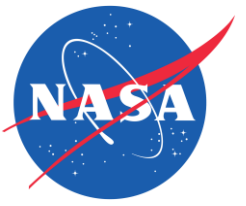
Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.



# Suspect Electronic Part

---

- **SUSPECT PART:** A part in which there is an indication by visual inspection, testing, or other information that it may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent part or counterfeit part provided below (AS5553).
- **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. (DFARS)



# In need of parts?

---

With many possible routes of part procurement, what are the routes that have less risk of procuring suspect/ counterfeit parts?







# 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.



# Sources of Supply

---

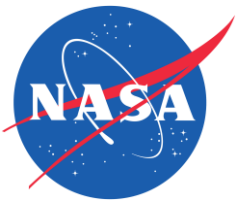
- **OPEN MARKET:** The trading market that buys or consigns primarily OEM and Contract Manufacturer's **excess inventories** of new electronic parts and subsequently utilizes these inventories to fulfill supply needs of other OEMs and contract manufacturers, often due to urgent or obsolete part demands.
- **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. See definition of "Authorized (Franchised) Distributor."



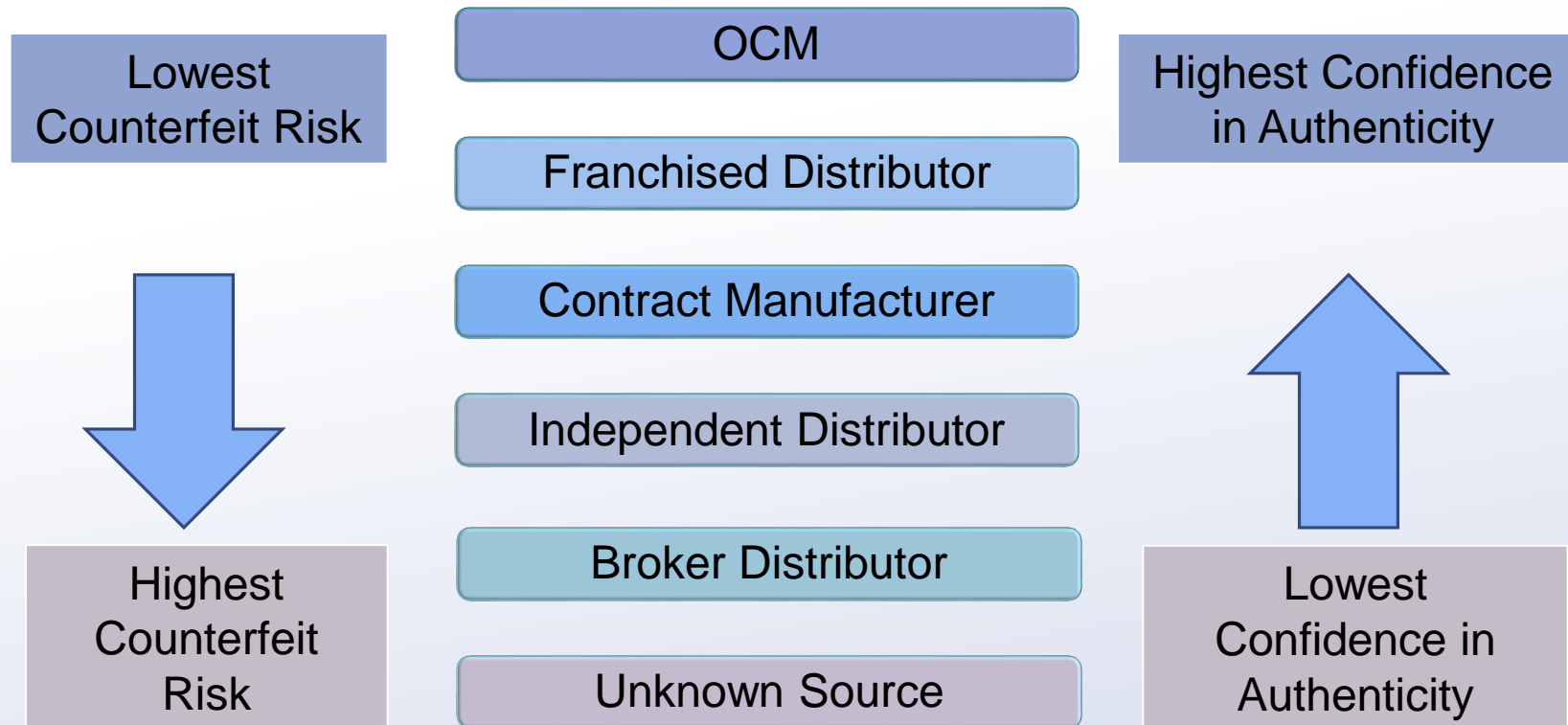
# Sources of Supply

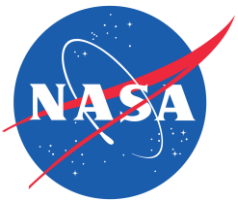
---

- **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.
- **APPROVED SUPPLIER:** Suppliers that are formally assessed, determined to provide acceptable risk of providing counterfeit parts, and entered on register of approved suppliers. Formal assessment can be performed by the procuring Organization or by a third party.



# the “Procurement Decision”



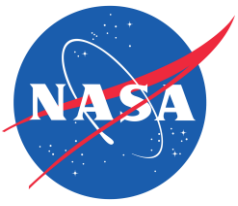


# How do independent distributors obtain parts?

---

- OCMs and Authorized Suppliers
  - Purchase parts directly to fill their stock
- OEMs and Contract MFGs
  - Buy excess stock no longer needed
- Other Unauthorized suppliers
  - Brokers
  - Independent distributors

} Highest Risk

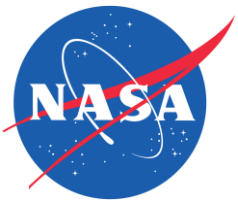


# SASC Investigation

- Investigation into counterfeit electronic parts in the DoDs supply chain, 2009-2011
- Many of the investigators pointed to China as a source for counterfeit electronics
- ASC staff were refused access to China
- Many of these parts came from resale points in the U.S., U.K., and Canada







# SASC Investigation

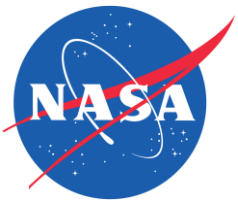
---

- 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
  - Parts sold by US companies originally from China!



Photo courtesy of: <http://static.progressivemediagroup.com/uploads/imagelibrary/dfg.jpg>

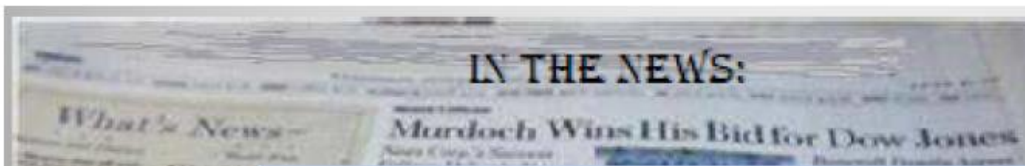




# Factors rendering defense/ government supply chain susceptible

---

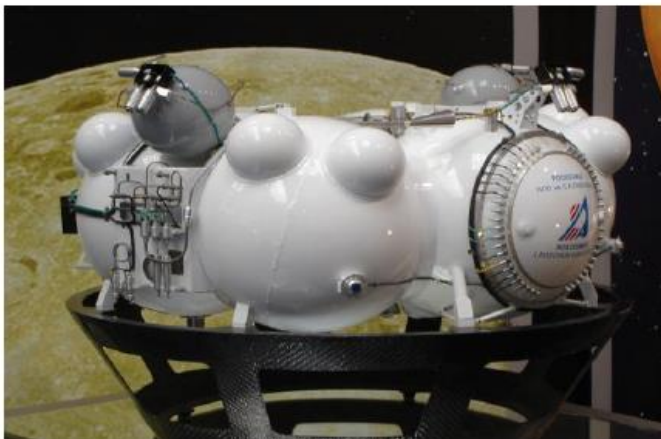
- Defense systems utilize military/ commercial-grade obsolete parts
  - Forces procurement from independent brokers and distributors
- Complexity of counterfeit trade
- Inaction of other governments to stop the manufacturing and distribution of counterfeit goods



### 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.

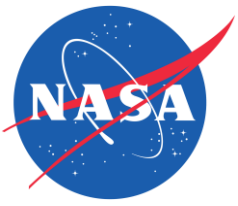
**Report cites malfunctioning WS512K32 chip (a single-package assembly of *static random access memory (SRAM)* chips) suspected to be counterfeit**



Mockup of Phobos-Grunt main propulsion unit

# Section 2 – the Extent of the Problem

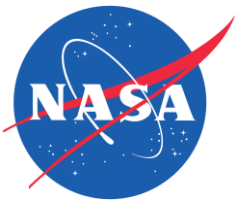
---



# Ways counterfeit parts re-enter the supply chain

---

- E waste
- Parts on the internet
- Excess Inventory
- Cloning/ Uprating
- Returns
- Value Added Processes



# The problem of E-waste

- Electronics Recycling is now the fastest growing solid waste stream in the world
- E-waste has “turned into an abundance of discrete electronic components and microcircuits for counterfeit parts” (Dept of Commerce)
- EPA estimated 2012 E-waste at 3.4 million tons
  - Only 29.2% is recycled
- EPA estimated 423k tons of computer disposed of in 2010
  - That’s 51 million computers!



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



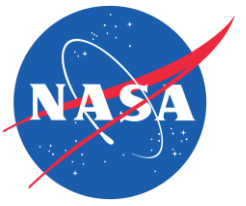


# The problem of E-waste

- E-waste stream creates opportunities for counterfeiters
  - A rich material source of product at the end of service life
  - Counterfeiters re-mark recycled e-waste with different part numbers, recent date codes, uprated characteristics and return it to the supply chain
  - Multiple opportunities for the introduction of counterfeit parts into the supply chain
- the “Digital Dumping Ground”
  - <http://www.pbs.org/frontlineworld/stories/ghana804/>



Source: the Basel Convention



# The problem of E-waste





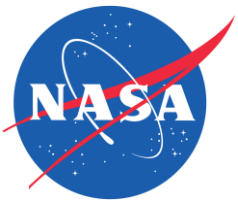


# The problem of E-waste

- Responsible Electronics Recycling Act-require domestic recycling of all untested, nonworking electronics



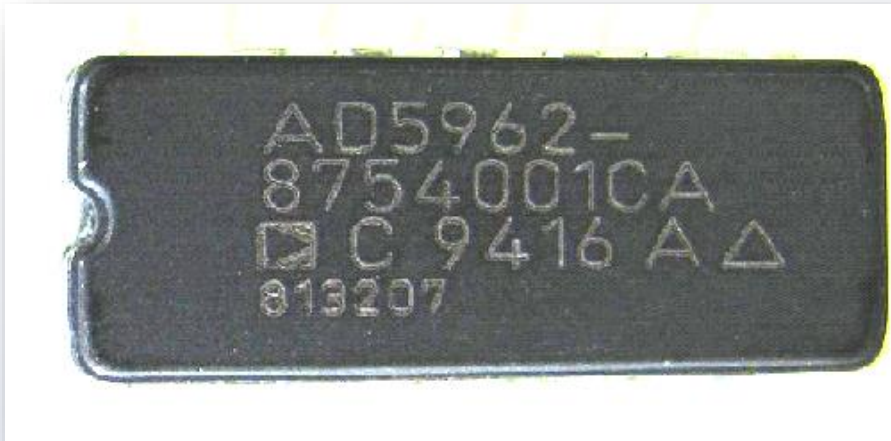




# False Advertising – Mil or Commercial

## Analog Device's AD585 Amplifier

- MILITARY GRADE QUALITY ASSURANCE LEVEL
- TEMPERATURE RANGE: -55C TO 125C
- INDUSTRIAL GRADE QUALITY ASSURANCE LEVEL
- TEMPERATURE RANGE: -25C TO 85C





# False Advertising – Mil or Commercial

- Pricing through Analog Devices site:
  - Military Grade >60 dollars more expensive
- Counterfeiters will falsify documents saying your purchasing a military grade when its 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	Prod'n	20 ld LCC	20	Mil	\$79.75	\$72.08	Tube, 54
5962-8754001CA	Prod'n	14 ld CerDIP	14	Mil	\$84.32	\$76.21	Tube, 25
AD585SCHIPS	Prod'n	CHIPS OR DIE	-	Ind	\$10.30	\$10.30	Tray, 100
AD585AQ	Not Rec**	14 ld CerDIP	14	Ind	\$22.43	\$20.30	Tube, 25
AD585JP	Not Rec**	20 ld PLCC	20	Comm.	\$20.53	\$18.55	Tube, 49
AD585JP-REEL	Not Rec**	20 ld PLCC	20	Comm.	-	\$18.55	Reel, 1000
AD585JP-REEL7	Contact ADI	20 ld PLCC	20		-	-	Reel, 250
AD585JPZ	Not Rec**	20 ld PLCC	20	Comm.	\$18.70	\$16.91	Tube, 49
AD585JPZ-REEL7	Not Rec**	20 ld PLCC	20	Comm.	-	\$16.91	Reel, 250
AD585SCHIPS	Prod'n	CHIPS OR DIE	-	Mil	\$36.77	\$36.77	Tray, 100
AD585SE	Prod'n	20 ld LCC	20	Mil	\$59.81	\$54.04	Tube, 54
AD585SE/883B	Prod'n	20 ld LCC	20	Mil	\$80.68	\$72.92	Tube, 54
AD585SQ	Prod'n	14 ld CerDIP	14	Mil	\$62.04	\$56.10	Tube, 25
AD585SQ/883B	Prod'n	14 ld CerDIP	14	Mil	\$80.65	\$72.91	Tube, 25



# Excess Inventory

---

- Excess inventory sold by OEM or authorized supplier in open market to non-franchised distributors
  - Counterfeits most often enter the supply chain through the open market
- Increased risk, inventory not managed the same way
- Original supplier's warranty no longer honored



# 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
- Some suppliers are no longer selling previously returned items to aerospace/ space flight industry



# Returns




- 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

 GOVERNMENT - INDUSTRY DATA EXCHANGE PROGRAM <b>PROBLEM ADVISORY</b>		
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



# Value added processes

---

- Any value added process sent out to another company creates risk
  - Such as further part level testing
  - MFG processes



Photo courtesy: engineeredtaxsolutions



# 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





# American Conspirators

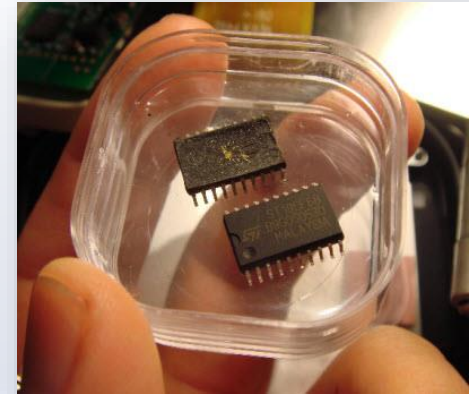
- Supplier D (independent distributor)
  - Nine employees
  - Sold large amount of semiconductor chips to 1,100 customers
    - Sold to every sector, most of devices have not been recovered
    - “it is impossible to retrieve the hundreds of thousands of counterfeit devices sold by Vision Tech”
  - Firm sold chips for over a five year period
  - Imported chips from China through various U.S. ports
    - 3263 shipments (59k parts) often changing the name of what they were importing
  - \$16 million counterfeiting operation
    - \$7.5 million for purchase of goods
    - \$14,742 testing

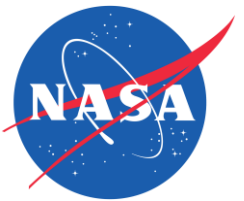




# American Conspirators

- Chips showed signs of black topping, incorrect P/Ns and date codes
- Chips were sold as “military grade” from Germany but were counterfeits from China
- Bait and switched good samples for companies to test
  - Used Armor all to make parts appear shiny
  - Forged CofCs
  - Returned chips returned and sold to another customer
- Employees were both arrested in Florida.
  - Police seized luxury vehicles, motorcycles, motor home, beach home and four other properties





# American Conspirators

- Supplier D prosecuted and charged with paying restitution to the companies it sold to and falsely represented

Total restitution to be ordered, per victim, all categories combined:

Altera	\$7,611.00
AMD	\$34,900.00
Analog Devices, Inc.	\$76,580.66
Cypress Semiconductor Corp.	\$33,446.00
Infineon Technologies, AG Corp.	\$10,036.00
Intel Corporation	\$100,889.50
Intersil	\$1,857.30
Electronics, N.V.	\$1,130.00
Linear Technologies, Corp.	\$32,018.75
Maxim	\$1,596.34
Mitel	\$2,645.93
Freescale <sup>35</sup>	\$40,021.00 <sup>36</sup>



# American Conspirators

---

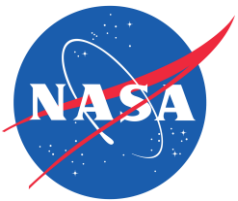
- Supplier E
  - Irvine, CA
  - Scheme ran from for only two years
  - Imported counterfeit parts under various company names
  - Falsified test reports/ material certs
  - 302 domestic customers



# The Takedown of a Supplier

---

- Employee hired by Supplier E as Quality Control Engineering Tech
  - Original job function to decap parts in order to detect counterfeits
  - Later started to extract die in large quantities from used parts to “refurbish”
  - Realized Supplier refurbishment process meant inserting used die in new packaging and selling as military grade
  - Secretly began informing customers and authorities about what was happening
  - In 2009, Supplier raided by NCIS (Navy Counter Intelligence Services)



# Potential parts in the supply chain

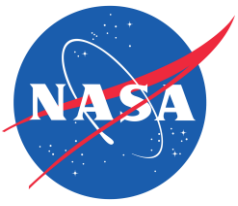
- The most popular part, ICM7170 IPG, was bought for \$.02 and on average sold for \$38.00 each as an ICM7170"**A**"IBG's equaling a potential gross profit of \$2,000,000 per month.
- 8 operators x 325 pieces per day = 2600 daily
- 2600 parts x 5 days x 4 weeks = 52,000 monthly
- Over 400k produced during MVP life cycle
  - Where are they now?



[http://www.usbid.com/assets/partphotos/89/ICM7170AIBG\\_0014062.jpg](http://www.usbid.com/assets/partphotos/89/ICM7170AIBG_0014062.jpg)

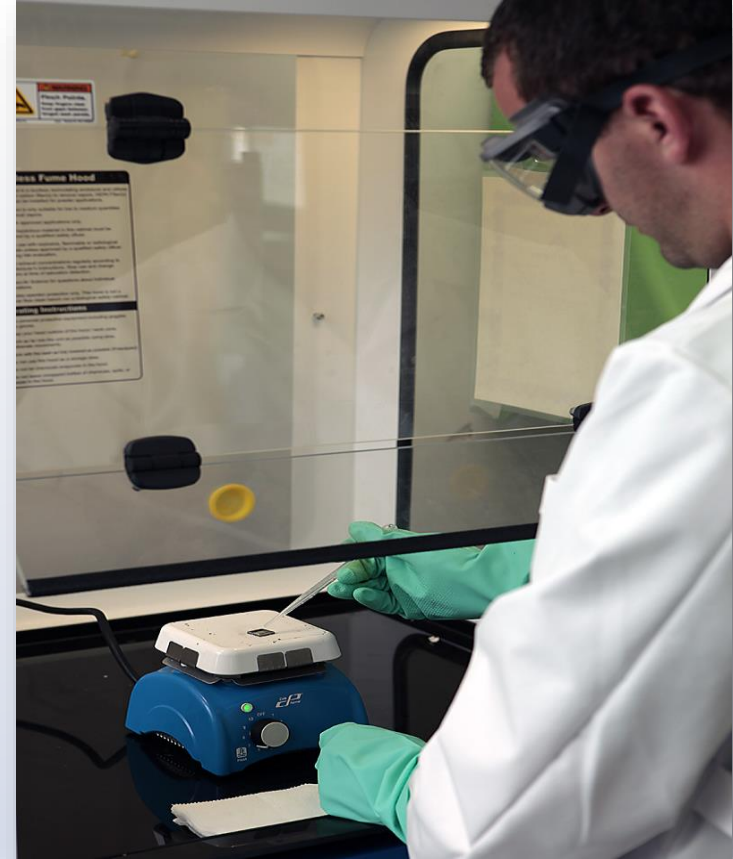


[http://i.ebayimg.com/00/s/MT1wMFgxNJAw/z/thoAAOxy6-tR-OYe/\\$T2eC16FHJHgFmDU0F7eBR-OYd03hw~60\\_35.JPG](http://i.ebayimg.com/00/s/MT1wMFgxNJAw/z/thoAAOxy6-tR-OYe/$T2eC16FHJHgFmDU0F7eBR-OYd03hw~60_35.JPG)



# Step 1 -Repackaging a die

- Decapsulation is the first step in the process to repackage the die.
- To harvest the quantities needed to make a profit, it can be a very dangerous and dirty process.
- The operators were put under pressure to perform which increases the chance for accidents with the toxic and oxidizing acids and their fumes.
- The chemicals used are very hard on the die and bonding pads.



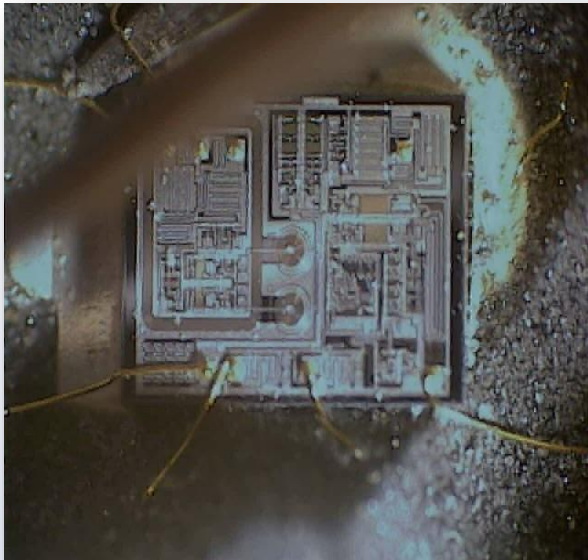




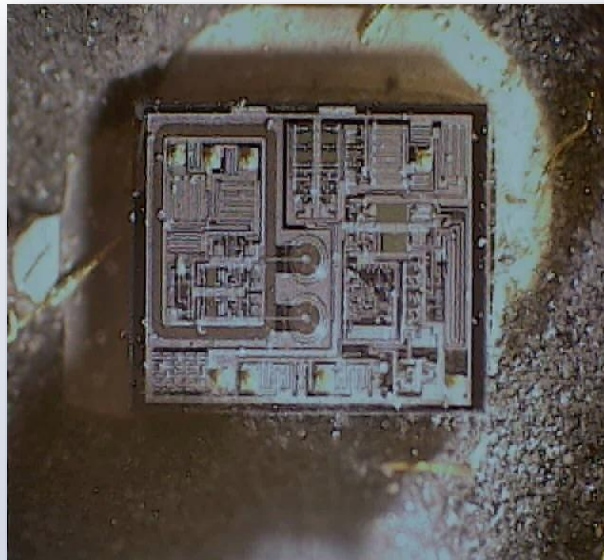
## Step 2 – Bond wire removal

- With precision tweezers and steady hands the operator must get under the wire and pull the wires the opposite direction of the ball bond attached to the pad.
- Breaking the wire at the top of bonds of a decapped part is the most difficult part of the this process without damaging the original ball bond.

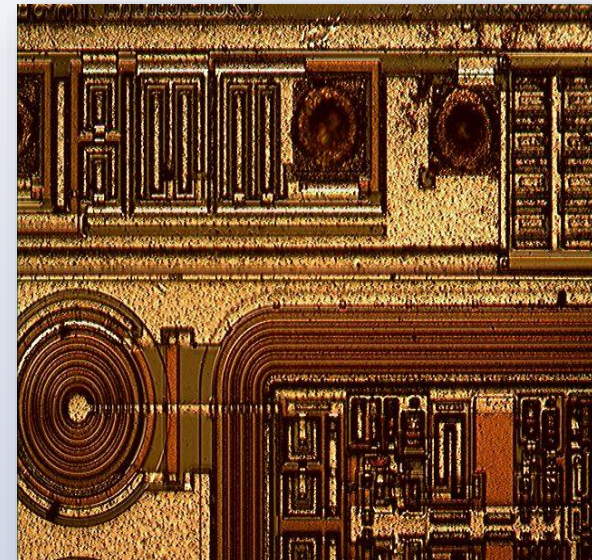
Plucking with tweezers



After plucking



Close up of bonding pad







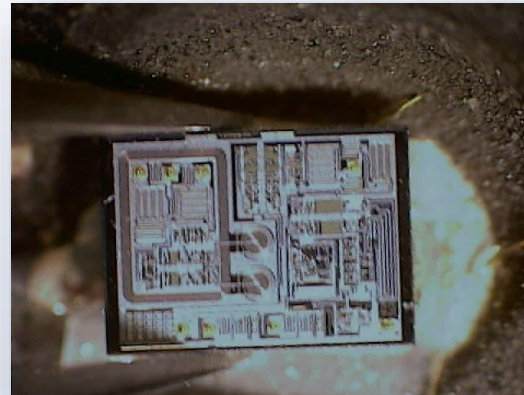
## Step 3 – Chip Removal

- To extract the die from the package and lead frame, the counterfeiter uses a hot plate not exceeding 100 degrees Centigrade to loosen the adhesive holding the die to the lead frame.
- The operator then uses an exacto knife and tweezers to pry the die gently off the lead frame or package mounting.

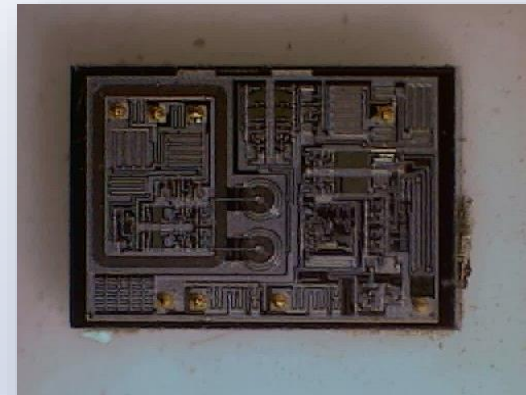
**Loosening of adhesive**

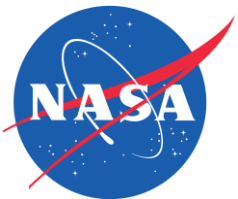


**Extraction process**



**Extracted die**





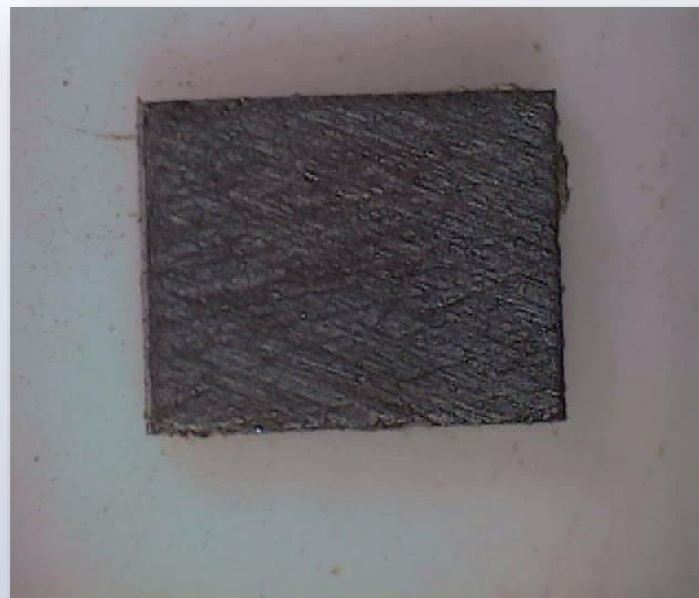
## Step 4 – Removing adhesive backing

- After the die is extracted the adhesive is left on the back of the die. The operator then sands the back to remove the adhesive leaving small abrasions that could later complicate the positioning of the die.

**Die back with remaining adhesive**



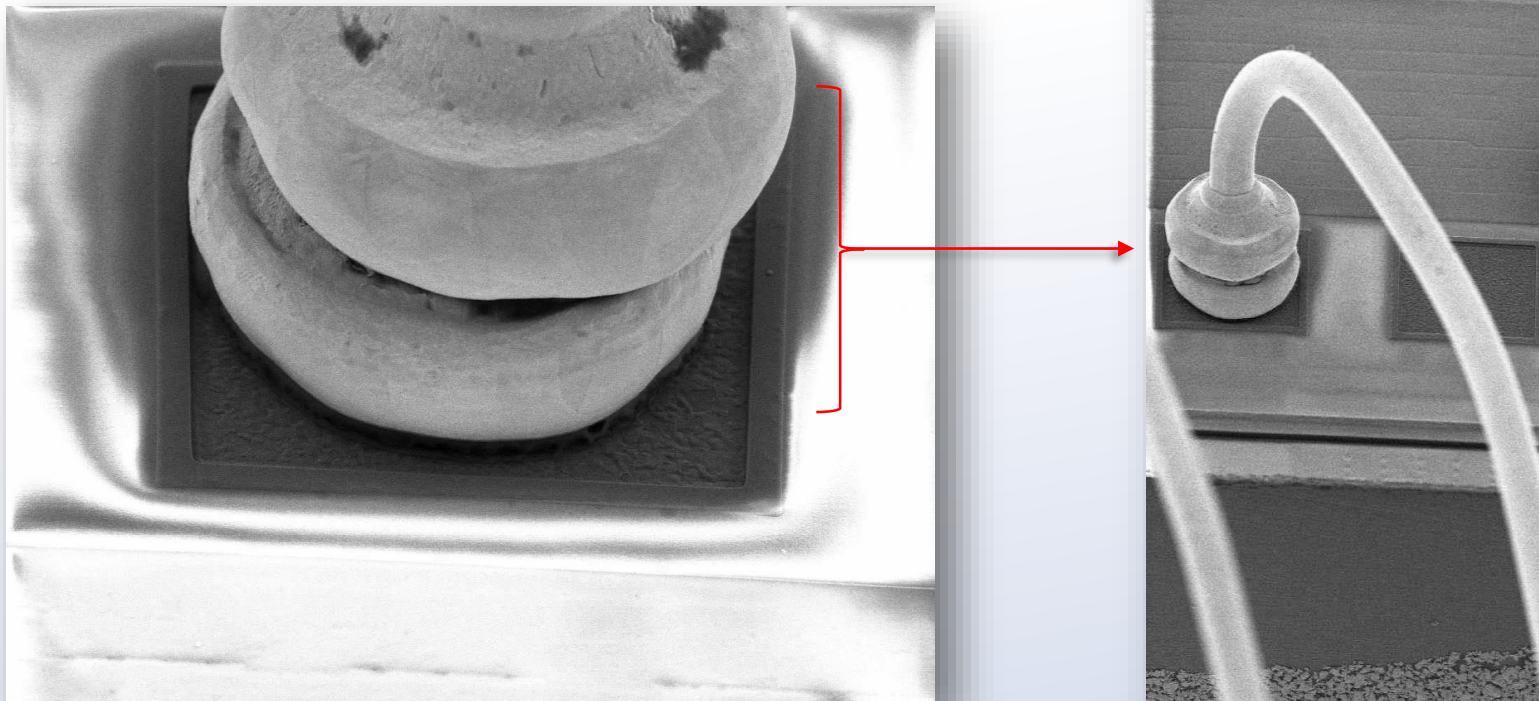
**Die back after adhesive sanded off**





## Step 5 – Bonding the New Package

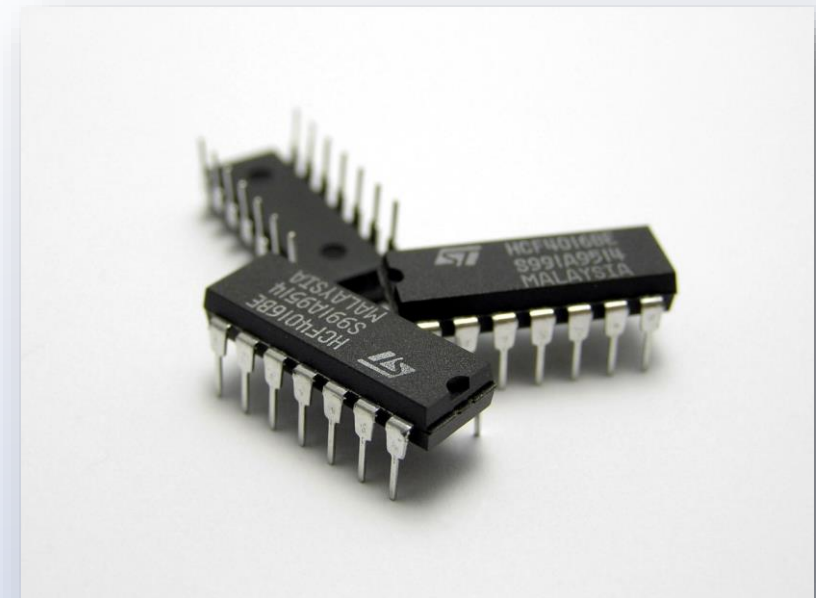
- The new wire bond is placed on top of the old ball providing a signature showing what has transpired.





## Step 5 – Finished product

- The finished product can look like the original. Once the components are complete they may undergo a simple electrical test, such as a curve trace, but the stresses from reclaiming and die harvesting can induce severe damage causing:
  - Lower life expectancy
  - Curve trace irregularities
  - Out of specification
  - Continuity failures
  - Unknown reliability







# Broker with Cage Code in California

Address is a private home

**Is this Broker selling genuine product?**

**Is he maintaining the product under proper conditions?**

**Do you Really Know this Supplier???**





# Harm from Counterfeits

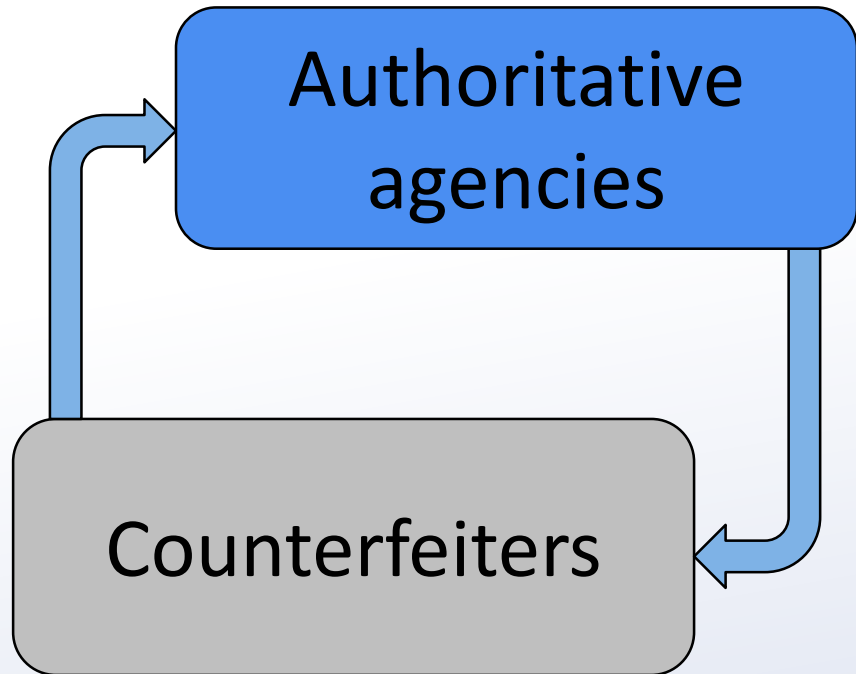
---

- Trademark holder & MFGs
  - Displaced sales, threat to public opinion, claims for warranty/ service
- Semiconductor industry and US economy
- Downstream buyers
- US military
  - Fail, performance, delay missions
  - Integrity and reliability of weapons
  - Safety of service personnel



# Counterfeiting is not static, it's dynamic!

- Counterfeiters are always one step ahead, new methods include:
  - Taking existing good commercial part, making it industrial grade, removing marking via laser ablation, then remarking – difficult to detect
  - Micro blaster/ sand blaster, removes even surface – difficult to detect
  - Removal of existing ink mark, no residue left, refined process – normal counterfeit detection will not work





# Section 3 – Risk Mitigation

---



# The importance of a risk mitigation plan

Created in response to significant and increasing risk of counterfeit electronic parts entering our supply chain

## Risks posed:

- Performance/ Reliability
- Cost/ Schedule



Photo courtesy of:  
<http://bayintegratedmarketing.files.wordpress.com/2012/07/parts.jpg?w=645>

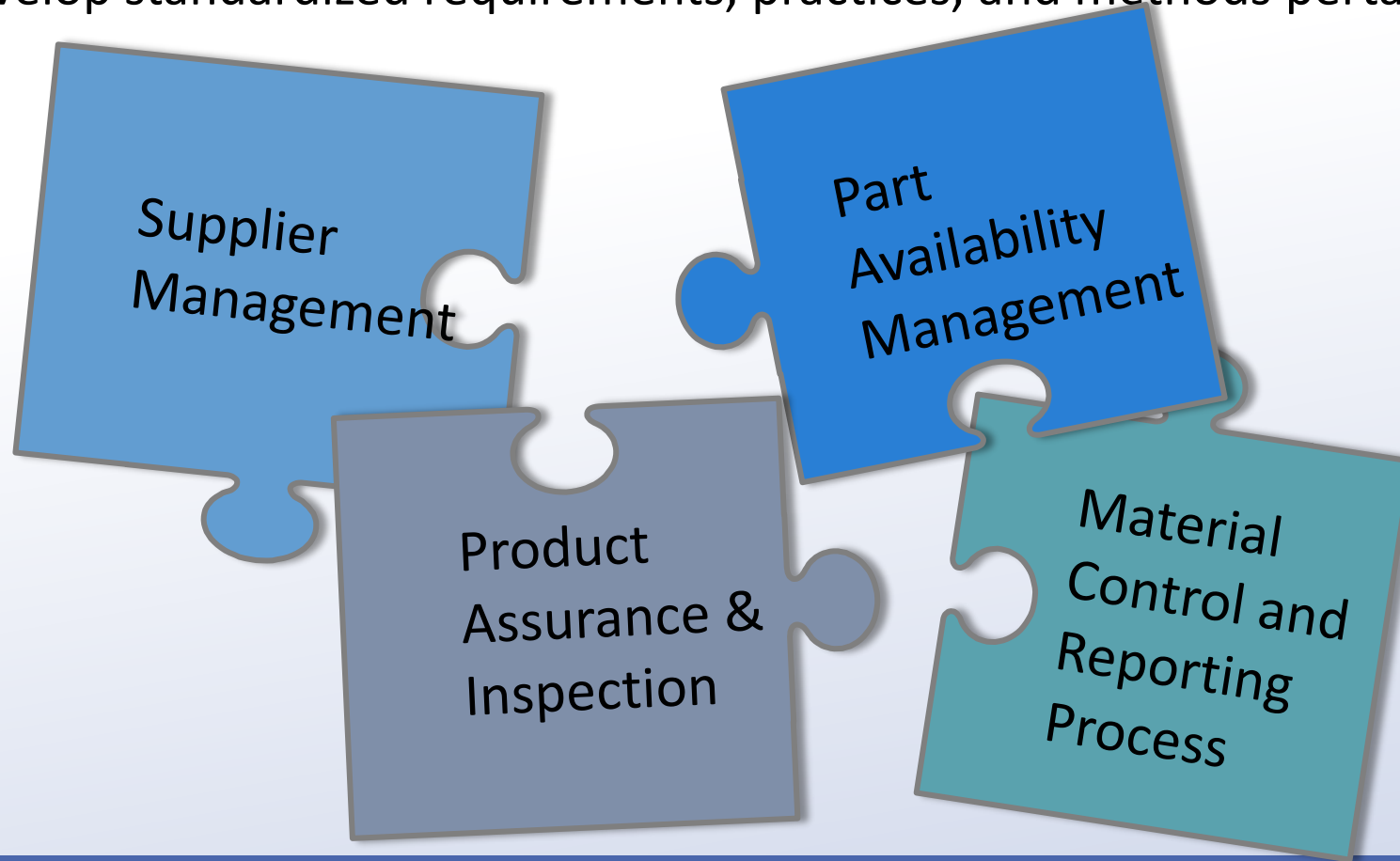


Photo courtesy of: <http://static.progressivemediagroup.com/uploads/imagelibrary/dfg.jpg>



# How is NASA trying to mitigate risk?

Develop standardized requirements, practices, and methods pertaining to:





# Supplier Management

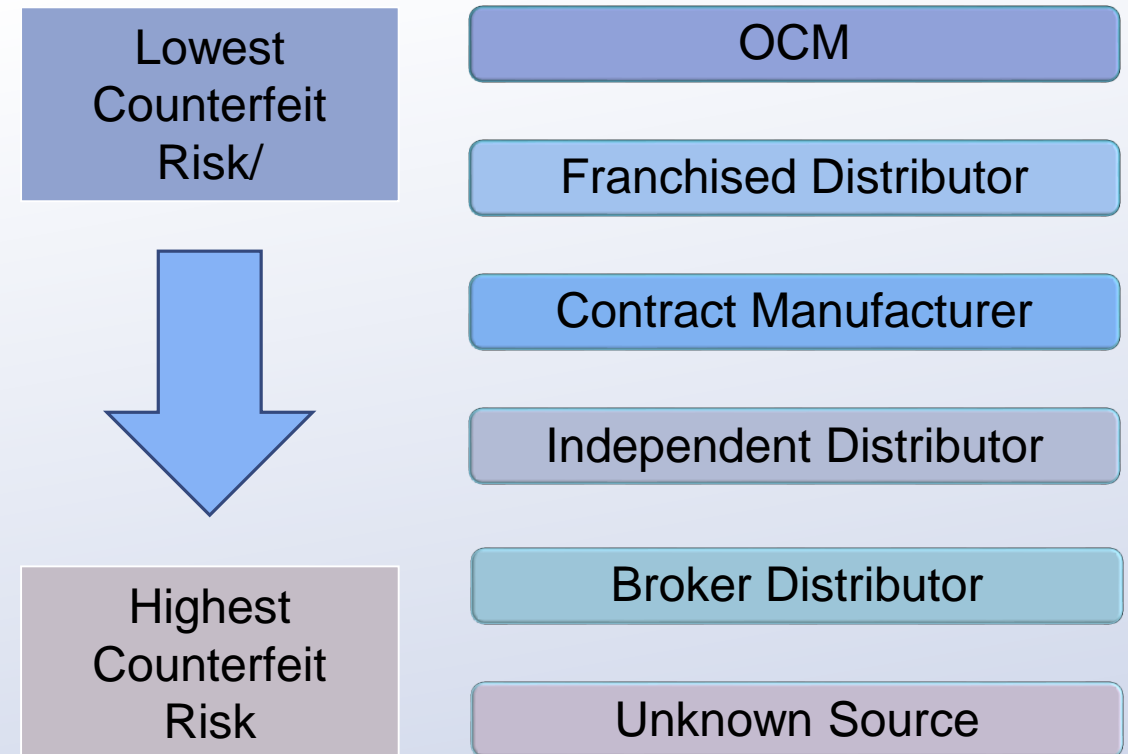
---

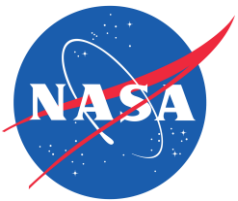
- Risks Include
  - Procurement of counterfeit parts
    - Returns process
  - Weak supplier selection process
  - Failure to detect and inspect counterfeit parts
  - Process in place is non-existent or inadequate in responding to counterfeit parts
  - Personnel unaware of counterfeit parts issue



# 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/ trends
  - Managing your supplier list
- Suppliers must demonstrate quality control, main source documentation history, and possess necessary certifications





# Supplier Management

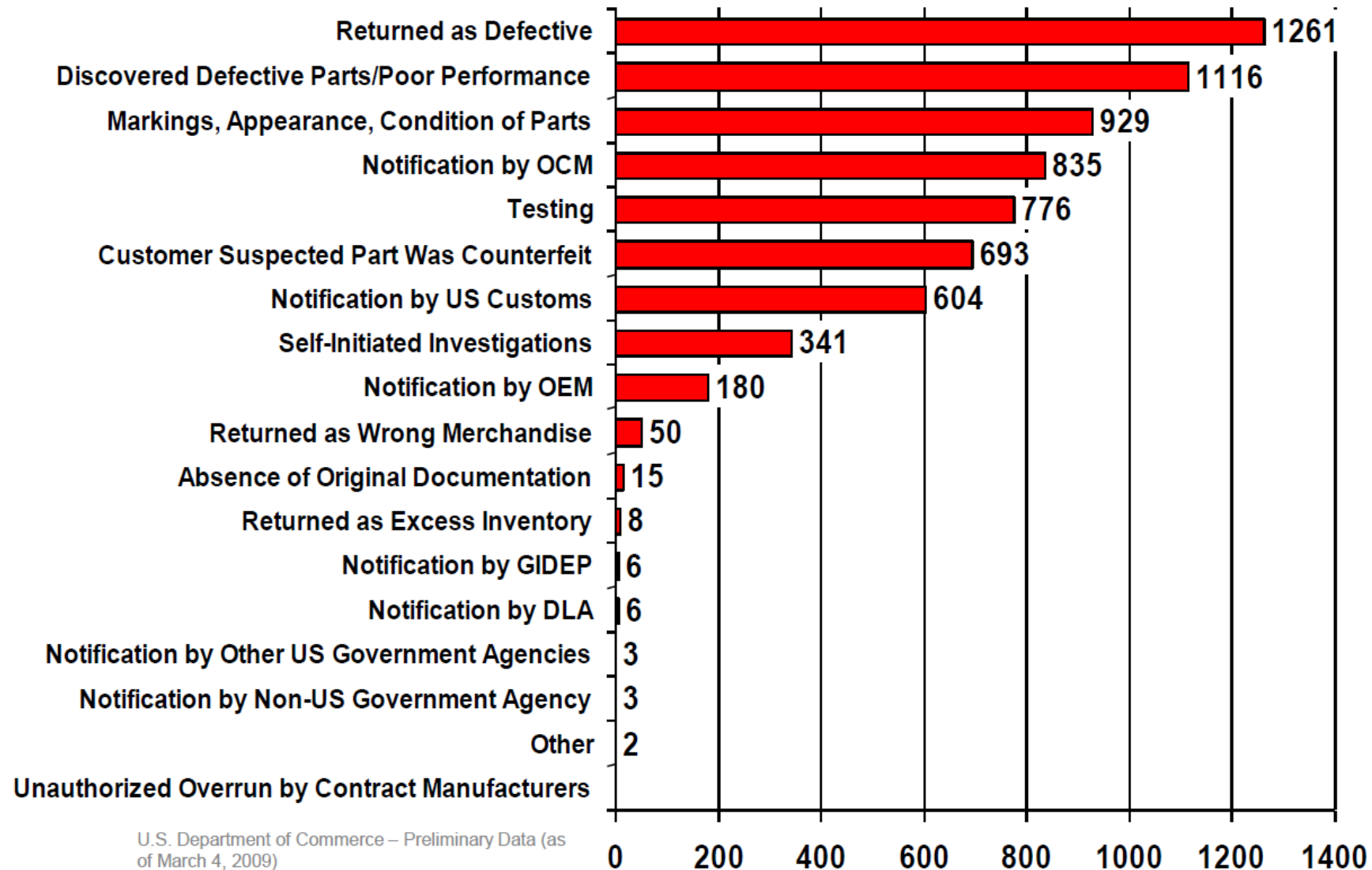
---

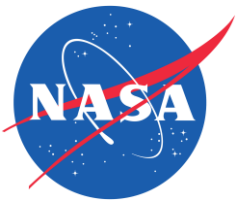
- Audits can reduce the risk of:
  - Breaking the chain of traceability of parts
    - Returns process
    - Outsourcing of work
  - Weak supplier selection process



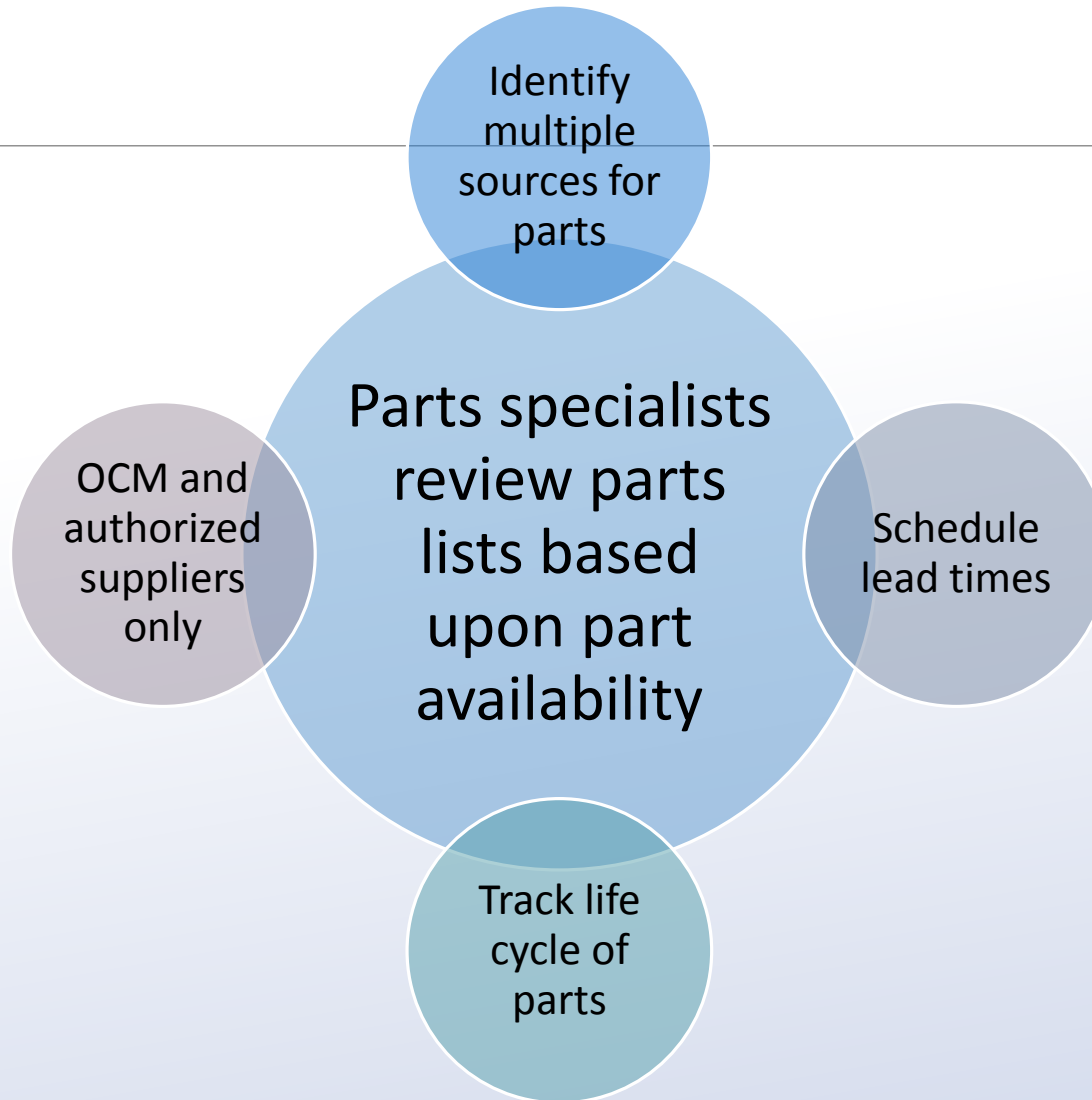


## How Companies are Uncovering Counterfeits



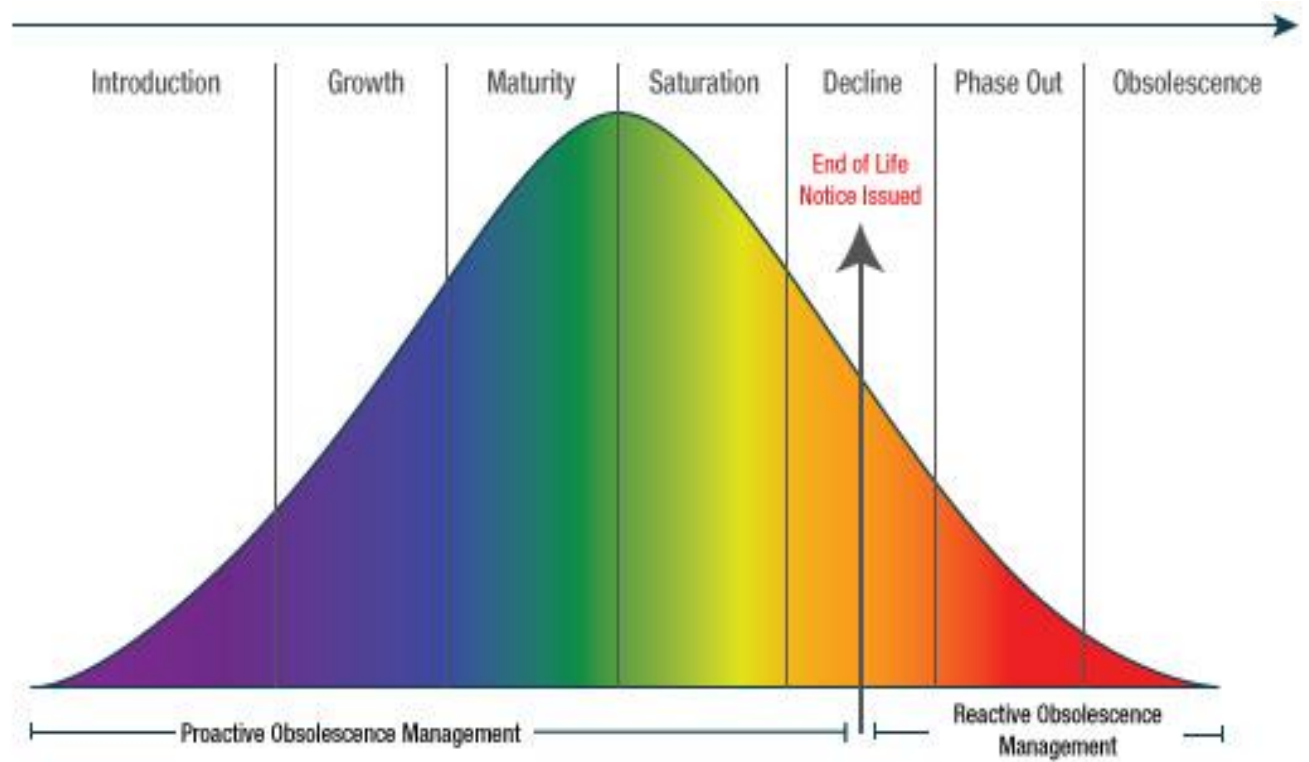


# Parts Availability Management

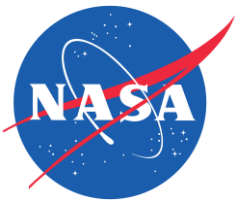




# Part Lifecycle (EOL, Last time buy)



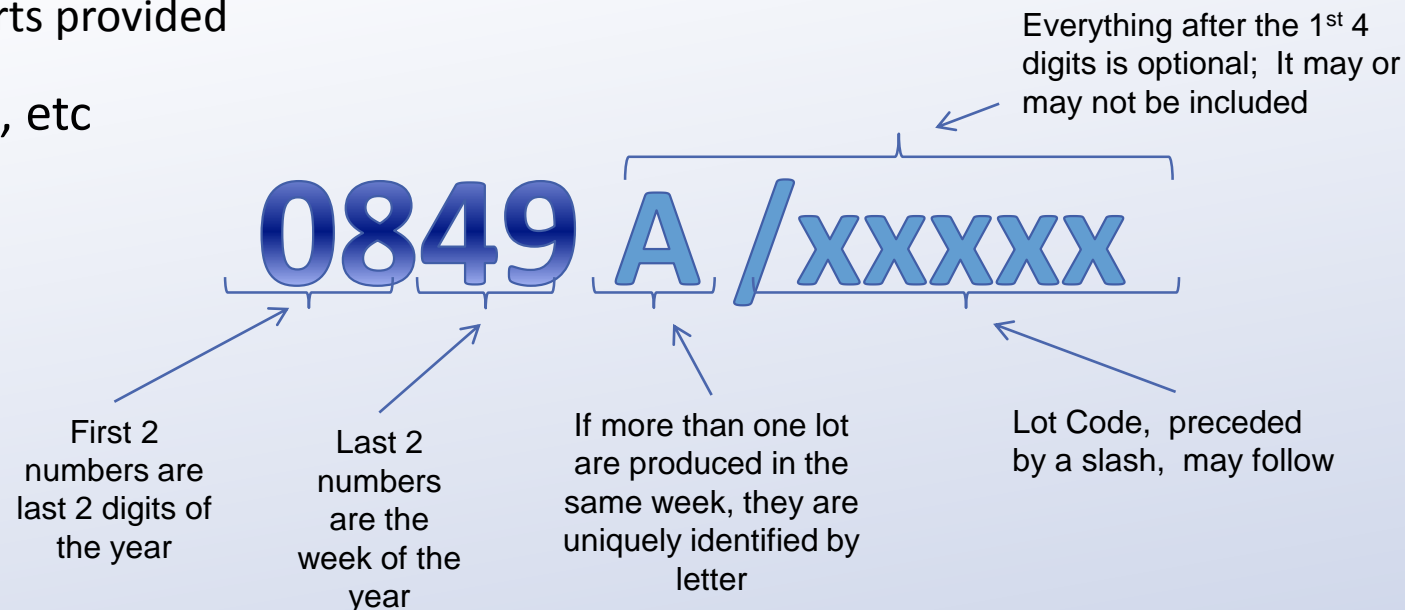
- Includes instructions for making a “last time buy” – often a window of 6-12 months is given for the customer to place an order
- Orders are generally NCNR
- Decisions should be made regarding procurement during project build



# Product Assurance & Inspection

- Inspection for all received flight parts
- Verify receipt of documentation (i.e. CofC, purchase order, packing list) to confirm authentic conforming parts and traceability to MFG
  - Traceable to specific manufacturer, part number, date code, lot number, and/or serial #'s
  - Assure QC's met and test/ material certs provided
- Visual, dimensional, electrical testing, etc
- Failure Analysis Lab

• Trust buy verify





# Product Assurance & Inspection

- **The Magic Part**

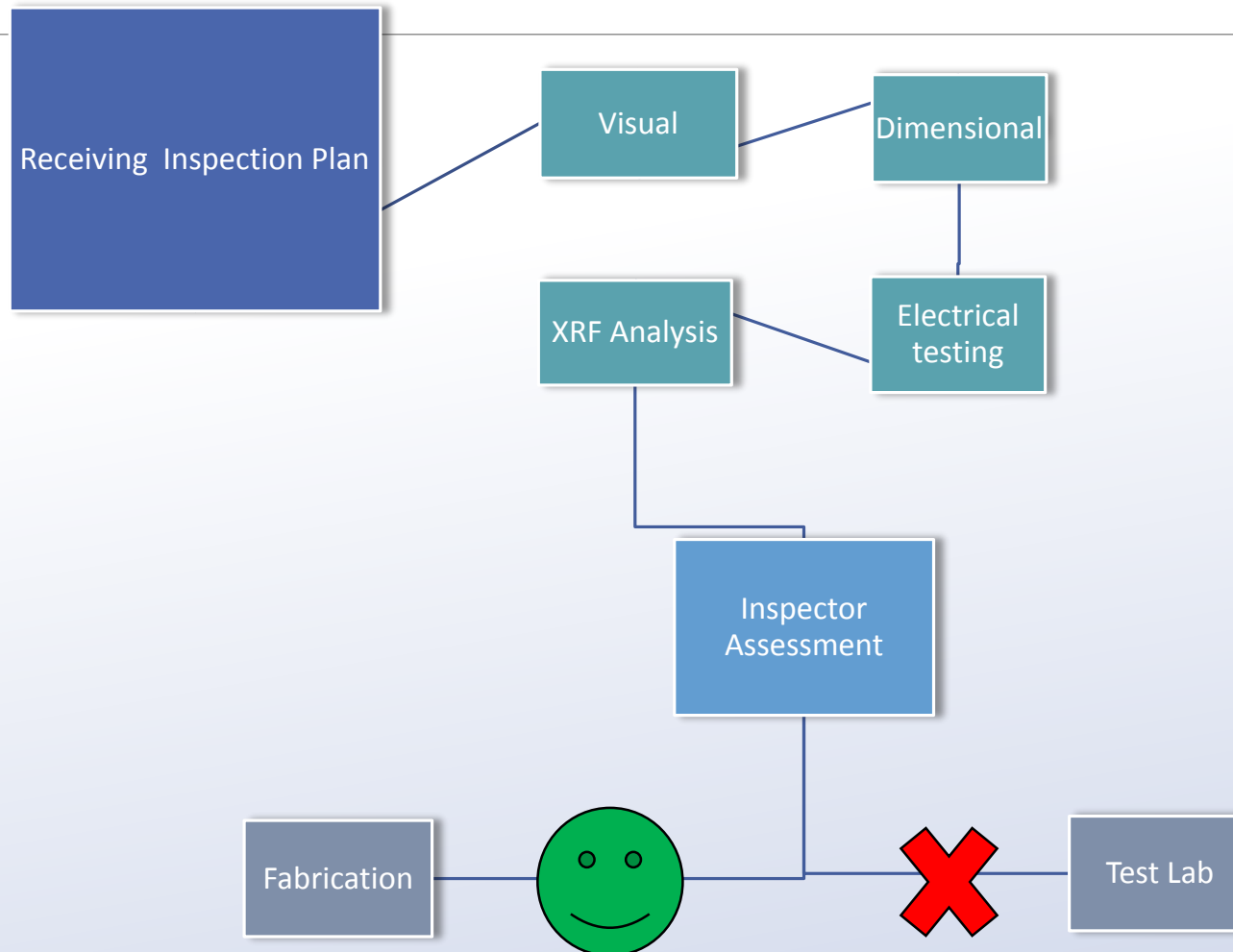
- Date code indicates:
  - Part was made in November of 2003 (47<sup>th</sup> week of 2003)
- Part was received on June 3, 2003



**Part marked with a date code five months into the future compared to the date of the receipt**



# Product Assurance & Inspection







# Material Control and Reporting Process

---

- Parts identified as suspect are tagged and segregated
- Further work can include further part testing/ assessment and communication with the supplier or OCM
- Upon conformation that a part is counterfeit, identify and place on “hold”
- Counterfeit parts are reported to the NASA Office of Inspector General and the NASA Director, Acquisition Integrity Program (AIP).
  - Reported in accordance with NASA GIDEP Advisory Program
  - Turn in counterfeit parts to investigative authorities



# NASA's counterfeit part mitigation foundation

---



# Section 4 – Government/ Industry Flowdowns

---



# National Defense Authorization Act

---

- Concerns over counterfeit part proliferation in U.S. government supply chain led to enactment of Section 818.
- Created Section 818 post SASC hearing
- Requires DoD to issue regulations regarding definition, prevention, detection, and reporting of actual/ suspected counterfeits in defense supply chain
- Law aims at **avoidance** of procurement of counterfeit parts

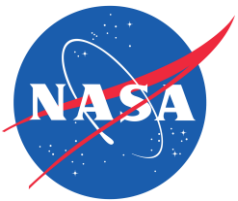


# NDAA Sec. 818

---

Contractors must detect and avoid use of counterfeit parts in DoD systems:

- Responsible for **all rework or corrective action**
- Procure parts from **OCMs or their authorized dealers**
- **Contractors to notify government** if parts procured from untrusted sources.
  - Requires additional inspection, testing, and authentication
- The DoD and its contractors shall establish a **mandatory reporting program** (GIDEP)
- Contractors must **established their own procedures and policies**
  - Flow down policies to subcontractors



# NDAA 2013 Sec. 833

---

- Covered contractors are not liable for the costs of counterfeit parts if (all three below):
  - The contractor has a DoD-approved counterfeit parts program
  - The parts were provided as Government property
  - The contractor provided timely notice of the counterfeit parts





# DFARS: 2012-D055

---

- Background:
  - DOD proposed to implement “Detection & Avoidance of Counterfeit Electronic Parts” of NDAA 2012
  - Issuance of DFARS regulations on contractor responsibilities
  - Applicable to CAS covered contractors
  - Requires CAS contractors to develop risk-based policies/ procedures that address 12 criteria
    - Direct implications for suppliers of those components
  - Contractors that are subject to the Cost Accounting Standards (CAS) and that supply electronic parts or products that include electronic parts and their subcontractors that supply electronic parts or products that include electronic parts, are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to do so may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments



# DFARS: 252.246.7007

---

- “A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas”:
  - 1) The training of personnel
  - 2) Inspection and testing of electronic parts
  - 3) Processes to abolish counterfeit parts proliferation
  - 4) Processes for maintaining part traceability
    - a) Tracking of supply back to OM
  - 5) Use of OMs and their authorized sources of supply
  - 6) Reporting and quarantining of counterfeit electronic parts
    - a) GIDEP and Contracting Officer



# DFARS: 252.246.7007

---

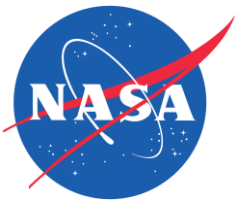
- 7) Methodologies to identify and determine if a part is suspect
- 8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts
- 9) Flow down of detection and avoidance requirements to subcontractors at all levels of supply chain responsible for buying/ selling electronic parts or assemblies, or performing testing
- 10) Process for keeping current counterfeiting information and trends, including detection and avoidance techniques
- 11) Process for screening GIDEP reports/ and other sources to avoid counterfeit procurements
- 12) Control of obsolete electronic parts



# AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

---

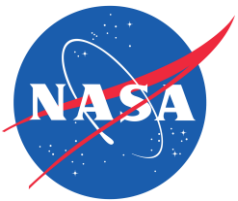
- Created in response to a significant and increasing volume of counterfeit electronic parts entering the aerospace supply chain, posing significant performance, reliability, and safety risks
- Provides uniform requirements, practices and methods to mitigate the risks of receiving and installing counterfeit electronic parts
- Highly recommended standard for use by all contracting organizations that procure electronic parts



# AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

---

- This standardizes practices to:
  - maximize availability of authentic parts,
  - procure parts from reliable sources,
  - assure authenticity and conformance of procured parts,
  - control parts identified as counterfeit,
  - and report counterfeit parts to other potential users and Government investigative authorities.
- Requirements: 4.1 Counterfeit Electronic Parts Control Plan
  - 4.1.1 Parts Availability
    - The processes shall maximize availability of authentic, originally designed and/or qualified parts throughout the product's life cycle, including management of parts obsolescence.



# AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

## •4.1.2 Purchasing

- Assess potential sources of supply (including electronic parts, assembly, and equipment suppliers) to determine the risk of receiving counterfeit parts. Assessment actions may include surveys, audits, review of product alerts (e.g., GIDEP, ERAI), and review of supplier quality data to determine past performance.
- Maintain a register of approved suppliers including the scope of the approval, to minimize the risk of counterfeit parts supply. Specify a preference to procure directly from OCMs or authorized suppliers on the approved supplier list.
- Assure that approved/ongoing sources of supply are maintaining effective processes for mitigating the risks of supplying counterfeit electronic parts. Assurance actions may include surveys, audits, review of product alerts, and review of supplier quality data to determine past performance.
- Assess and mitigate risks of procuring counterfeit parts from sources other than OCMs or authorized suppliers. This shall be accomplished and documented for every application when it is necessary to procure from other than the OCM or an authorized supplier.
- Specify supply chain traceability to the OCM or aftermarket manufacturer that identifies the name and location of all of the supply chain intermediaries from the part manufacturer to the direct source of the product for the seller. If this traceability is unavailable or the documentation is suspected of being falsified, a documented risk assessment is required.
- Specify flow down of applicable requirements of this document to applicable contractors and their sub-contractors. In the event that one or more supply chain intermediaries do not have a counterfeit part control plan compliant to this document, a risk analysis shall be required for every application of the part.





# AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

---

- 4.1.3 Purchasing Information

- The documented process shall specify contract/purchase order quality requirements to minimize the risk of being provided counterfeit parts.

- 4.1.4 Verification of Purchased Product

- The documented processes shall assure detection of counterfeit parts prior to formal product acceptance. The rigor of the verification process shall be commensurate with product risk. Product risk is determined by the criticality of the part and the assessed likelihood of receiving a counterfeit part. Examples of verification actions include: review of data deliverables, visual inspection, measurements, non-destructive evaluation and destructive testing (e.g., marking permanency, x-ray, destructive physical analysis, thermal cycling, hermeticity, burn-in).

- 4.1.5 In Process Investigation

- The documented processes shall address the detection, verification, and control of in-process (post acceptance) and in- service suspect counterfeit parts.



# AS5553: Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

---

- 4.1.6 Material Control

- Control excess and nonconforming parts to prevent them from entering the supply chain under fraudulent circumstances.
- Control suspect or confirmed counterfeit parts to preclude their use or reentry into the supply chain.

- 4.1.7 Reporting

- The documented processes shall assure that all occurrences of counterfeit parts are reported, as appropriate, to internal organizations, customers, government reporting organizations (e.g., GIDEP), industry supported reporting programs (e.g., ERAI), and criminal investigative authorities.



# Useful SAE documents

---

- AS6496-Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution
  - Requirements for mitigating counterfeiting products
- 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



# NASA Act Sec. 1206 – Counterfeit Parts

---

- Plan, develop, and implement a program in coordination with other federal agencies

Counterfeit part training  
identification for all  
employees that procure,  
process, distribute, and  
install

Internal database to track  
all suspected and confirmed  
counterfeit parts



# NASA Parts Policy: 8730.2

---

- Policy to control risk and enhance reliability in NASA flight and critical ground support/ test systems:
  1. Develop, document, and implement a counterfeit EEE parts control plan for the avoidance, detection, mitigation, disposition, control, and reporting of counterfeit EEE parts
  2. Perform surveys, audits, product inspections, qualification testing, and risk assessments to verify supply sources.
  3. Develop and implement integrated parts management requirements, procedures, and plans
- Similar structure to AS5553: Documents adopted around similar timeline

# Section 5 – External Visual Inspection

---





# Inspection Exercise

- Dino-Lite USB Microscope

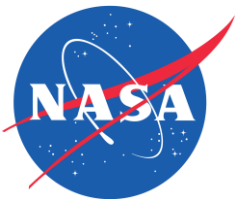




# Assessing Incoming Parts

---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) Physical mold features
  - b) Part surface
  - c) Part markings
  - d) Indents
  - e) Pins



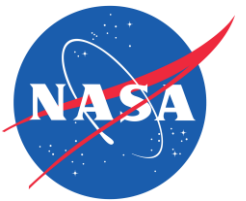
# Assessing Incoming Parts



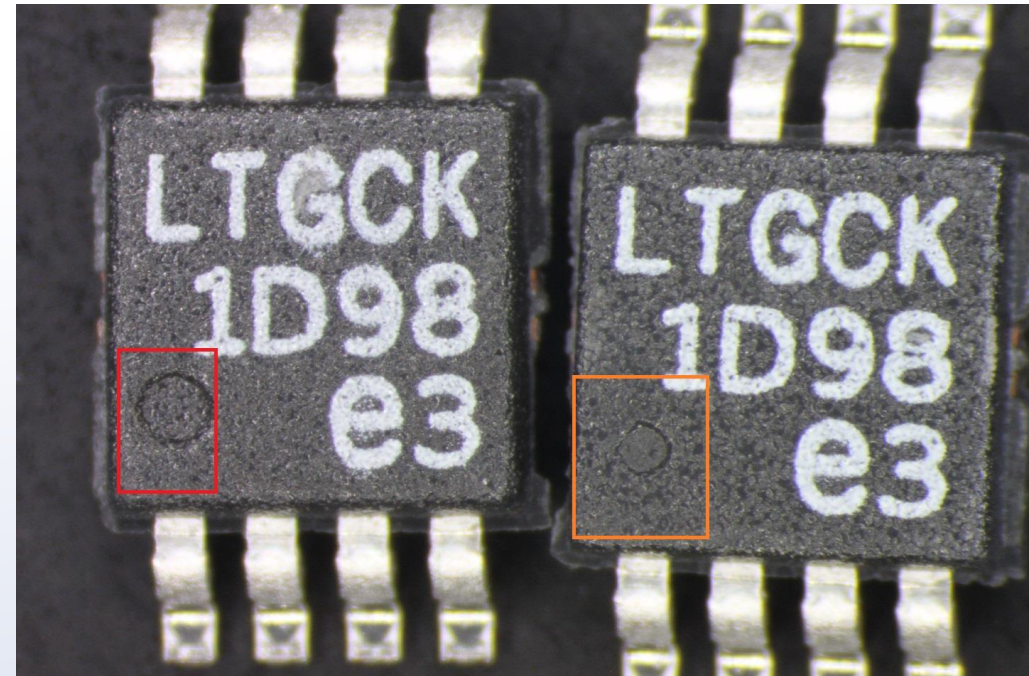
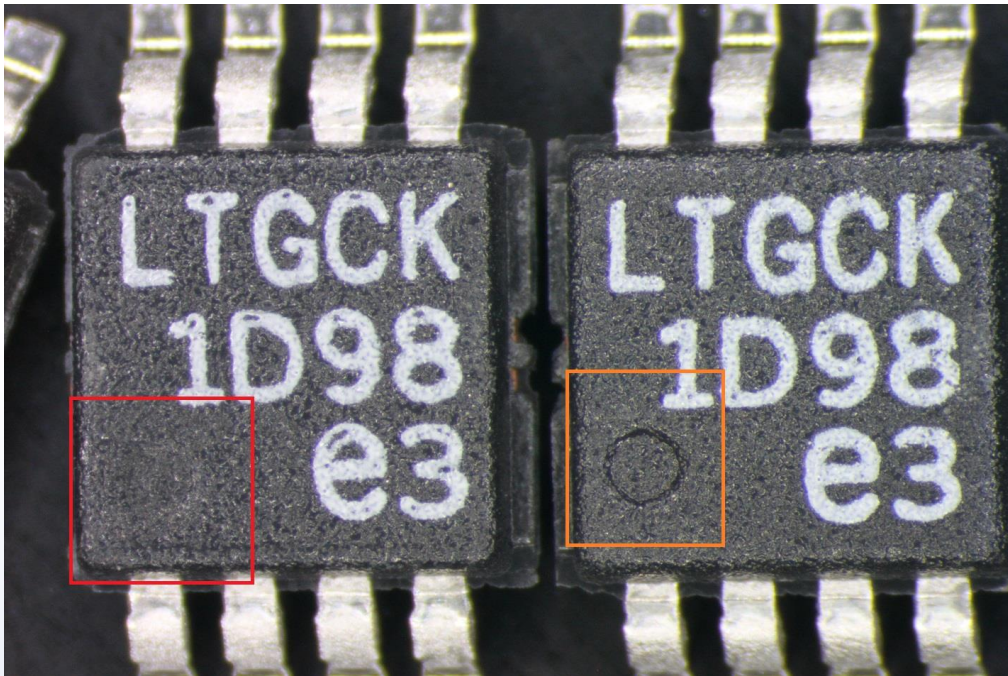
Is this part suspect of counterfeit?

- The part is **suspect**.
- Determining if a part is counterfeit depends upon the subsequent investigation.





# Assessing Incoming Parts



Parts are suspect, but are they counterfeit?



# Assessing Incoming Parts

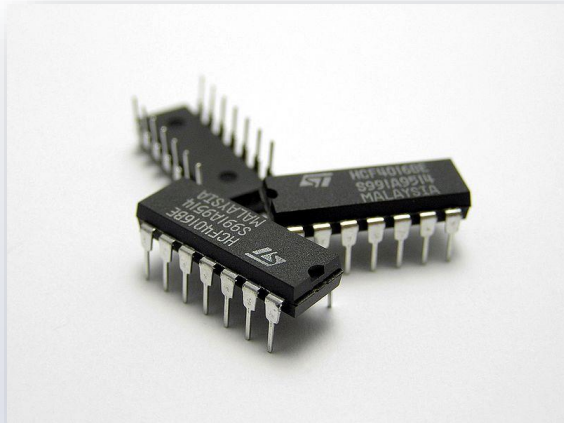
---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) **Physical mold features**
  - b) Part surface
  - c) Part markings
  - d) Indents
  - e) Pins

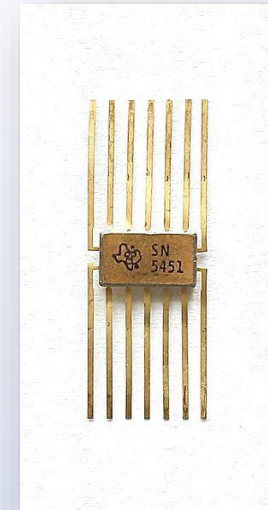


# IC Packaging

- **INTEGRATED CIRCUIT PACKAGING:** Final stage of semiconductor device fabrication, followed by IC testing. The die is encased in a support that prevents physical damage and corrosion and supports the electrical contacts required to assemble the integrated circuit into a system. The term packaging generally comprises the steps or the technology of mounting and interconnecting of devices.

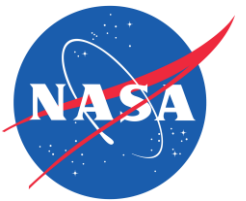


Three 14-pin (DIP14) plastic dual in-line packages



A TTL logic gate in a flat pack package





# IC Packaging

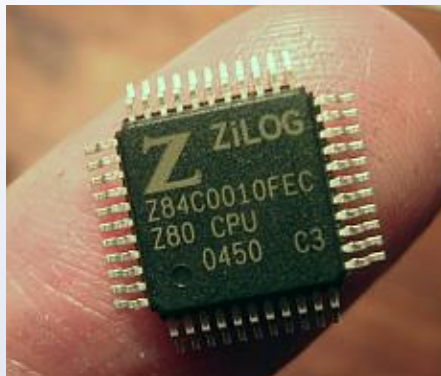
---



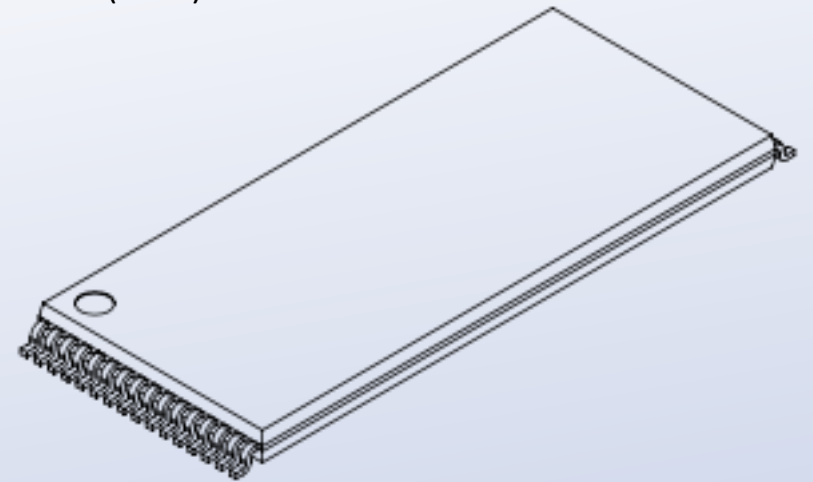
A small-outline integrated circuit (SOIC)



Plastic leaded chip carrier (PLCC)



Plastic quad flat pack(PQFP)



thin small-outline packages (TSOP)

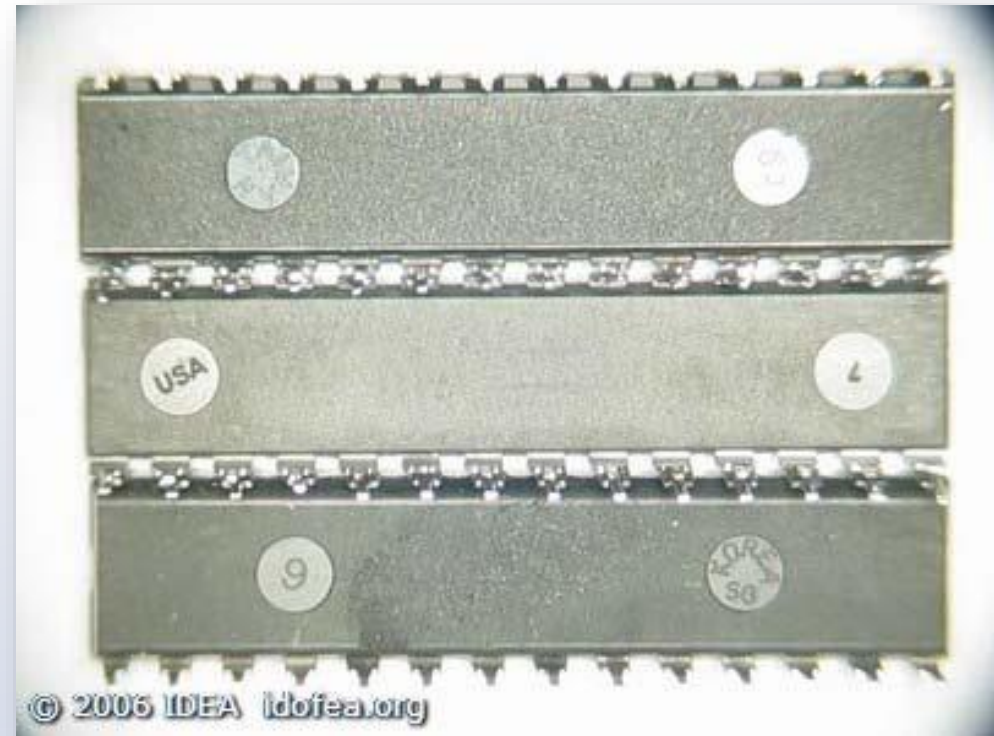


# Suspect-mold features

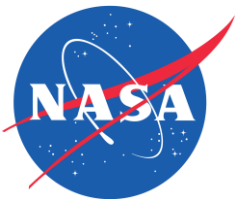
Top of Parts



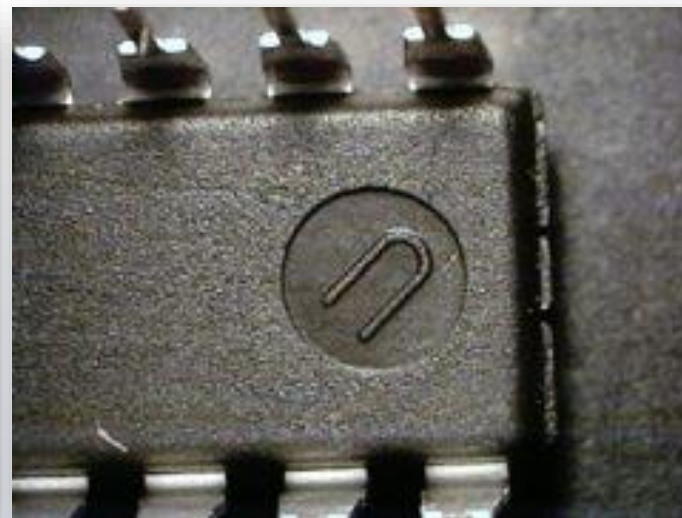
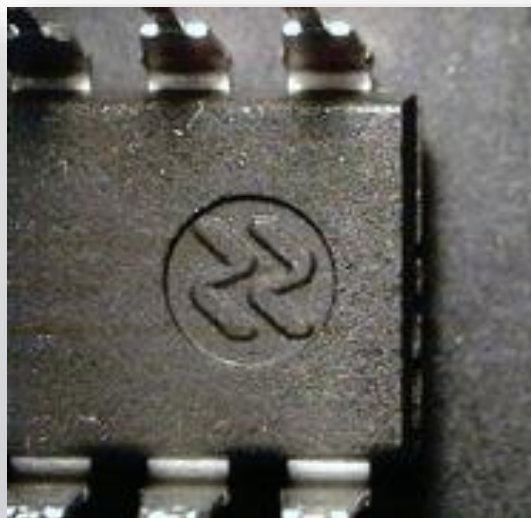
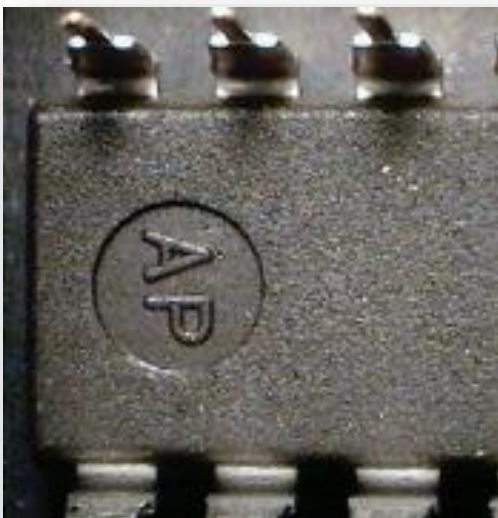
Bottom of Parts



Same P/N, MFG, D/C but three different molding!

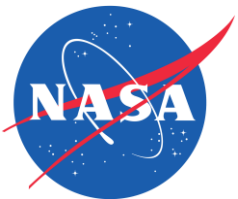


# Suspect-mold features

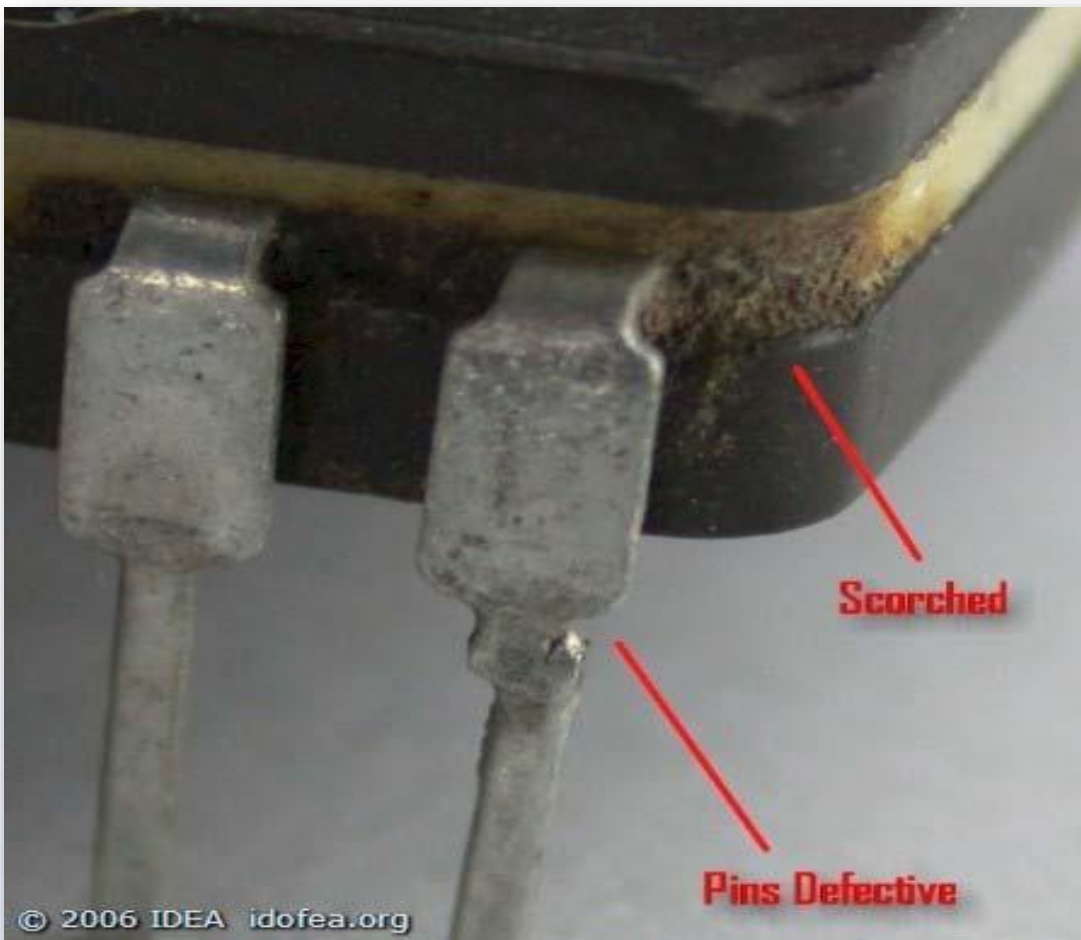


- Top surface: Identical parts
- Bottom surface: **three completely different markings**

Courtesy: AERI.com



# Suspect-mold features



- Damaged leads
  - Lead may have been re-soldered back onto existing lead.
- Scorching indicates prior use

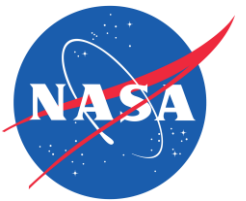


# Assessing Incoming Parts

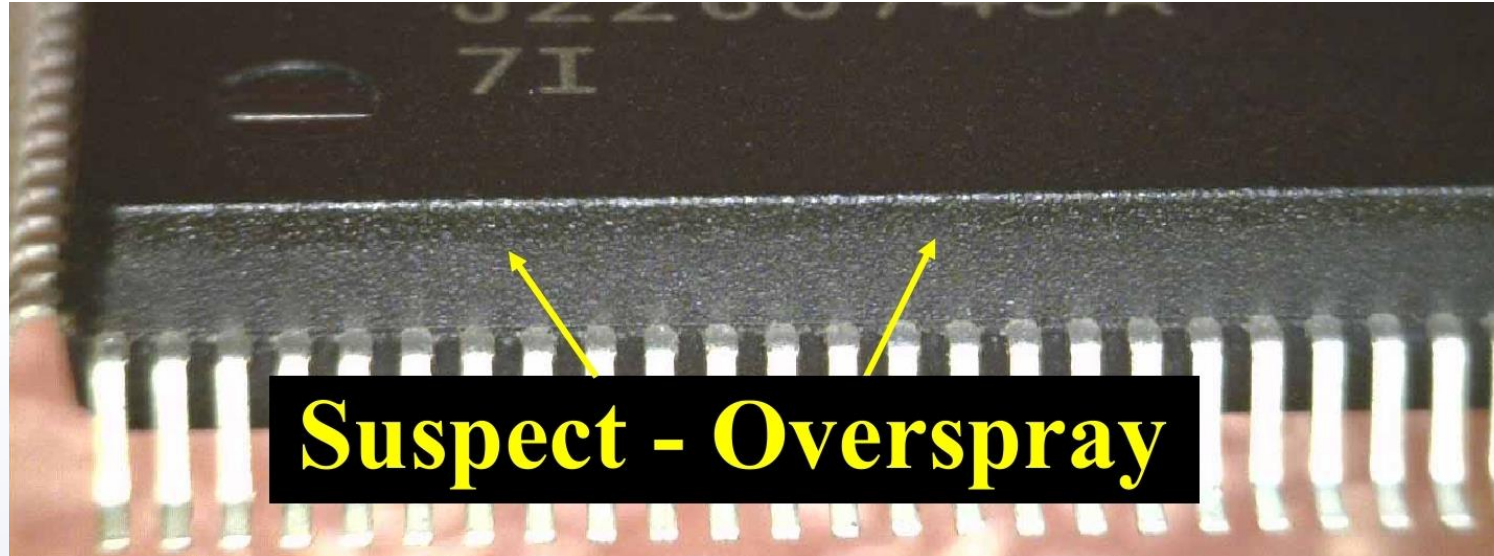
---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) Physical mold features
  - b) **Part surface**
  - c) Part markings
  - d) Indents
  - e) Pins





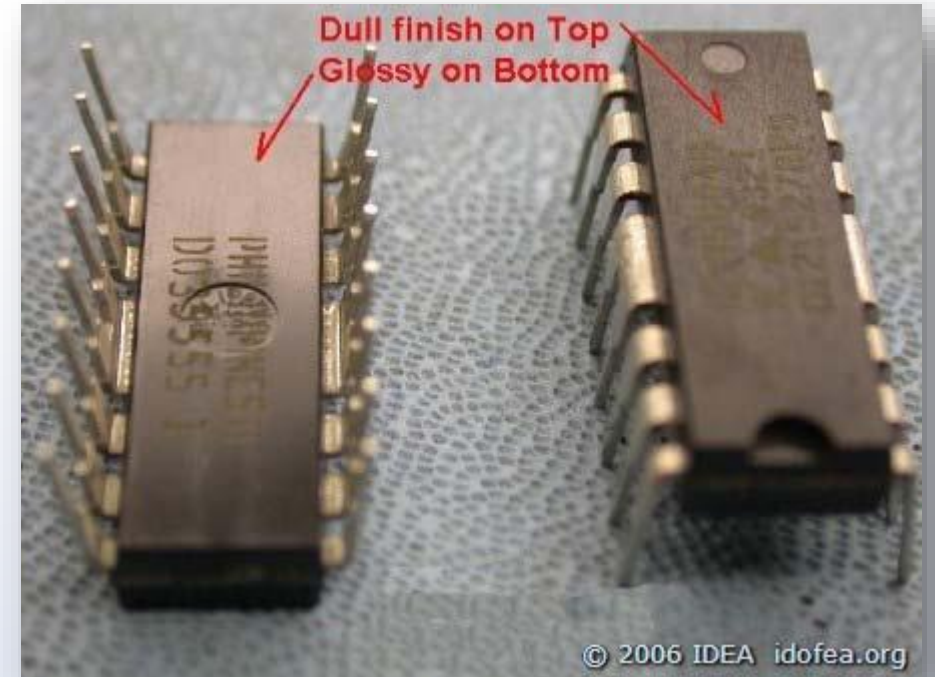
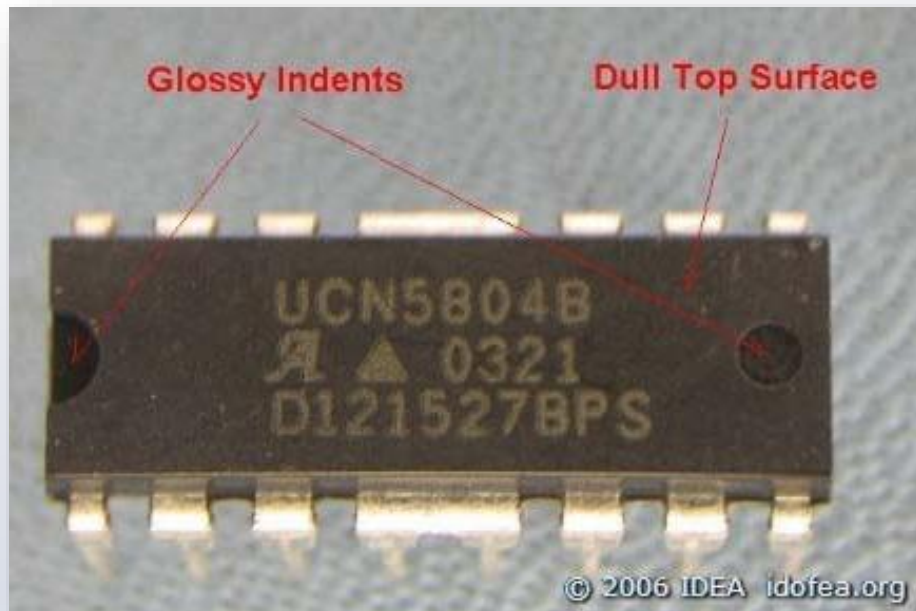
# Suspect-part surface



**Blacktopping:** resurfacing of a component so it can be remarked

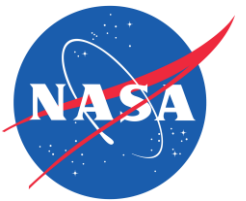
# Suspect part surface

- Different textures can be indicative of remarking
- Top and bottom of part should have same texture



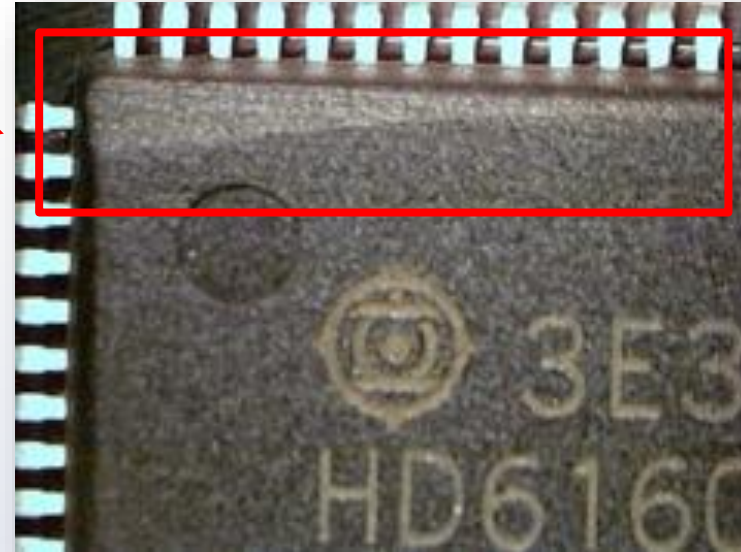
- Top and bottom of the same part have two different textures: rough vs smooth





# Suspect-part surface

Over-sanding



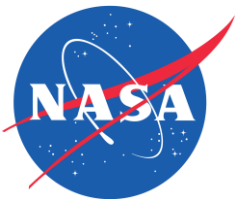
- Black topped surface was shiny and smooth but with a unnatural orange peel finish
- Scrapping the top layer revealed the Altera logo underneath



# Assessing Incoming Parts

---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) Physical mold features
  - b) Part surface
  - c) **Part markings**
  - d) Indents
  - e) Pins



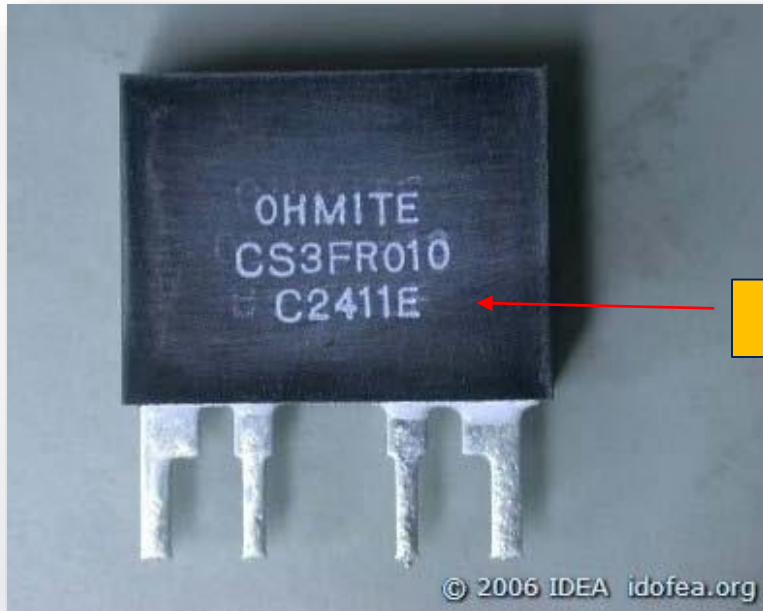
# Suspect-Part markings

- OCMs follow quality standards and major imperfections are uncommon
  - P/N will be in a certain location on the part
  - P/N will not be misaligned, crooked or misspelled
  - MFG logos do not vary from part to part
  - Part markings designed to withstand rigors of testing
- Part on right has laser burn markings
- Markings missed the part on the left hand side
- Part on right belongs to batch that had markings in a slightly different location on each part





# Suspect-Part markings



Ghost markings



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

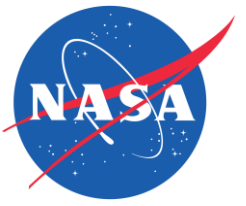


# Assessing Incoming Parts

---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) Physical mold features
  - b) Part surface
  - c) Part markings
  - d) **Indents**
  - e) Pins





# Suspect-Part indents

---

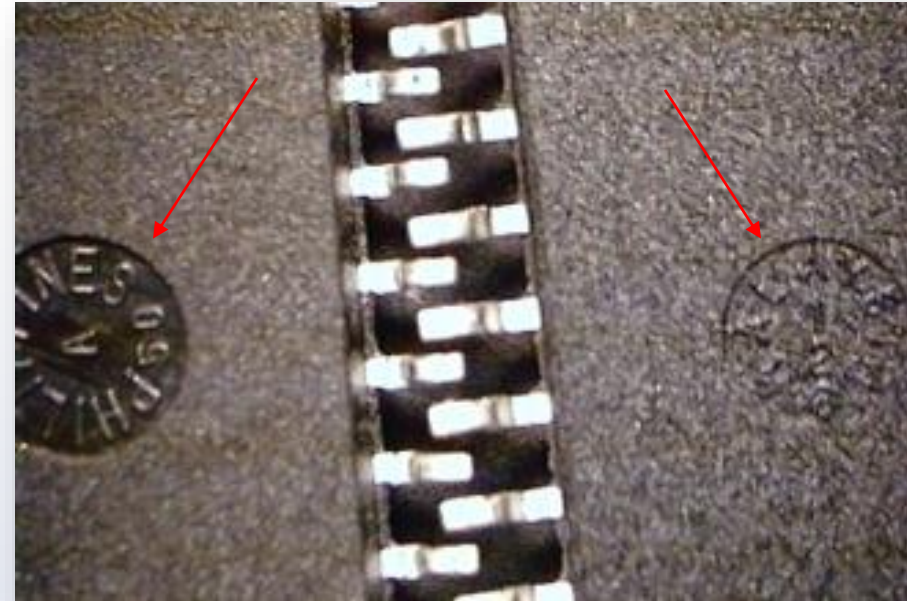


- Indent has been filled in with black topping material
- Original indents are always clean

# Suspect-Part indents



- Indent is half-filled with black top
- Letters have rough texture



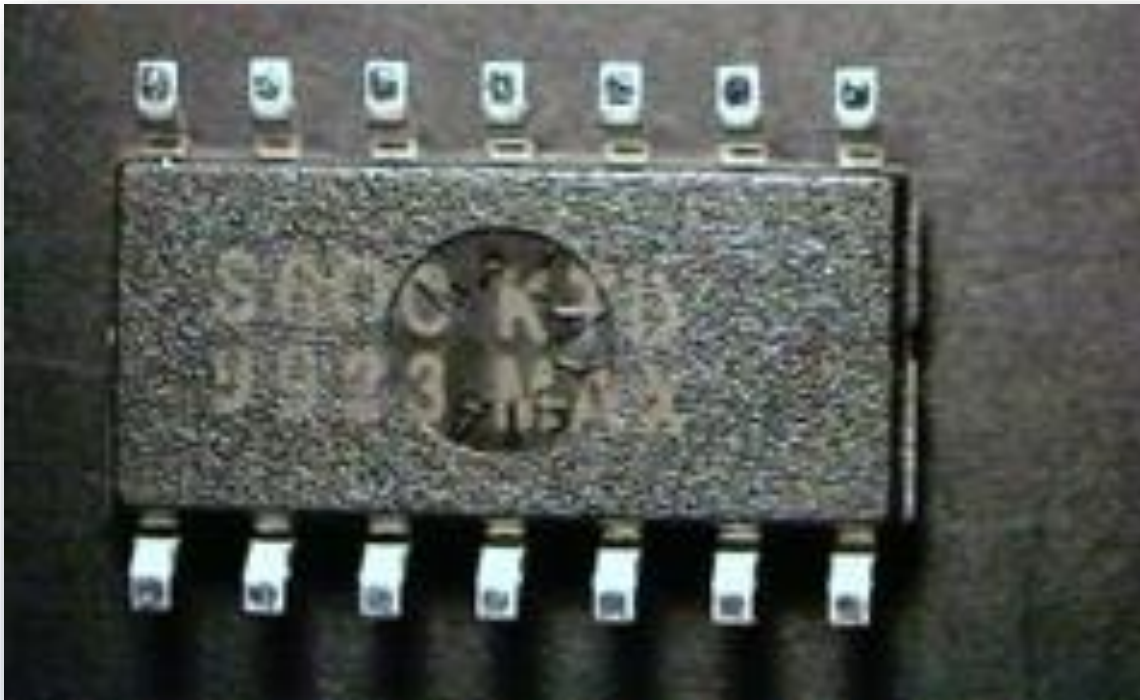
- Identical parts
- Parts on the left is marked Philippines, part on the right is Malaysia





# Suspect-Part indents

---



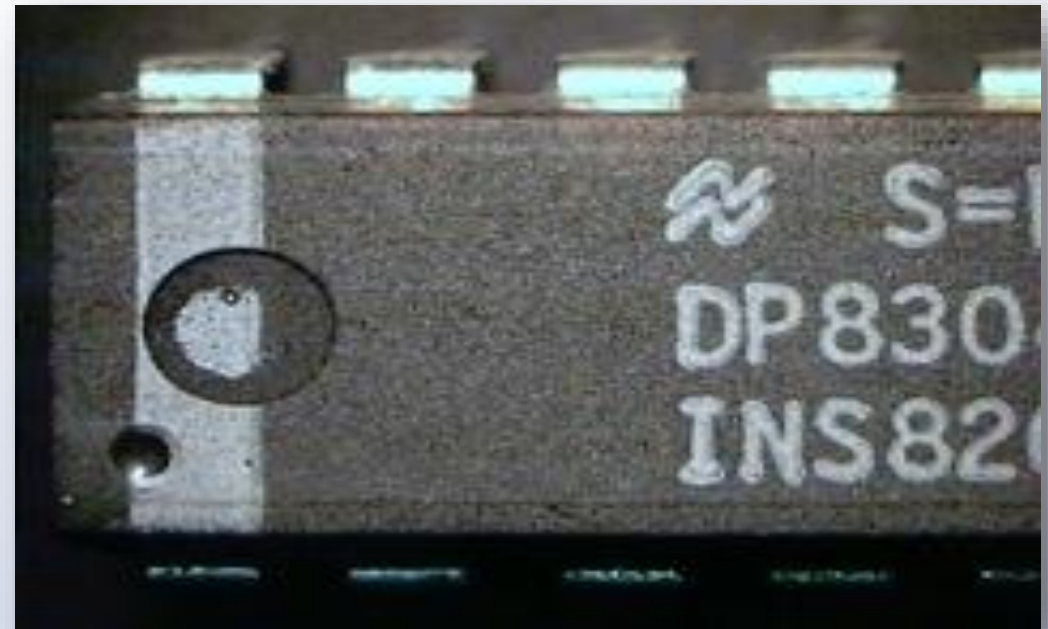
- Indents should be cleaned and unmarked
- Indents with markings can signify a suspect part

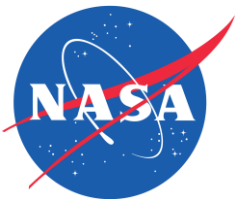


# Suspect-Part indents

---

- Identical parts
- Indents between the two parts are not identical





# Suspect-Part indents

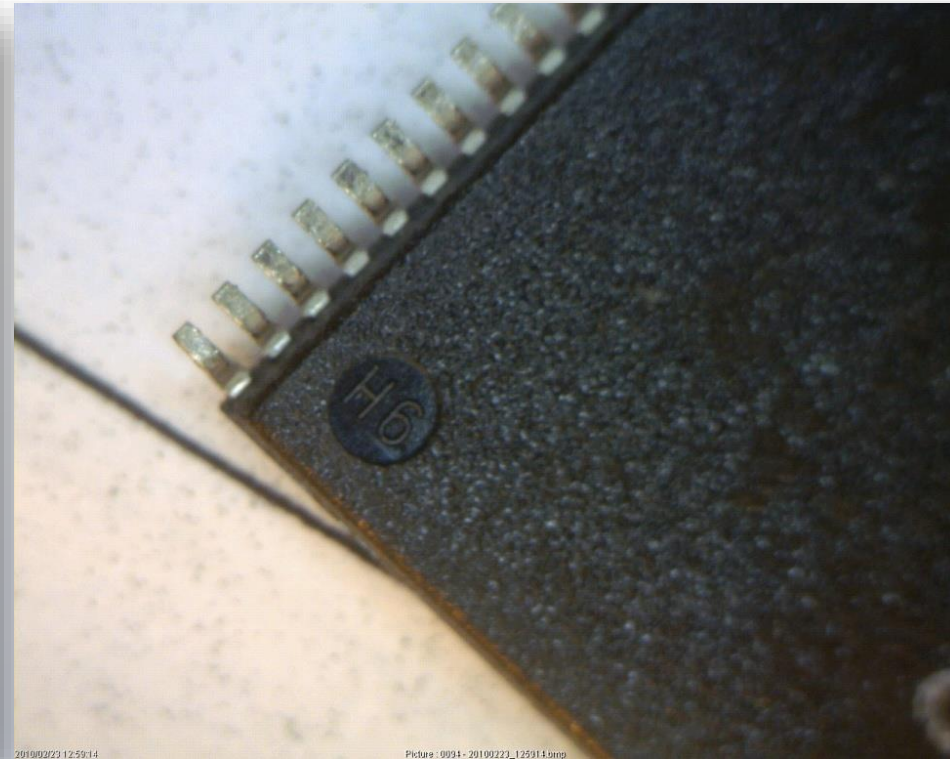
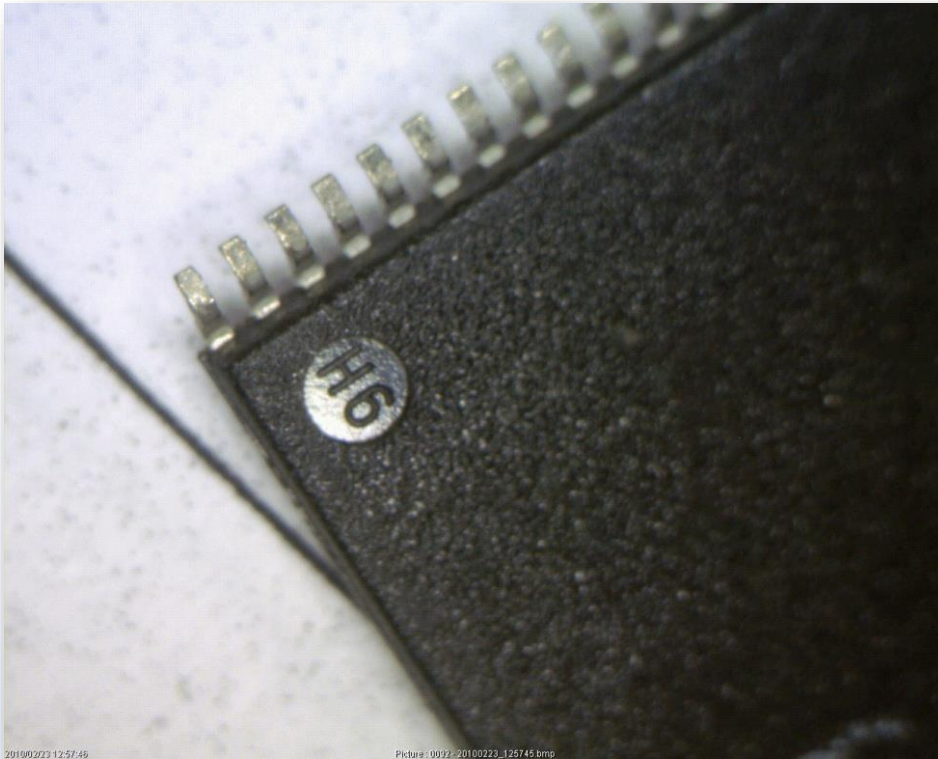


- Good
  - Same part number
  - Indents on the lower left are the same
- Suspect
  - Right indent not apparent on the bottom part

Part could have been blacktopped,  
filling in the indent



# Good-Part indents



- Example: clean indents on good parts under two different lighting scenarios

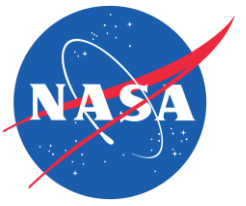




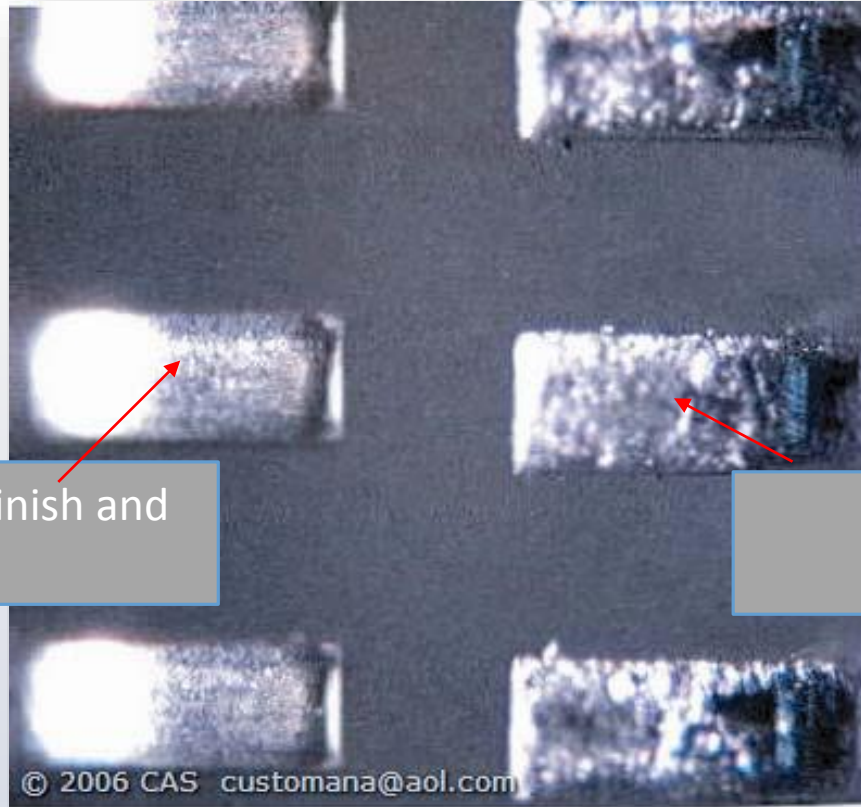
# Assessing Incoming Parts

---

1. Shipping/ Packaging
2. Documentation
  - a) Traceability
3. External visual
  - a) Physical mold features
  - b) Part surface
  - c) Part markings
  - d) Indents
  - e) Pins

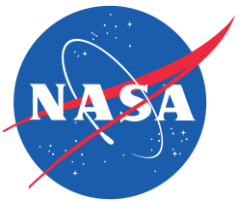


# New vs Suspect Part Leads

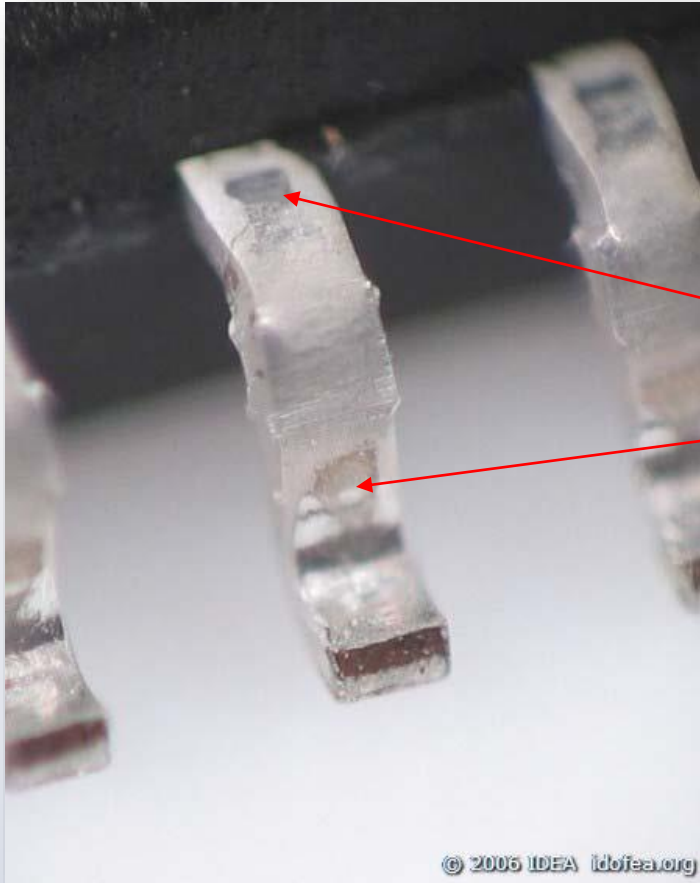


New leads: uniform, consistent finish and shape

Used leads: rough texture



# Good-Part leads



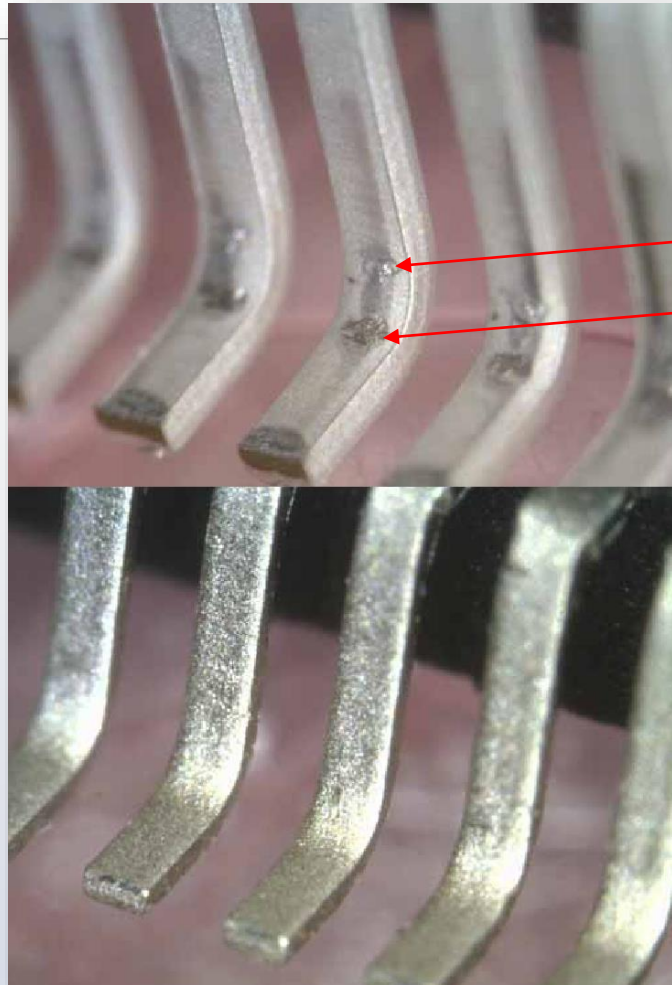
Tooling marks: result of lead formation or “bending” of leads to meet specification

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





# New vs re-tinned leads



Leads with obvious tooling marks

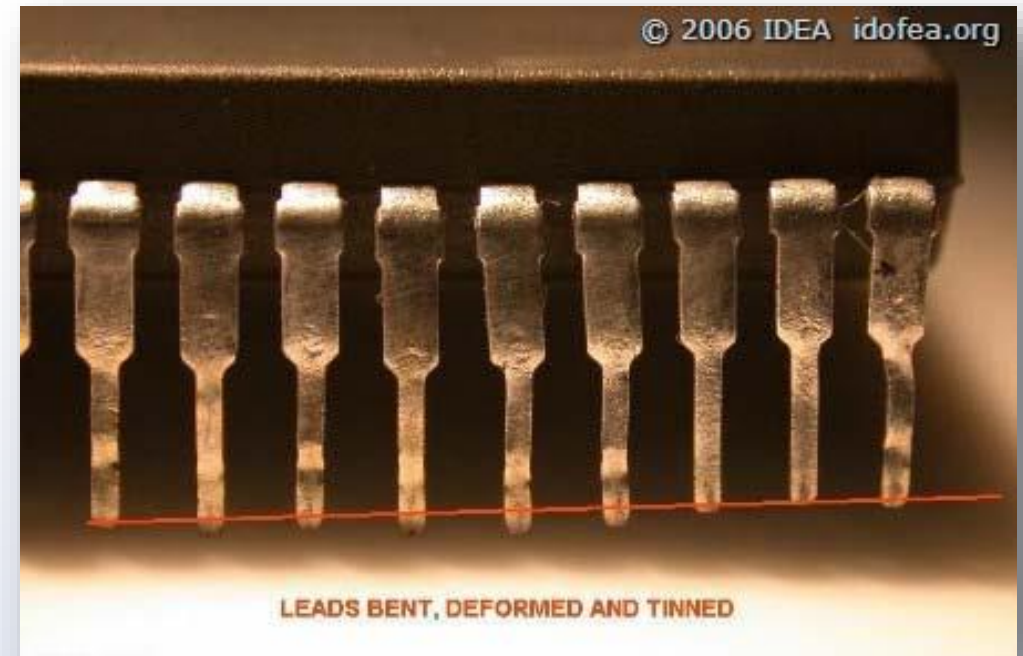
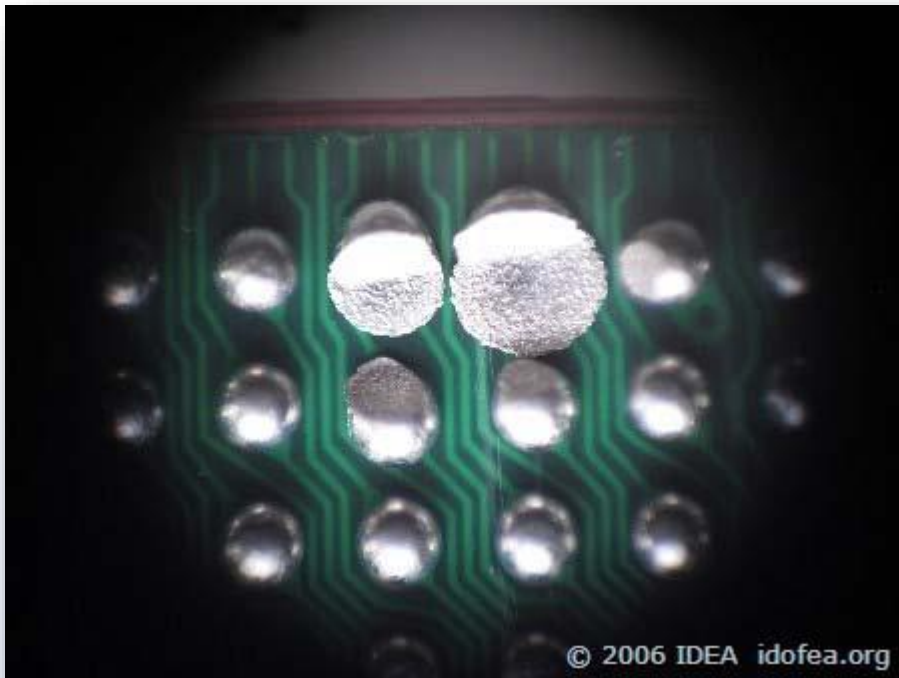
Same part re-tinned, tooling marks are hidden

Courtesy: SMT Corp



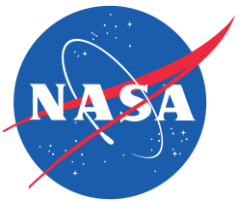
# Suspect-Part leads

- Crushed BGA solder spheres from mishandling or previous use



- Bent, re-tinned, and deformed leads

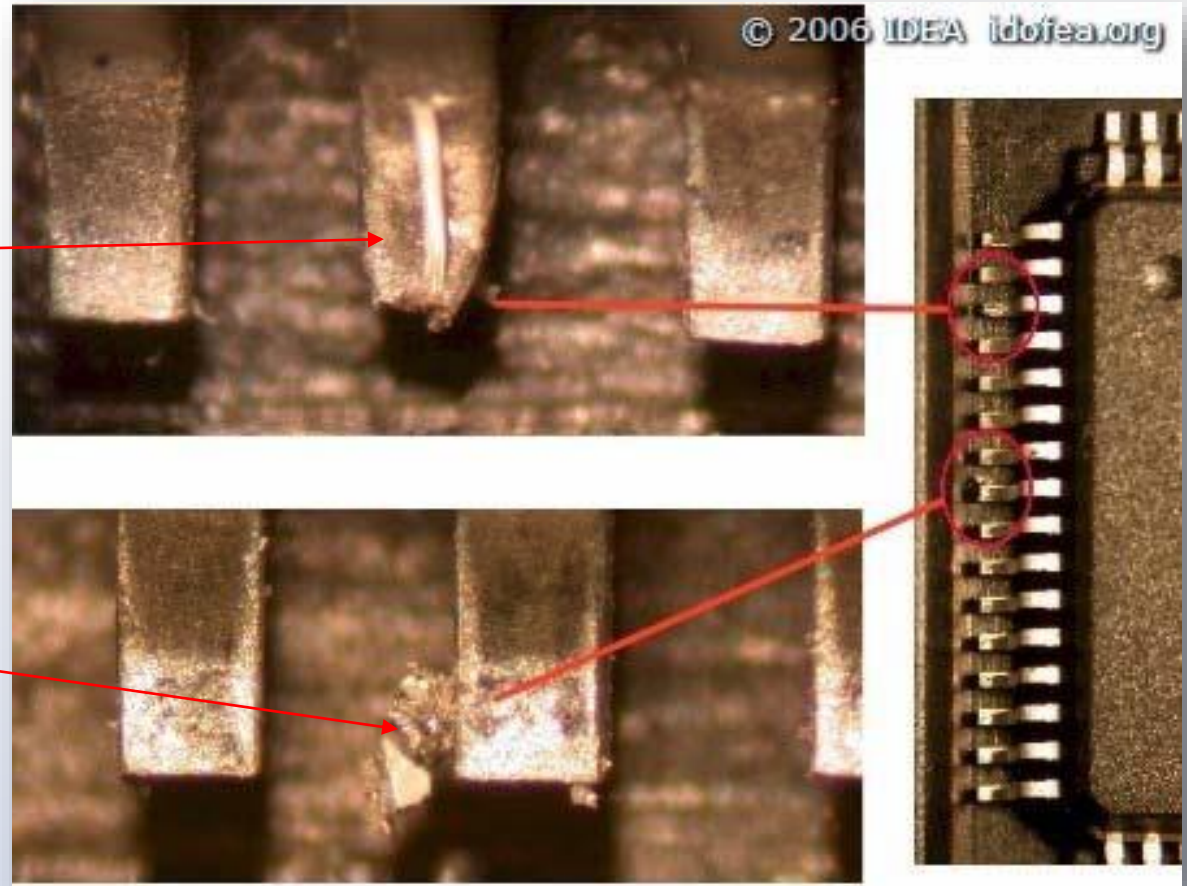
Courtesy: IDEA-STD-1010-A: Acceptability of Electronic Components Distributed in the Open Market



# Suspect-Part leads

Damaged leads can occur from previous use and from salvaging of ICs from old boards

Leads with loose solder and debris



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

# Section 6 – Additional Testing Examples

---



# Marking Permanency/ Solvents Testing

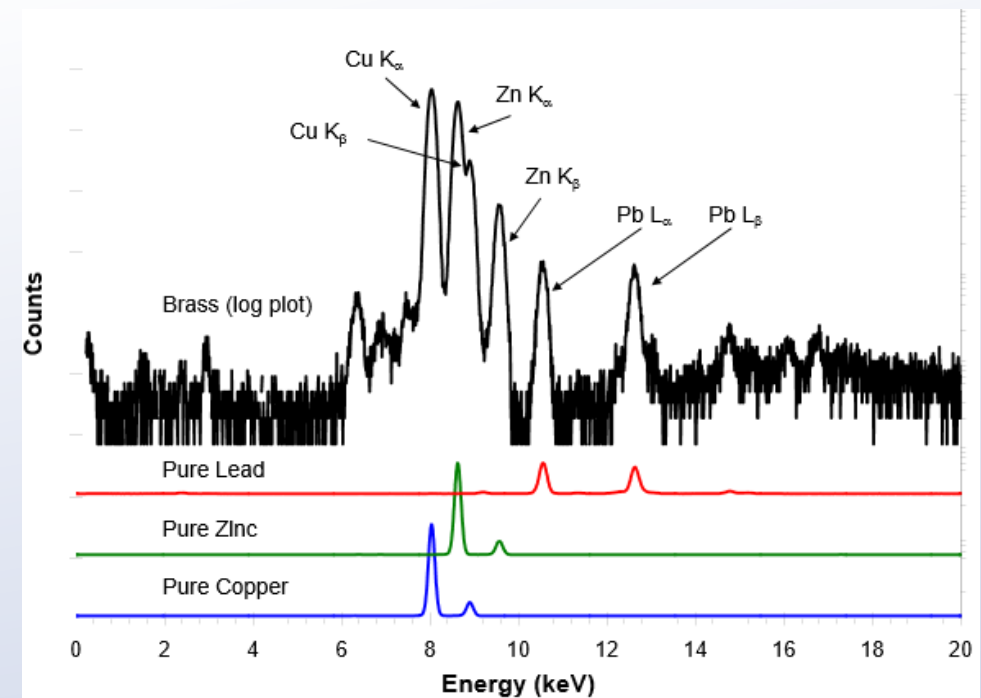
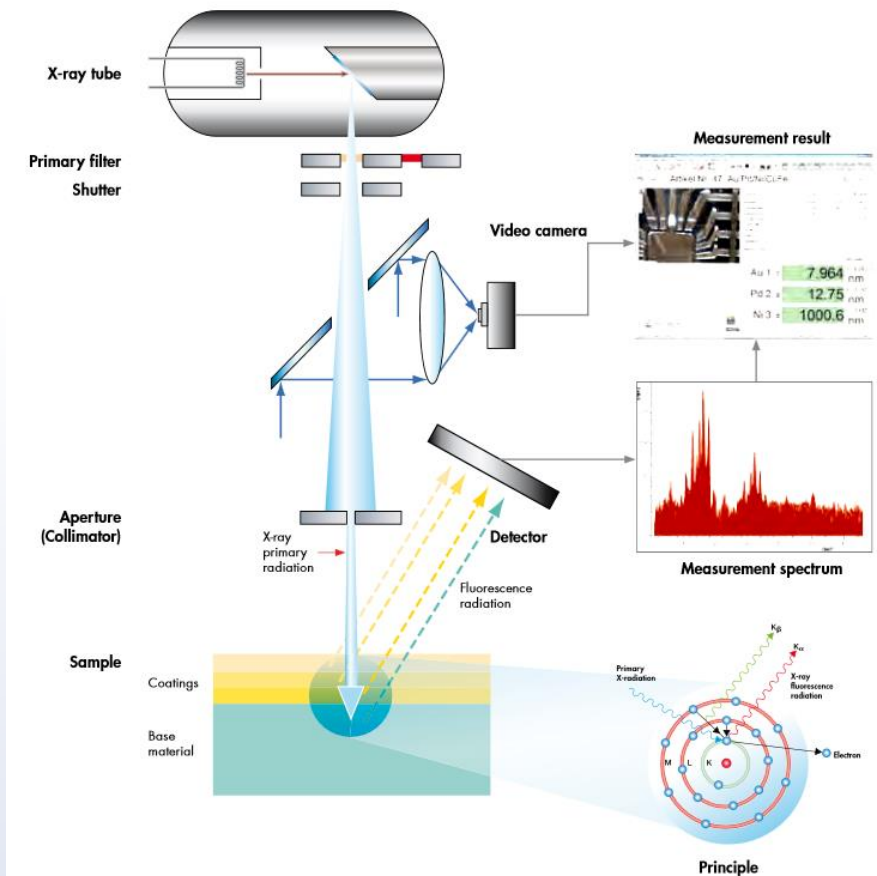
- Inspection for Re-marking or Re-surfacing
  - Standard “resistance to solvents” test methods can be effective, but more aggressive methods may be necessary to remove coatings applied to disguise sanding marks, and to reveal other indications that the original device marking has been removed.
    - Scrape surface of part w/a razor blade
    - Dilute acetone 3:1 with water & swab with Q-Tip
    - 3:1 mineral spirits/alcohol
    - Pure/heated acetone
    - DynaSolve
  - If part has been re-marked, a grayish to black substance might come off







# X-Ray Fluorescence (XRF)







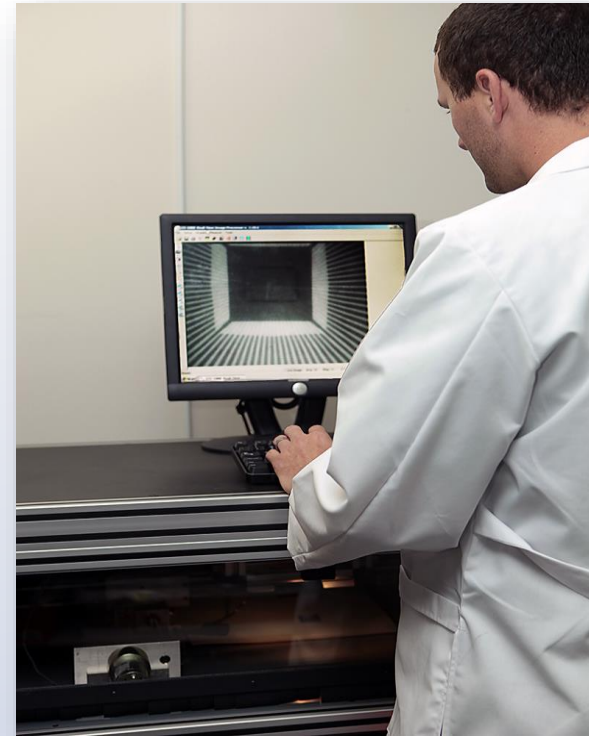
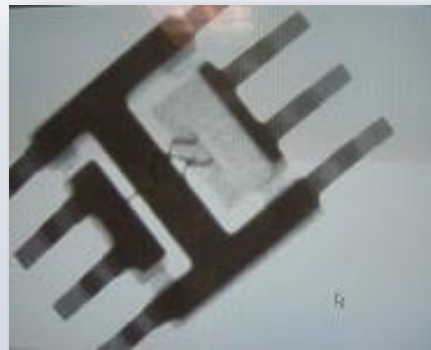
# Detecting a repackaged part: X-ray

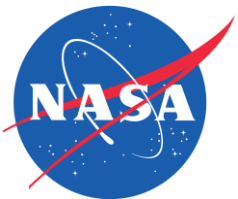
- X-ray - effective to look for manufacturing differences in die size, lead frame, bond wire patterns and voids. In some cases there have been no bond wires.

**Bond wires present**

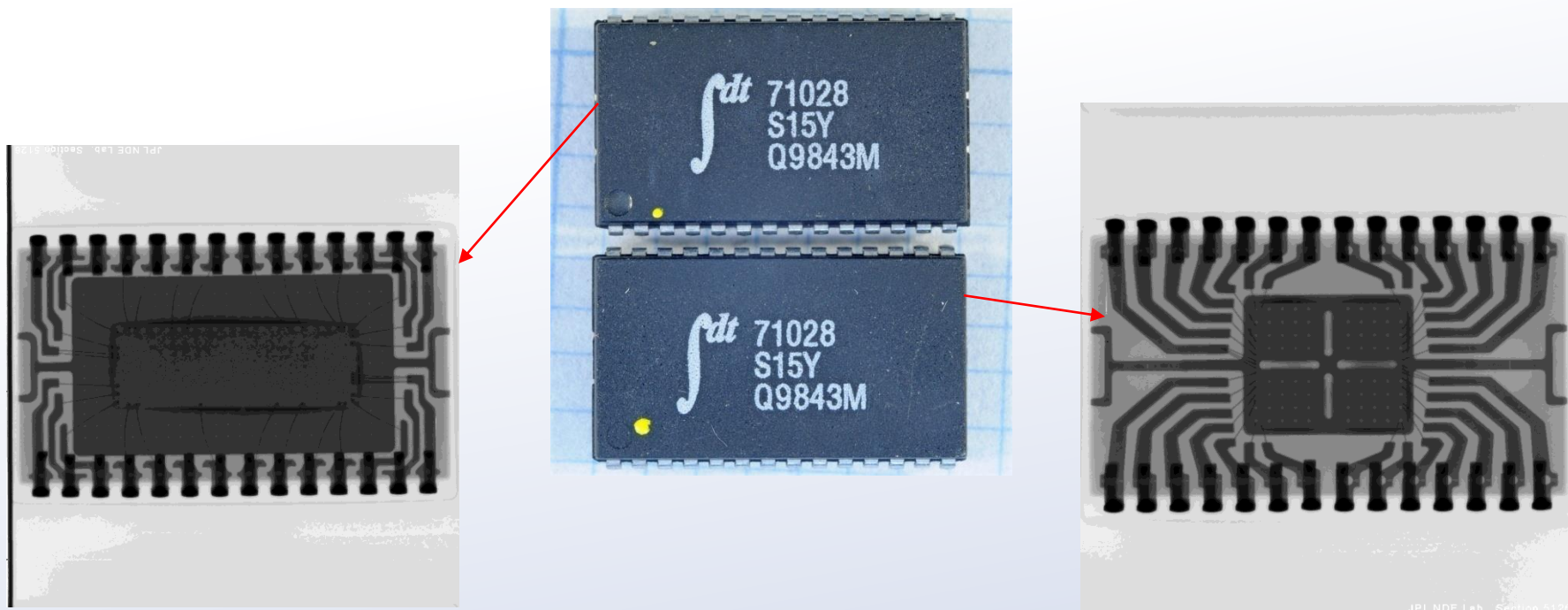


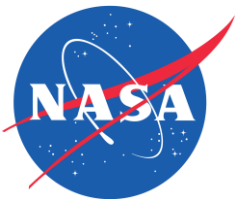
**Some bond wires missing**





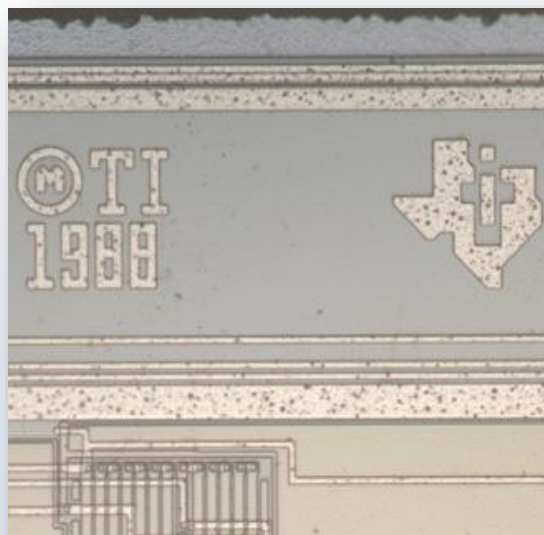
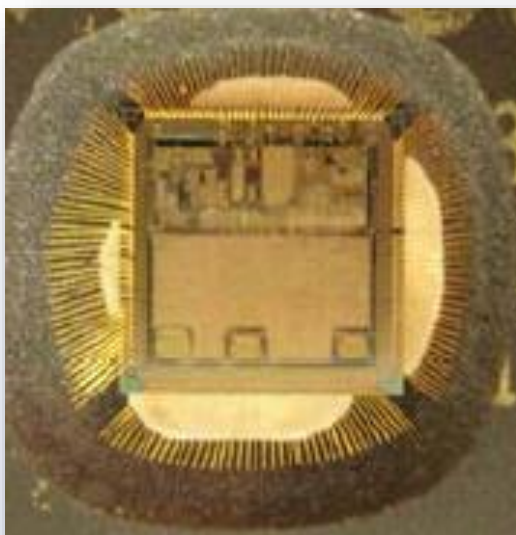
# Detecting a repackaged part: X-ray

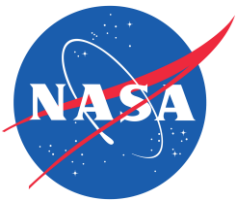




# Detecting a repackaged part: decapsulation

- Decapsulation-verify die MFG, year, and P/N are consistent





# the New Frontier: Hardware and Software hacks

- Trojan: innocuous piece of software that contains malicious code
- Hardware Trojan: small change in an IC that can disturb chip operation
  - Failure at crucial time
  - Produces false signals
  - Added backdoor
- When they are inserted:
  - During coding
  - MFG/ FAB



Photo Courtesy: <http://s.hswstatic.com/gif/trojan-horse-1.jpg>



# Conclusion

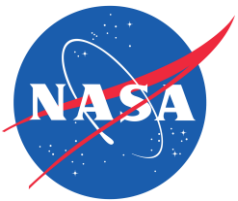
---

- Understanding of the electronics parts counterfeit issue
- Knowledge of the supply chain environment for EEE parts
- Familiarity with some of the methods used in counterfeiting
- Learned how to develop risk mitigation steps
- Hands-on verification and inspection processes for the detection of suspect parts

## Contacts:

Mark LeBlanc  
Mark.leblanc@jpl.nasa.gov  
818-354-0953

Carlo Abesamis  
Jose.carlos.s.Abesamis@jpl.nasa.gov  
818-354-0211



# References

---

- NASA
- Independent Distributors of Electronics Association (IDEA)
- Government Industry Data Exchange Program
- ERAI
- SMT Corp
- American Electronic Resource, Inc
- U.S. Dept of Commerce
- Environmental Protection Agency
- PBS: Frontline