

Raytheon

Customer Success Is Our Mission



IEEE Joint Section Reliability Chapter monthly meeting

[Boston – New Hampshire – Providence]



MISSION:
A WORLD OF INNOVATION



Counterfeit Analysis-

**Detection & Quality Control
Non-Conformance Issues**

Prevention-

**Hardware & Data Destruction,
Assured Domestic
Electronics Recycling**

Aaron DerMarderosian Jr.

**Principal Electrical Engineer
Raytheon Company**

Morgan Deptola

**Quality Control & Inventory Manager
TCG Components**

February 12th, 2014 18:00

Copyright © 2014 Raytheon Company. All rights reserved.
Customer Success Is Our Mission is a registered trademark of Raytheon Company.

Outline- *Supply Chain Issues & Case Studies*

- Background & History Regarding Counterfeit
- Industry Issues & Awareness
- Existing Standards- *Overview*
- Issues- *Detection, Analysis & Interpretation*
- Supply Chain & Raytheon Case Examples
- Example Report- *Suspect Counterfeit*
- Conclusions & Recommendations- *Standards, Training, Reporting*

Background & History

- 1. Prior domestic counterfeit issues:** *(Incidence rate in-frequent)*
Crude re-marks, lot reject scavenging, marked mechanical samples
- 2. Current Global counterfeits:** *(Above plus re-claimed scrap & clones)*
Sophisticated refurbish & remarking techniques. Increase in incident / detection rate
Matriculation throughout the supply chain Effects: Brokers, ID's, OEM's, AD's Even OCMs!
- 3. U.S. Counterfeit Ring Investigation:** IC counterfeits, MVP Micro & VisionTech highlighted how serious this issue is
2003: Reported to DOJ by an OCM, ICE investigation initiated
04-12: Investigation ; Warrants ; Indictments ; Convictions ; Sentencing, **8 yr.** timeframe
10s to 100s of thousands counterfeit ICs sold prior & during the investigation!
- 4. SASC Hearings Nov. 2011:** Levin-McCain listen to witness testimony
Representation: MDA, GAO, SIA, Independent Distributors & OEMs
- 5. NDAA 2011 - 2013:** Counterfeit laws passed, 2014 edits & DFARS *pending*

Counterfeit IC's are pervasive & Impact the Legacy Supply Chain

Industry Issues & Awareness

6. **Domestic Transition to EU RoHS & WEEE:** Implemented mid-2006
Non-uniform OCM adoption- Part marking & numbering conventions not standardized
Added complexity & confusion to the supply chain- Particularly 05-07 timeframe
Reclamation requirements- Provided an endless supply of high value legacy components!
7. **Conferences & Workshops:** Counterfeit theme raises industry awareness
Components for Military & Space Electronics: CMSE (CTI)
U. Maryland Joint with SMTA: Calce Counterfeit Symposium (East & West)
ERAI Executive Conference: Theme dedicated to counterfeits (ERAI)
U. Conn ARO / CHASE Workshop on Counterfeits
Counterfeit Component Awareness Workshop, CCAW (CTI)
MDA Workshops- Counterfeit Materiel Training (Supports PMAP)
Diminishing Manufacturing Sources & Material Shortages Conference (WG, supports DoD)
8. **Industry Standards Generation:**
SAE, IDEA & iNEMI, also TechAmerica, ECA, IEC & GIFAS
Standards released or pending. Several require updates & CB criteria!
9. **Industry, DoD & Government awareness:** Dramatic increase since 2011
Highlights analysis, interpretation disparities & knowledge gaps within the electronics industry

Laws & Requirements precede standards adoption & awareness

Policies & Standards- *Targeting Counterfeit Components, Materials*

Counterfeit Products Risk Mitigation and Prevention: **Raytheon**

243-RP: Corp. Policy includes procurement, controls, supplier requirements, based on **AS 5553A** (7.24.12)

SP-345: IDS procedure, References RTN policy & **IDEA-STD-1010**, articulates BU needs (12.15.11)

IDEA: “Acceptability of Electronic Components Distributed in the Open Market”

IDEA-STD-1010B Released April 2011- *Independent Distributors of Electronics Association*

- Visual & surface inspection of electronic components traded in the open market

IDEA: **IDEA-1005-D “IDEA Inspection process guideline checklist”**

- **Decommissioned** updated checklist, chapter 16 (p. 244-245) **IDEA-STD-1010B**
- Best practice Industry process sheet & visual inspection guide, provides a generic framework
- Comprehensive, assumes users are trained in inspection techniques, procedures & knows how to tailor to applicable work instructions

SAE: “Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition”

AS 5553A Released Jan 2013- *SAE International (Society of Automotive & Aerospace Engineering)*

- Policies / requirements flow down, to sub-tier organizations that procure electronic parts
- Utilized by Aerospace / Defense OEM Integrators, Contains RTN policy elements

OEMs & Supply Chain: *Authorized, Franchised, Independent Distribution*

Standards & Programs- *Counterfeit Components & Materials*

SAE: “Counterfeit Electronic Parts: Avoidance, Detection, Mitigation & Disposition”

AS 6081: Released November 2012- Mandatory practices for Independent Distributors,
Implementation in process

AS 6171: Initial draft pending- Testing & Analysis Methods, applies to Failure Analysis Labs. *in review*

AS 6174: Released May 2012- Parts and Materials Initial draft, released

Component Technology Institute: “Counterfeit Component Avoidance Program”

CTI-CCAP-101 *Established in 2008, now in Revision D*

- Mandatory practices for Independent Distributors
- Detection / avoidance of acquisition & delivery of counterfeit electronic components

Inspection Certifications & Training:

IDEA-ICE-3000- Inspector Certification Pre-requisites, IDEA training & Inspection experience

Counterfeit Component Avoidance Workshop (CTI)- 2 day hands on event hosted in a FA lab

NASA JPL- Beginner to advanced workshops, offered at Industry conferences

IDEA-STD-1010B- Offered through IDEA / IPC certified training centers (IE: EpTac)


MDA Workshops- Counterfeit materiel training, provided to DoD suppliers

Implementation, CB criteria & compliance within industry will TAKE TIME!

Inspection Guidelines-

IDEA-STD-1010B {Ch. 16}

Used by permission from IDEA www.idofea.org



IDEA Inspection Process Guidelines Checklist
This checklist shall be used in conjunction with all requirements stated in
IDEA-STD-1010 and ANSI/ESD S20.20
www.IDofEA.org
Page 1 of 2

1 General Carton Inspection
(Section 10.1.5.1)

- Weigh product contents and record
- Inspect outer package for evidence of damage
- Photograph/record any findings
- Inspect the sealing tape for evidence of tampering
- If damage or evidence of tampering is present note findings and alert vendor and carrier for a possible freight claim

2 Outer Product Carton Inspection
(Section 10.1.5.2)

- Inspect package for any signs of damage or signs of being opened
- Photograph contents while in box if they exhibit damage, tampering, or nonconformance
- Photograph labels and sealing tape if they exhibit damage, tampering, or nonconformance
- Inspect sealing tapes
- Inspect labels and verify data
- Examine the box and compare with manufacturer's website or golden sample
- Scan barcode to verify information is readable

3 Inner Contents Inspection
(Section 10.1.5.3)

- Inspect inner contents, packaging, bag seal and labels; photograph if they exhibit damage, tampering, or nonconformance
- Inspect bag seal
- Compare inner labels with outer carton labels and photograph
- Verify bag seal date with product date code
- Scan the bar code to verify the information is readable and matches the product identification; record results
- Verify the product is properly packaged for the required Moisture Sensitivity Level (MSL) and compare the MSL level with datasheet
- Verify the package is ESD compliant

4 Inspection of Carrier
(Section 10.1.5.4)

Read and record status of Humidity Indicator Card (HIC). To test card for validity, see J-STD-033 for HIC test.

Tubes:

- If factory packaged, verify tubes are imprinted with manufacturer name/logo
- Verify all tubes are the same length and look clean and new (not yellowed or excessively scratched)
- Verify parts in the tube are all oriented the same direction
- Verify quantity of parts in tubes is consistent
- Verify all tubes have stoppers and they are the same in each tube

Reels:

- Verify labels and label placement
- Scan and verify that barcode scan and printed information on label are consistent with each other
- Verify that size of reel and the material (paper/plastic) match manufacturer spec sheet
- Verify factory reel has proper leader tape
- Verify reel count (no empty pockets) and cover film is properly attached
- Compare part orientation in tape with manufacturer spec sheet and verify the parts oriented in the tape are consistent
- Verify that there are no splices or cuts in the tape

Trays:

- Verify the color and width of the banding is what is expected
- Note if the banding has any preprinted markings
- Verify that the trays are oriented the same way
- Verify that there is a top tray to protect the parts
- Verify and record if covered by cardboard and verify if cardboard is anti-static
- Verify the chips' orientation in the tray is consistent with no missing pieces
- Verify and record date/lot code of parts
- Verify that the date/lot code match outside packaging/label on the box, if any


Bulk:

- Verify count
- Verify the bag is correct for the type or parts received, (i.e., ESD or MBB)
- Verify any mfg markings on the bag against manufacturer spec sheet
- Scan and verify that barcode scan and printed information on label are consistent with each other
- Verify and record date/lot codes

Continue Inspection Process on Page 2

Revision A

For the exclusive use of Aaron C. DerMarderosian Jr. (Raytheon Company). Copyright 2012 Independent Distributors of Electronics Association.



IDEA Inspection Process Guidelines Checklist
This checklist shall be used in conjunction with all requirements stated in
IDEA-STD-1010 and ANSI/ESD S20.20
www.IDofEA.org
Page 2 of 2

Continued from Page 1

5 Initial Inspection
(Section 10.2.1)

- Verify the part number, manufacturer and quantity match the purchase order and packing slip
- Verify that there is an original factory label; ensure there is not a label over label
- Confirm the manufacturer's logo is printed on the label; inspect the spelling; the label should not be capable of being smudged
- Verify and record the country of origin, date codes, and lot codes and ensure they are consistent throughout the packaging
- Confirm the date code meets any restrictions specified on the purchase agreement
- Record any signs of damage to the product or packaging

Note: Refer to IDEA-STD-1010-B Section 10.2.1.4 for additional information on inspecting discrete components.

6 Detailed Inspection (Visual)
(Section 10.3.1)

- Verify the logo and markings match the manufacturer's specifications
- Confirm the markings are clear and do not appear to be re-marked or re-stamped
- Confirm the markings are consistent throughout the package type from part to part and on the top and bottom of the parts (placement, font type, color, and texture)
- Inspect laser marks for burn holes caused by aftermarket laser equipment
- Inspect for inconsistencies in package indents shape, size and locations
- Confirm that there are no burn or blister marks, or evidence of exposure to excessive heat
- Ensure there are no colored dots or ink marks on the tops of components indicating previous testing or programming, unless allowed or required by the purchase order.
- Look for flux or chemical residue and and tool marks or heat-sink markings indicating refurbished parts
- Confirm there are no cracks on the surface of the parts
- Verify the lead/pin count and formation or type of lead (DIP, SMB, Gull Wing, etc.) match the datasheet
- Verify pins or terminal layout/count match manufacturer specs
- Inspect for damaged leads (bent, scratched, broken, dented, missing, coplanarity, etc.) indicating the part has been salvaged or mishandled
- Ensure that leads are not oxidized, re-tinned with solder (re-balled for BGAs), show signs of corrosion, or contamination from foreign substances
- Look for leads that are too shiny for older date codes or too dull for new date codes; the pins should be similar in gloss or shine, color, and texture
- Confirm there are no scratches on the inside and outside of leads; scratches under the BGA spheres are typically a sign of re-balled parts.
- Inspect BGAs, LGAs, and any terminals, lugs, or connectors to ensure that the component has not been used, refurbished, mishandled or contaminated
- Photograph markings front and back for records
- If nonconforming, document and photograph nonconformance(s)

7 Detailed Inspection (Solvents)
(Section 10.3.2)

- Perform Device Marking Test (test for remarking – Mineral Spirits & Alcohol swab)
- Perform Device Surface Test (test for blacktopping – Acetone swab)
- Perform Scrape Test (as needed)

8 Detailed Inspection (The Mechanical Inspection)
(Section 10.3.3)

- Determine the min/max or acceptable tolerance range of each measurement being taken from the mfr datasheet
- Measure, verify and record the package dimensions
- Measure for Thickness Variation

Revision A

For the exclusive use of Aaron C. DerMarderosian Jr. (Raytheon Company). Copyright 2012 Independent Distributors of Electronics Association.

[Formerly IDEA-1005-D] Assumes user knows how to implement

Issues- *Detection, Analysis & Interpretation*

- Industry awareness of counterfeits subject components to heightened scrutiny
- Standards provide requirements, procedures, analysis techniques & generalized examples of compliant & suspect devices
- Analysis / Inspection data interpretation guidance & how to perform investigation, is **NOT** provided!
- Training & certification for counterfeit inspection not required
- Counterfeit inspection techniques are NEW for many in the industry
- OCM quality non-conformances, misinterpreted as “suspect” counterfeit issues
- Packaging & component construction knowledge, REQUIRED to interpret results
- Analysis & data requirements in “Industry” consortia databases, are NOT well established. Many entries lack documentation / evidence to indict parts
- Parts categorized as “suspect” require analytical tests to determine if it is counterfeit, cost prohibitive to most organizations

Follow on examples illustrate some of these issues

Supply Chain Case Studies

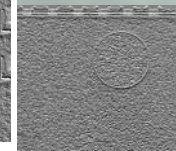
Counterfeit Test Detection & Interpretation Issues



Supply Chain Case Example 1- High volume flash memory ; Training Issue

Raytheon
Integrated Defense Systems

- Parts contained in OCM packaging. Labeling, Component finish / quality consistent with OCM
- Visual Inspection & surface tests executed per 1010B: *for Authenticity (06 week 42)*
 1. Barcode readout, verify component info.
 2. Inspect mold cavities
 3. Dimensions per datasheet
 4. Verify OCM markings, P1 location
 5. Top / Bottom surface Match
 6. Marking Permanency
 7. Surface Test (Blacktopping)
 8. No reported ERAI Instances
 9. Date code verified with supplemental EOL information
- Customer noted mold mark opposite Pin1 was textured, claimed part was re-surfaced, **lot rejected**
- Surface test in-correctly executed, results misinterpreted
- P1 mark is always smooth, alternate mold marks can be textured!
- Enhanced optical / textured images Revealed acetone and excess Burnishing smoothed part surface
- **Enhanced digital imaging highlights black top evidence. NONE present**

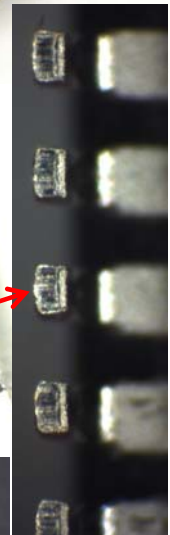
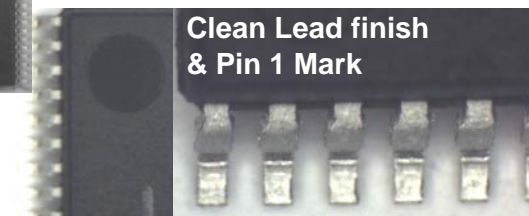
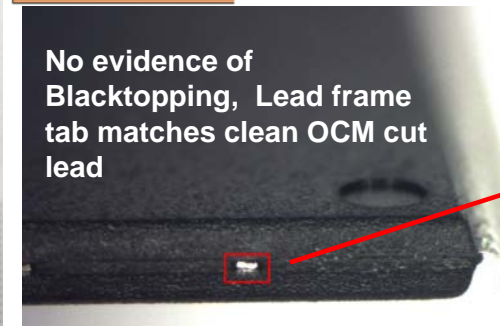
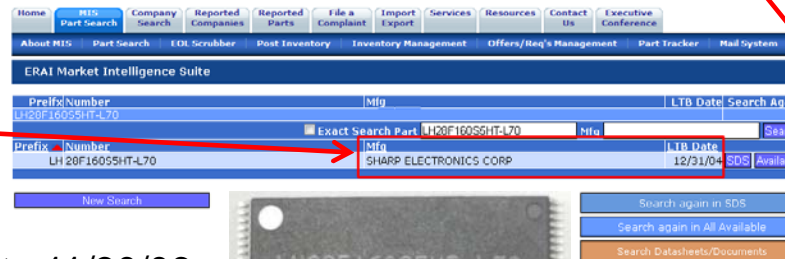
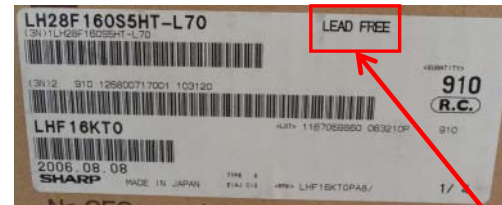


Training, test execution & Interpretation leads to false Indictments!

Supply Chain Case Example 2- **Raytheon** Integrated Defense Systems

High volume flash memory ; Database Issue, RoHS Interpretation

- OCM packaging & consistent component finish, pass 1010B QC inspection. No report history in ERAI database
- Customer questioned date code (06 week 32), ERAI database reports a LTB of 12/31/04. Incorrect info. entered in IHS
- OCM responds with PCN / EOL LTB date of 8/31/06, last ship date 11/30/06 {builds continue 6-12 months after LTB}
- Customer part number search indicates product is Tin/Lead, box states "Lead Free"
- RoHS transition year- *Some OCMs DID NOT change part numbers or add LF markings*
- OCM did not respond to tech. support LF request. **Customer accepted part on risk, verified parts were "Lead free" via XRF**

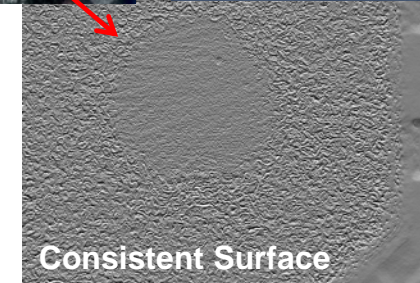
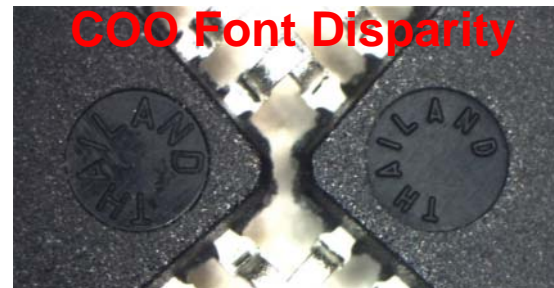


Industry is looking at ICs with a lot of scrutiny & are risk adverse!

Supply Chain Case Example 3- **Raytheon** Integrated Defense Systems

8 Bit Micro-controller ; **Font Disparity, OCM QC Issues**

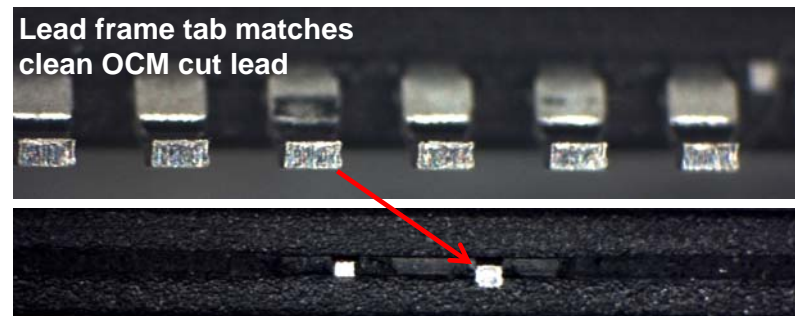
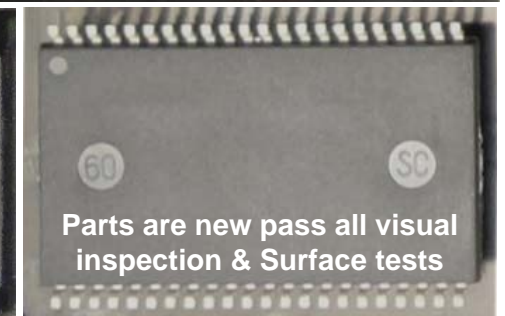
- IC Packaging with varied component finish, pass 1010B QC inspection (08 week 28) IC's construction consistent with OCM QC
- No ERAI reports or EOL notice (still in production) = Lower Risk
- Acquired from manufacturer, purchased directly from OCM's AD
- Issues discovered in inspection: Varied COO mark by date codes, faded P1 indicator
- No evidence of tampering / blacktop (Passes Surface Tests)
- Enhanced imaging suggests QC process issue at OCM: Part marking requiring surface re-work OR injection Mold issue NOT effecting functionality
- COO font disparity likely related to supplier Injection mold differences (factory supplier location)
- **OCM ICs may have QC non-conformances, that can be indicted as counterfeit!**



Parts scrapped Pin 1 & COO font Issue will not pass basic QC Inspection!

Supply Chain Case Example 4- **Raytheon** Integrated Defense Systems 3 Mb , 256K, 12 bit Field Memory ; **Training, Construction Knowledge**

- OCM packaging & consistent component finish, pass 1010B QC inspection
- Component packaging pristine, copper NOT present on the lead ends
- Inspection training includes verifying presence copper, lead frame (LF) formation marks, OCM cut striations *Evident*
- LF can come in other metals, IE Kovar (iron Alloy) vs. Sn / Ni / Cu, LF base metal **not** identified on datasheet
- XRF or SEM-edx could verify lead materials
- For low quantity sales, **cost** of analytical testing can exceed the lot value!
- **Rules of thumb do NOT always apply**
- **Engineering judgment & further investigation required to verify authenticity**



No evidence of blacktopping

Datasheet / App. note review & contacting the OCM may be required



Raytheon Case Example-

Fixed Delay Line, Data I/O ; Training, Construction Knowledge

- Components provided to FA lab as **“suspect counterfeit”**
Failing during CCA assembly- Leads de-wetting from the board
Components indicted as “suspect”- Based on appearance due to counterfeit awareness

- Component construction typical of specialized components:
 - > Fixed Digital Delay Lines (DDLs)
 - > Time Delay Units (TDUs)
 - > Bite Line Filters
 - > Low Noise Amplifiers (LNAs)
 - > RF Filters (LP, HP, BP)

- Supplier makes timing devices based on customer’s circuit design application
 - Wired & assembled using manual assembly “commercial best practices”
 - Substrate cap is epoxy potted, following assembly
 - **Surface sanding marks part of assembly process**
 - **Part markings & surface finish consistent with manually assembled specialty components**

Analysis Revealed:

- Component in-correctly indicted initially as “Counterfeit”
- **Supplier Issue, SEM-EDS showed intermetallic formation under the Tin/Lead plate**
- Observations of parts from Stores, lead plating procedures at supplier required review
- Leads could be reworked to meet production needs
- DDD Inc. needed to be contacted, determine if replacement stock is available

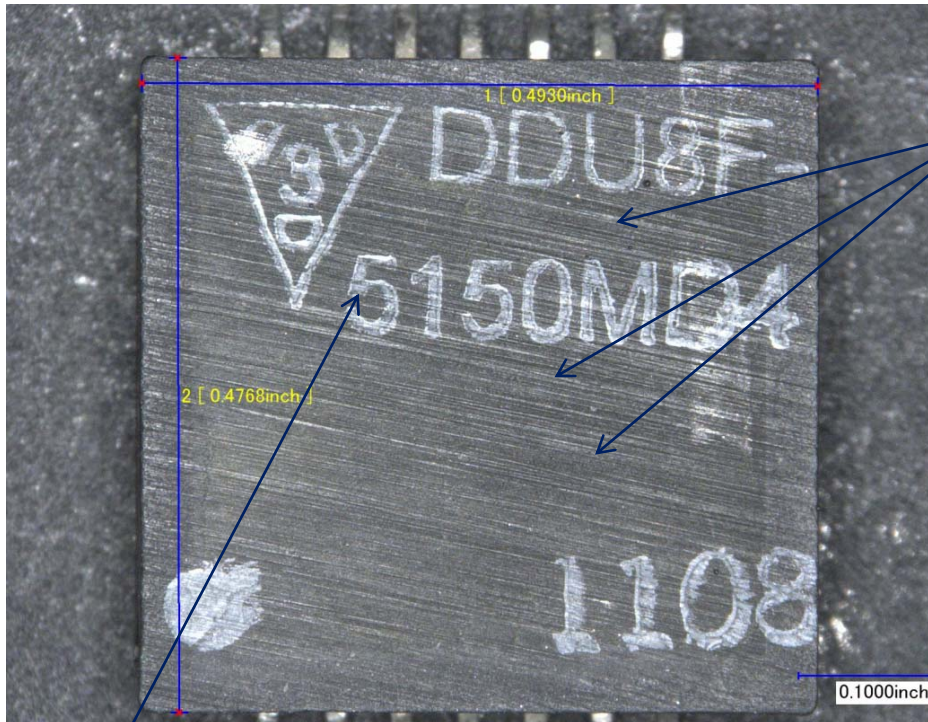
Supplier Issue indicted as *counterfeit* based on cursory knowledge

Raytheon Case Example-

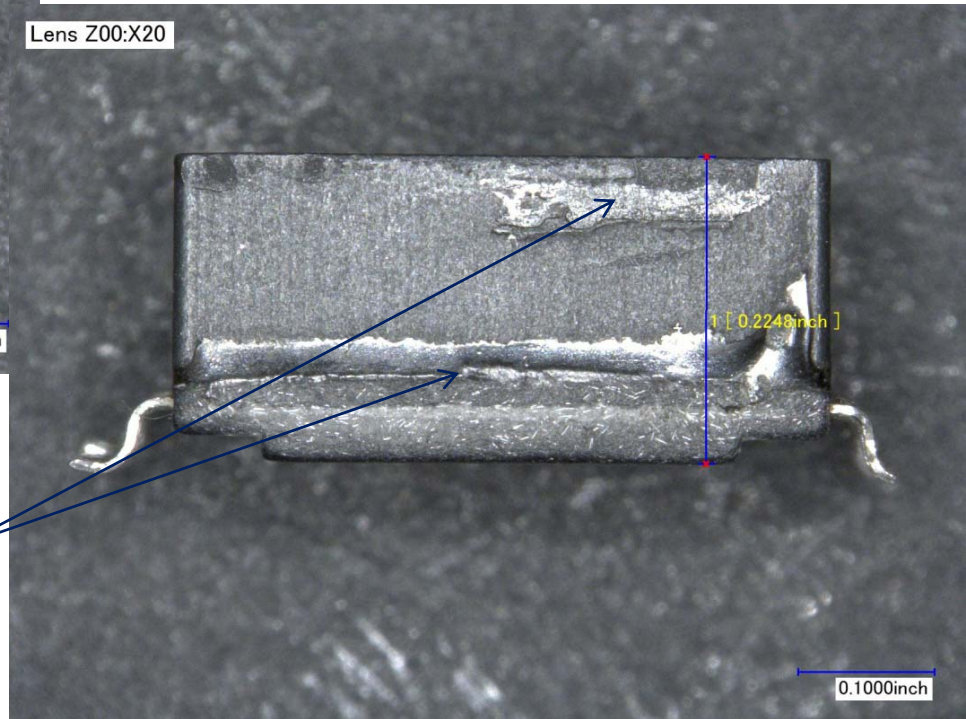
Fixed Delay Line, Data I/O; Sanding Marks, Poor Construction & Print Quality

Raytheon

Integrated Defense Systems



Consistent Sanding Marks, From Manual Assembly



Manually stamped Ink Marks

Component wall epoxied in place, Cavity filled with potting & sanded

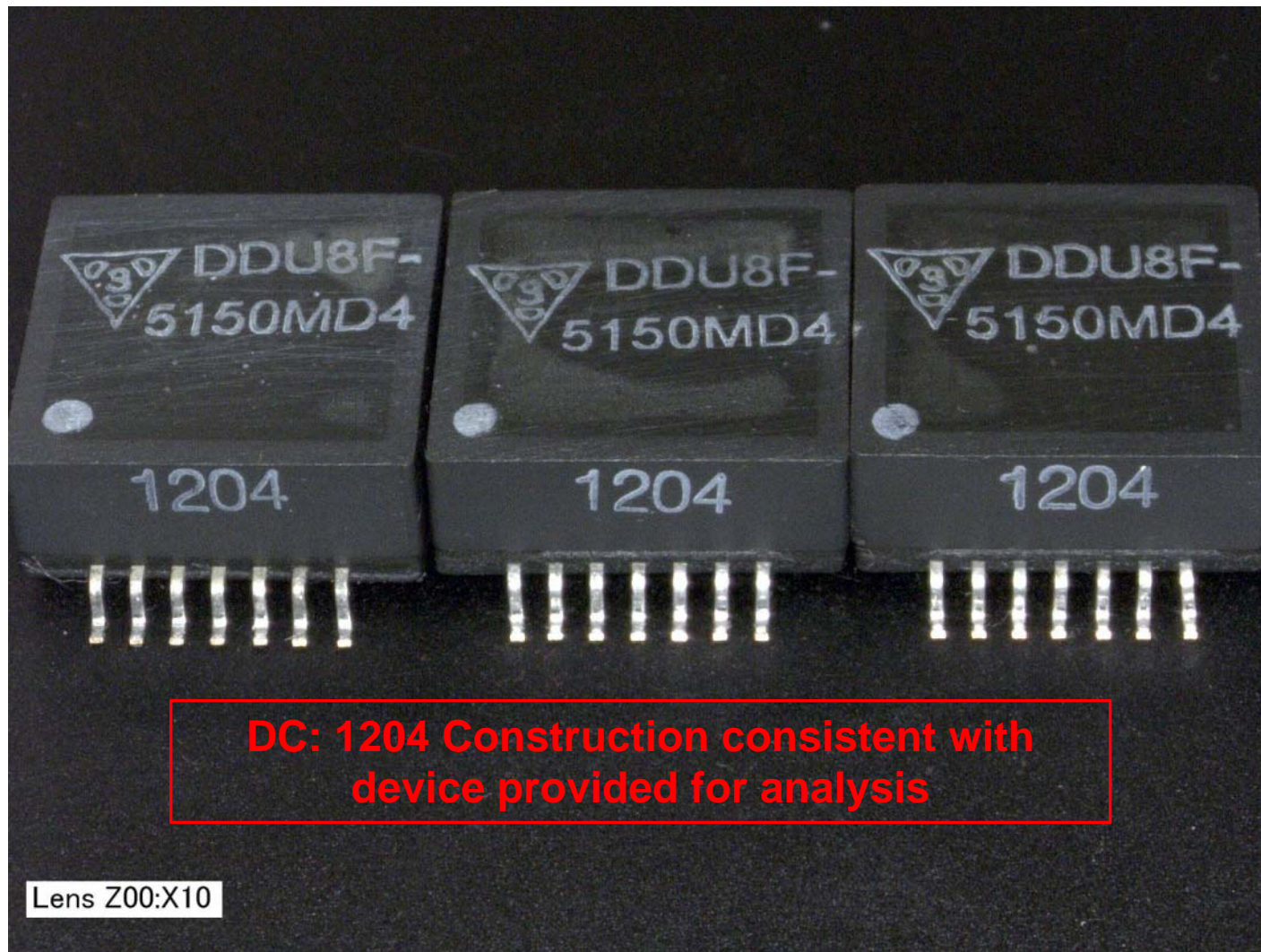
Top & Side View: All dimensions & lead formation meet print

Raytheon Case Example-

Fixed Delay Line, Data I/O; Components from Stores provided

Raytheon

Integrated Defense Systems



Side View: overall, 45 Degree 3D depth up, Purged Devices

Example Database Report-

Category: Suspect Counterfeit

Part: FM93C56M8

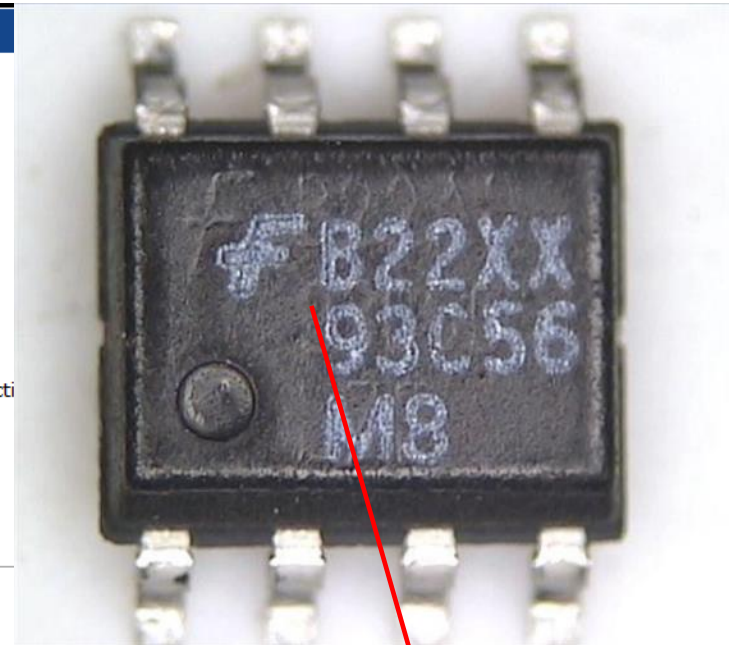
Part Number: FM93C56
Manufacturer:
Date Code: 22
Lot Code: B22XX
Country of Origin:
Suspect Counterfeit: Yes
Date Reported: 08/28/2013

Description of Nonconformance:

Parts were represented as new and unused, however the following nonconformities were observed during inspection of entire lot:

1. Parts failed resistance to solvents (RTS) testing.
2. Parts failed scrape test.
3. Obvious visual evidence of ghost markings.

Available Images and Test/Nonconformance Reports:



- 8/28/13, suspect counterfeit. Fails visual & surface tests per IDEA-STD-1010B
- Ghost markings, WELL known practice for 2 Major OCMs who remarked components to downgrade & sell off production excess to Rochester Electronics, Landsdale, etc. at EOL
- Some OCMs do NOT control markings or conform to QC finish requirements
- Report submitted inaccurate, incorrect category & missing information!

Reporting entity should check with resellers, Ads & OCMs; Gather background information

Summary, Recommendations- *Analysis, Training & Reporting*

- Industry requirements and procedures define inspection techniques but do not provide guidance on interpretation
- Supply chain knowledge / experience gaps exist on execution of visual and surface inspection analysis techniques
- Interpretation is subjective, requires working knowledge of IC supplier assembly / packaging construction, OCM markings & finish quality levels. Quality can vary significantly by supplier!
- Training should include: Analysis interpretation & investigation techniques; Component construction methods; Examples of IC supplier quality issues
- Minimum reporting guidelines for analysis, supporting images & documentation, *Required* to improve data collection & reporting
- Reporting databases NEED a new category: “Lessons learned” or “Exceptions to the Rule”

**DoD and Industry established standards
& procedures require optimization**

Integrated System Product Life Cycle

Secure Hardware & Data Destruction



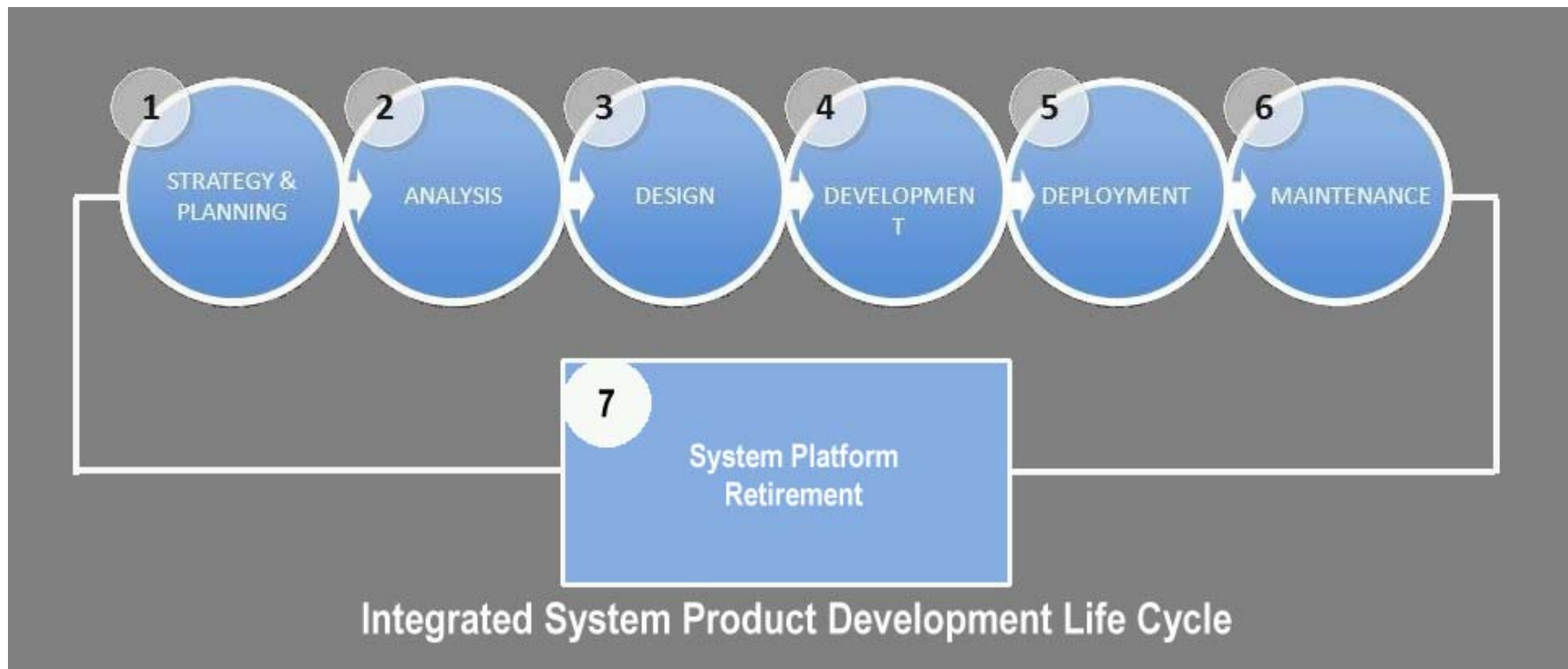
Outline- *Secure Hardware & Data Destruction*

- Systems Product Life Cycle Process (PLCP)- *Issues & Concerns with retired electronics proliferation*
- Quality Management Systems- *Overview of ISO-14000 & R2 / RIOS*
- Security Policies- *Facilities & Personnel*
- Overview Hardware Destruction- *Shredder Process, Raw Material Reclamation*
- Overview Data Destruction (MIL-STD vs. NIST)- *Data storage devices, Destruction & Recycling*
- Other Services- *Assured Destruction, Refurbishment, Equivalency Reports*
- Conclusions & Recommendations

PLCP- Overview

Diagram: Integrated System Product Life Cycle Process

- Systems within DoD & Aerospace have service life requirements that span decades
- Aging equipment is iteratively upgraded to integrate additional capabilities & take advantage of advances in electronic IC's & components



Platform design/development takes years, deployment = decades

System PLCP- *DoD / Aerospace life cycle issues*

Issues: Integrated System Product Life Cycle

- Modernized Defense, Weapon & Aerospace systems contain high value ICs in electronics packaging which meet system environmental requirements
Processors, Memory, Micro-controllers, FPGAs, Mil-Grade specialty components
- Large percentage of components (>80%) are commercial grade!
- HOW** do we ensure valuable electronics ICs are NOT re-claimed by counterfeiters and returned to the supply chain to be re-sold as new?
- Presents SERIOUS system, reliability, readiness (up time) & security concerns
- DoD, MDA & DHS share concerns regarding electronics technology export, IP Infringement (technology matriculation), sensitive data containment & IC re-use through E-Waste exports
- Procedures ARE in place to ensure Classified & Critical Information is destroyed. Collateral system level hardware & data containment needs to be addressed
- Retired / Failed hardware that contain high value legacy electronics MUST be disposed of in accordance with all EHS regulations (Federal, State & local)
- Certified domestic companies provide specialized services to address these concerns

PLC 5 – 7 generate valuable E-waste, domestic services can address this!

Environmental Standards-

ISO 14000 Overview

- **ISO 14001:2004** Environmental quality management standard
Assures proper handling, disposal & reclamation of materials
 - Applicable to organizations that want to establish, implement, maintain & improve an environmental management system. Assures & demonstrates conformity within stated environmental policies
 - Requirements to develop / implement an Environment Management System & Policy
 - Includes legal & other requirements to which the organization subscribes & information about significant environmental aspects
 - Applies to environmental traits that the organization identifies, which it can control & influence, does not state specific environmental performance criteria
 - Certification & registration conformance performed by an accredited CB, conformance includes customer and other interested party audits (Federal/state/local agencies)
 - **Annex A-** provides informative guidance on it's use & Implementation



Standards promote proper handling / disposal of high value electronics

Environmental Standards- R2/RIOS Overview

- **RIOS:2006** Recycling Industry Operating Standard
 - Similar to ISO 9001 Quality Management System (QMS)
 - For recycling companies that want to establish a Quality & Environmental, Health & Safety (QEHS) management system
 - Responsible / secure material de-construction and recycling
 - Requires Independent certification & on-site audits

- **R2 (R2:2008)** Electronics Recycling Operating Standard
 - Specific facility certification for responsible electronics product recycling
 - Includes a broad consortia of electronics recyclers & the Environmental Protection Agency
 - Currently there are 432 Certified E-recyclers
 - Updated **R2:2013** includes **additional** requirements on proper handling of components, traceability & security
 - Consortia Members (Including TCG) working towards updated Compliance requirements in **R2:2013**, anticipated adoption in 2014

Adoption is NOT Mandatory

Establishes a Certified QMS to address proper handling of E-waste



Security Requirements- *ITAR Registered Company*

Security & Containment: *Personnel & Facilities, ALL*

- Employees subject to drug & background checks (7 years- Federal/State/Local)
- Required to use electronic access badges {maintains control of restricted areas}
- Sites monitored with an extensive video surveillance / security system network. 90 day continuous video loop
- Premises alarmed with central security system, restricted Manager / Owner access
- Qualified employees granted access to restricted material areas:
 - ✓ Data Destruction- Biometric restricted access, Limited / cleared employees
 - ✓ Components side- At risk “suspect” components, Locked QC manager access only
- High security fences , Metal detectors in entrance / exit of all facilities



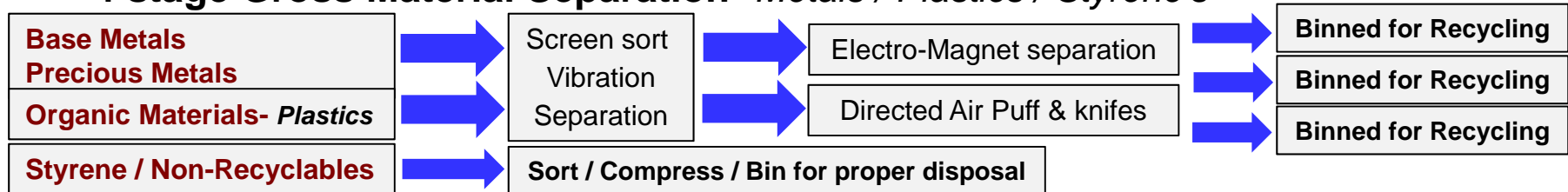
Clearances & controlled limited access ESSENTIAL for containment!

Secured Destruction- *Hardware*

➤ **Industrial Shredder:** Multi-Stage Separation / Reclamation process

Crush & Shred- 2 Stage Multi-Tine electro-hydraulic roll pins

4 stage Gross Material Separation- *Metals / Plastics / Styrene's*



- Reclaimed Base, precious metals & plastic, applied to rebate or payout to customer
- Hardware, data / disk & memory devices can be marked for destruction regardless of condition, ***Based on customer requirements***

Initial Shred

Shredder
Facility
@ TCG



Example, Material Separation



Hardware & Data bearing devices destroyed at customer request



Secured Destruction- *Hardware*

➤ **Industrial Shredder:** 4 stage Separation- Base / Precious Metals, Plastics, Styrene's & other (non-recyclables)



Automated Industrial shredder, Sorts & bins de-constructed materials



Secured Destruction- *Data*

- **Disk Drives (Storage):** Data *ERASED*; drives recycled or destroyed
 - Data security / destruction exceeds federal information protection acts (Multi Write-Clear operations)
 - Area Biometric Access: (authorized personnel only)
Limited / Restricted access
 - Multiple Hard Drive Interfaces:
SATA, IDE, SCSI, ESDI, UDMA, Fibre Channel, USB
 - Data destruction to NIST STD 800-88 (TCG is a NAID member)
[National Association for Information Destruction]
 - Requires Write / Clear operations on all drive data bits 7 Times VS. outdated MIL-STD which requires 3
 - Longer cycle time BUT assures destruction of ALL critical data!
 - Ideal for proprietary, sensitive, company information
 - Does **NOT** include Classified & CPI/CI storage assets. Handled in accordance with OEM / DoD requirements



Automated NIST procedure preferred industry Standard

Secured Destruction- *Data & Other services*

- **Memory devices** (Solid state, Microcontrollers, FPGAs):
 - Destroyed in accordance with secured hardware destruction procedures, based on customer requirements
- **Other Services:** Electronics Refurbishment / Witnessed Destruction
 - **Certificates of information Destruction:** Assure assets are sanitized
 - **Witnessed on-site or remote destruction:** Based on Customer requirements, resources can be on-site to observe destruction or have video of procedure provided with the Destruction Certificate
 - **Microsoft certified asset refurbishment:** Testing / refurbishment requirements imposed. Option to resell/reuse assets for material disposition return
 - **Annual / Semi-Annual equivalency reports:** Based on EPA Waste Reduction Model (WARM), EPEAT & EPA GHG calculators estimate:
 - ✓ **Energy & Solid Waste Savings**
 - ✓ **Green House Gas reduction**
 - ✓ **Compliments & supports corporate “Green” initiatives**



Hardware / Information Destruction Tailored to Customer requirements

Conclusion & Recommendations

- ✓ Containment & Secure destruction of system platform electronics ensures legacy components do not re-enter the supply chain as counterfeit devices!
- ✓ Domestic ISO-14001 R2/RIOS certified electronics recycling companies have Quality, Environmental & Security management systems in place to address the need of Secure Hardware & Data Destruction
- ✓ For secure information destruction work with a company who is a NAID member & utilizes enhanced data clear requirements NIST STD 800-88
- ✓ ITAR Registered facilities have enhanced security requirements in place
- ✓ Confirm your E-Recycler is working towards R2:2013 compliance
- ✓ Services including witnessed / remote destruction & certificates of information destruction assure end of use electronics are traceable and handled in accordance with customer needs
- ✓ Refurbishment is an option to reduce waste reclamation Costs, Work With a Certified Microsoft asset refurbishment organization
- ✓ Equivalency Reports **SUPPORT** corporate EHS “Green” Initiatives



Acknowledgments

The presenter / co-author would like to thank the following from Technology Conservation Group for providing background & inputs for this presentation:

Morgan Deptola- (Quality Control & Inventory Manager ; Components division) Peer review, security procedures / protocol, supply chain examples & supporting images

Steve Craig- (EHS Corporate Compliance Director) Shredding Facility & data destruction tours, review of corporate security protocol & assurance measures, RIOS / R2 & ISO-14001 overview

Hamilton Rice- (CEO) Knowledge sharing for industry awareness & training, facility host & tour



Acronyms, Definitions

AT&L: Acquisition, Technology & Logistics; DoD undersecretary (OSD)

AD: Authorized Distributor

BU: Business Unit

CAT: Counterfeit Avoidance Team (Enterprise wide)

COTS: Commercial Off The Shelf (components, products)

CB: Certification Body

CPB: Customs Protection & Borders

CPI/CI: Critical Program Information / Counterintelligence

CTN: Components Technology Network (Enterprise wide)

DFARS: Defense Federal Acquisition Regulation Supplement

DHS: Department of Homeland Security

DLA: Defense Logistics Agency

DLAD: Defense Logistics Acquisition Directive

DMS: Diminishing Manufacturing Supply (source)

DoD: Department of Defense (U.S.)

DoJ: Department of Justice (U.S.)

ECA: Electronics Components Association Standards

EHS: Environmental Health & Safety

EOL: End Of Life (System Refurbishment / Upgrades)

ERAI: Electronic Resellers Association Incorporated

ETMA: Engineering Technology & Mission Assurance

FD: Franchised Distributor

GAO: Government Accountability Office (U.S.)

GIDEP: Government-Industry Data Exchange Program

GIFAS: French Aerospace Industries Association

ICE: Immigration & Customs Enforcement

IEC: International Electrotechnical commission

IC: Integrated Circuit

ID: Independent Distributor

IDEA: Independent Distributors of Electronics Association

iNEMI: International Electronics Manufacturing Initiative

Infringement: Describes a violation of rights on intellectual property, copyright or patent

IP: Intellectual Property, patented or trade secret body of work

ITAR: International Traffic in Arms Regulations

KPA: Key Process Area

Legacy: Previous generation system (Military / Aerospace)

LF: Lead Free

LMS: Learning Management System, Raytheon Training tool

LTB: Last Time Buy

MDA: Missile Defense Agency

MIL Spec: Military Specifications

MIL-STD: Military Standard (specifications)

NDAA: National Defense Authorization Act, Implemented Annually

NHA: Next Higher Assembly

OCM: Original Component Manufacturer

OEM: Original Equipment Manufacturer (Systems)

OSD: Office of the Secretary of Defense (U.S.)

PCN: Product Change Notice

PLCP: Product Life Cycle Process

POC: Point Of Contact

PPP: Program Protection Plan

Prime: System Design Lead / Provider

QC: Quality Control

RESA: Raytheon Enterprise Supplier Assessment

RoHS: Reduction of Hazardous Substances

RTN: Raytheon

SAE: Society of Automotive & Aerospace Engineering

SEM-edx: Scanning Electron Microscopy-energy dispersive x-ray spectroscopy

SASC: Senate Armed Services Committee

SIA: Semiconductor Industry Association

SME: Subject Matter Expert

SMT: Surface Mount Technology

Supplier: Sub-system component provider, Sub-Contractor

WEEE: Waste Electrical & Electronic Equipment Directive

WG: Working Group

XRF: X-ray fluorescence