Counterfeit Protection & Detection Strategies: When to Do It / How to Do It

IPC Webinar
December 15, 2011
Instructor Biography

- Cheryl Tulkoff has over 22 years of experience in electronics manufacturing with an emphasis on failure analysis and reliability. She has worked throughout the electronics manufacturing life cycle beginning with semiconductor fabrication processes, into printed circuit board fabrication and assembly, through functional and reliability testing, and culminating in the analysis and evaluation of field returns. She has also managed no clean and RoHS-compliant conversion programs and has developed and managed comprehensive reliability programs.

- Cheryl earned her Bachelor of Mechanical Engineering degree from Georgia Tech. She is a published author, experienced public speaker and trainer and a Senior member of both ASQ and IEEE. She holds leadership positions in the IEEE Central Texas Chapter, IEEE WIE (Women In Engineering), and IEEE ASTR (Accelerated Stress Testing and Reliability) sections. She chaired the annual IEEE ASTR workshop for four years and is also an ASQ Certified Reliability Engineer.

- She has a strong passion for pre-college STEM (Science, Technology, Engineering, and Math) outreach and volunteers with several organizations that specialize in encouraging pre-college students to pursue careers in these fields.
Introduction

- This webinar addresses the unique sources of counterfeit components and provides insights into how they occur.
  - Counterfeit components are a rapidly growing area of concern. The Department of Commerce has identified a 141% increase in the last three years alone!
  - Counterfeit Parts are no longer an emerging threat: they’re real, and they’re here to stay.
  - A counterfeit is any item that is not as it is represented with the intention to deceive its’ buyer or user. The misrepresentation is often driven by the known presence of defects or other inadequacies in regards to performance. Whether it is used for a commercial, medical or military application, a counterfeit component can cause catastrophic failure at a critical time.
  - Detection methodologies, such as visual inspection, mechanical robustness, X-Ray, XRF, C-SAM, Infrared Thermography, electrical characterization, decapsulation, and marking evaluations will be compared and contrasted.
  - Multiple examples of counterfeit parts identified using these techniques will be highlighted.
Topics

- State of Counterfeiting – Background, Facts & Statistics
- Counterfeits Defined
- Strategies for Prevention and Mitigation
- Case Studies and Examples
- Detection and Failure Analysis Techniques
- Summary
The State of Counterfeits

- Increasing concern across all electronics industries
- Department of Commerce measured 141% increase over past three years
- Recent DfR counterfeit activities
  - Military Communications
  - Internet Routers
  - Air Traffic Control
  - Consumer (Repair)
ERAI (Electronic Retailers Association International) Data

- Recent 2011 example of two weeks of ERAI data, www.erai.com
  - Five suspect counterfeit shipments (3 ICs, 1 transistor, 1 capacitor) worth ~$55,169
    - 6,233 ICs at $44,154 = $7.08 per
    - 500 transistors at $1,015 = $2.03 per
    - 200,000 capacitors at $10,000 = $0.05 per
  - Just the companies that were reported by ERAI members, usually due to disputes

- Seldom reported to GIDEP (Government Industry Data Exchange Program), www.gidep.org, but should be!
The Counterfeit Crisis - 2011 Special Report
- Counterfeits in the Crosshairs
- Best-in-class Component Risk Mitigation Practices to Avert Procuring Counterfeits
- Setting the International Standard(s) in the Fight against Counterfeits
- The Role of Standards Management Technology in Mitigating Counterfeit Risk
- Supply Chain Best Practices for Supplier and Parts Risk Mitigation
- Case Study: Fighting The Fakes
- When Predators Lurk, Keep a Close Eye on the Leader
Who is ERAI?

- Founded in 1995, ERAI is an information services organization that monitors, investigates and reports issues affecting the global hi-tech electronics supply chain.
- ERAI provides tools to mitigate risks on substandard parts, counterfeit parts, vendors and even customers.
- Subscribers include OEMs, CMs, Distributors, OCMs, government agencies and industry associations.
- Founding participant in SAE International G-19 Counterfeit
  - Not a distributor or parts broker
  - Not a sourcebook or online catalog
  - Not a component manufacturer or OEM
  - Not a test lab or inspection service
  - Not a quality standards organization
What is GIDEP?

- GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information. Since 1959, over $2.1 BILLION in prevention of unplanned expenditures has been reported.
The Lucrative Economics of Counterfeiting (ACE Example)

- ICM7170 is a microprocessor-compatible real-time clock, manufactured by Harris/Intersil
  - ICM7170IPG:
    - -40C to 85C Temperature Range
    - 24-Lead Plastic Dual-In-Line Package (PDIP)
    - 20uA Maximum Standby Current at 32kHz
  - ICM7170AIBG:
    - -40C to 85C Temperature Range
    - 24-Pin Small Outline Plastic Package (SOIC)
    - 5uA Maximum Standby Current at 32kHz
- ICM7170IPG
  - Counterfeiter bought for $.02
  - Sold for $38.00 each as ICM7170AIBG’s
  - Built around 45k/month which equals a potential gross profit of $2,000,000 per month!
Counterfeit Parts Defined

- What are they?
- What is their impact?
- Where do they come from?
- Identification
- Industry
- Countermeasures
- Avoidance
- Mitigation
What are counterfeit parts?

- Any part or component that is not as represented
  - Duplication of another manufacturer’s product
  - Manufacturer’s product that failed test, inspection, or burn-in or was an engineering sample
  - Empty package or wrong functionality

- Parts being counterfeited include:
  - Newest parts & components
  - Obsolete parts
  - Inexpensive parts as well as high value parts
Top 4 Types of Counterfeits

- Used product marked as higher grade new product
  - These types of counterfeit parts may work, but will not operate at the same level as the higher grade part and may fail under stress that would be expected under normal conditions.
  - Electronics recycling or salvage sources
- Fake, non-working product
  - Disguised parts
- Defective Scrap
  - Inside sources
- New product re-marked as higher grade product
  - Like re-marked used product, re-marked new product will work, but not at the desired level of functionality.
# Types of Confirmed Counterfeits

- **Microcircuits**
  - Microprocessors
  - Other Microcircuits
  - Memory
  - Radio
  - **Radio Frequency/Wireless**
  - Logic, Standard
  - Special Purpose Logic

- **Discretes**
  - Electromechanical
  - Thyristors
  - Capacitors
  - Other Discretes
  - Circuit Protection/Fuses
  - Diodes
  - Resistors
  - Sensors & Actuators
  - Optoelectronics
  - Power Transistors
  - Rectifiers
  - Small Signal Transistors
  - Magnetics
  - Crystals/Oscillators
Primary Generators of Counterfeit Parts

- **Inside Job**
  - Failed parts off the production line
  - May operate in benign environment

- **Competitors**
  - Unknown competitor may package and label the same as a known company
  - May function as a direct replacement (may not)

- **Fraudulent**
  - Empty package or wrong chip
  - Will fail immediately
Primary Sources of Counterfeit Parts

- Most counterfeit parts come from parts brokers that deal in small and odd lots
- Low volume of obsolete parts bought off the internet
- Authorized parts distributors rarely have counterfeits because they receive them directly from the original component manufacturer (OCM)
- Regions with highest counterfeit activity:
  - China
  - Middle East
  - Eastern Europe
  - But truly a global problem!
Environmental Legislation

- Providing additional opportunities
  - Recycling
  - Need for obsolete SnPb parts

### Immigration and Customs Enforcement (ICE) Top Commodities Seized 2004 – 2006

<table>
<thead>
<tr>
<th>Commodity</th>
<th>M $</th>
<th>Commodity</th>
<th>M $</th>
<th>Commodity</th>
<th>M $</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wearing Apparel</td>
<td>$51.7</td>
<td>Wearing Apparel</td>
<td>$16.0</td>
<td>Footware</td>
<td>$63.4</td>
</tr>
<tr>
<td>Cigarettes</td>
<td>$24.2</td>
<td>Handbags/Wallets/Backpacks</td>
<td>$14.9</td>
<td>Wearing Apparel</td>
<td>$24.3</td>
</tr>
<tr>
<td>Handbags/Wallets/Backpacks</td>
<td>$23.2</td>
<td>Cigarettes</td>
<td>$9.6</td>
<td>Handbags/Wallets/Backpacks</td>
<td>$14.7</td>
</tr>
<tr>
<td>Consumer Electronics</td>
<td>$8.8</td>
<td>Footware</td>
<td>$8.9</td>
<td>Computers/Hardware</td>
<td>$14.2</td>
</tr>
<tr>
<td>Media</td>
<td>$5.0</td>
<td>Consumer Electronics</td>
<td>$8.7</td>
<td>Consumer Electronics</td>
<td>$7.0</td>
</tr>
<tr>
<td>Toys/Electronic games</td>
<td>$3.9</td>
<td>Toys/Electronic games</td>
<td>$8.5</td>
<td>Media</td>
<td>$6.9</td>
</tr>
<tr>
<td>Watches/Parts</td>
<td>$2.5</td>
<td>Computers/Hardware</td>
<td>$4.7</td>
<td>Headwear</td>
<td>$3.2</td>
</tr>
<tr>
<td>Batteries</td>
<td>$2.3</td>
<td>Watches/Parts</td>
<td>$3.0</td>
<td>Healthcare</td>
<td>$3.0</td>
</tr>
<tr>
<td>Footwear</td>
<td>$2.0</td>
<td>Perfumes</td>
<td>$2.7</td>
<td>Watches/Parts</td>
<td>$2.8</td>
</tr>
<tr>
<td>Computers/Hardware</td>
<td>$1.6</td>
<td>Pharmaceuticals</td>
<td>$2.0</td>
<td>Pharmaceuticals</td>
<td>$2.2</td>
</tr>
<tr>
<td>All Other Commodities</td>
<td>$13.2</td>
<td>All Other Commodities</td>
<td>$13.5</td>
<td>All Other Commodities</td>
<td>$13.0</td>
</tr>
</tbody>
</table>

Total FY 04 Domestic Value       $138  Total FY 05 Domestic Value $92.5  Total FY 06 Domestic Value $154.7
Cost Impacts of Counterfeiting to Semiconductor Manufacturers

- **Visible Costs**
  - Revenue Loss
  - Device level anti-counterfeiting measures
  - Personnel measures

- **Hidden Costs**
  - Avoiding potentially lower cost manufacturing companies or regions of the world
  - Reputation / Brand
  - Loss of Credibility to buyers
Anti-counterfeiting Personnel Costs

- Training
- Tracking
- Inspection
- Testing
- Paperwork
  - Control
  - Analysis
  - Procedures
Procurement training
  - Limiting potential sources and purchasing controls

Staff/operator training

Incoming product inspection
  - Time, tracking, test equipment

Control and testing of product sourced from non-approved or infrequently used sources.

Loss of manufacturing time and output while re-sourcing device if counterfeits are found or delivered

Costs if counterfeit gets into manufacturing process
  - Rework or scrap
End Component User Costs

- Additional servicing and spares
- Premature equipment failure
- Equipment downtime
- Defects or bugs causing malfunction
- Legal expenses: downtime, damage, failure to perform, injury, loss
Establishing an Anti-Counterfeiting Protection and Detection Program
Potential Obstacles to a Successful Anti-Counterfeit Program

- **Complacency**
  - Won’t or can’t happen here
  - Hasn’t happened yet
  - Unclear ownership of issue

- **Not understanding or underestimating the threat**
  - Only expensive parts are counterfeited
  - Buy from an “American” company
  - Parts use latest design
  - Distributor provides a Certificate of Conformance (C of C)
  - Receiving inspection or test process will catch fakes

- **Federal Acquisition Regulation (FAR)/ Defense (DFAR) issues**
  - FAR/DFAR says use the lowest bidder
  - Need to meet Small Disadvantaged Business quota
  - If I restrict where I buy from, I will pay more money

- **Supply chain excuses or push back**
  - Expensive: here’s the bill for it, $$
  - You want to know every time I buy a high risk part?
  - Other customers don’t have the requirement
  - Liability
Potential Obstacles to a Successful Anti-Counterfeit Program

- Affordability is key
- No one size fits all strategy
- Mitigations must pass the cost versus outcome test
- Counterfeit Parts are no longer an emerging threat. They’re real, and they’re here to stay.
Cost-Effective Counterfeit Protection Approach

- Research
- Carefully Select Sources
- Purchasing Best Practices
- Lot Validation Testing
Counterfeit Protection Strategies

- **Do Your Homework**
  - Contact Original Component Manufacturer (OCM) and franchise distributors first
  - Confirm product status
    - Is the product end of life (EOL)?
  - Check for authorized aftermarket sources
  - Determine if/when the product went EOL
  - Determine EOL production lot date codes
  - Try to locate a known good device
  - Check with industry sources like ERAI or GIDEP for counterfeit activities of the product needed.

- **Choose Sources Wisely**
  - Don’t use cost as sole/primary criteria for purchase
  - Quality Product is goal
  - Use industry sources like ERAI to evaluate potential sources
  - Ask for accreditations, certifications & memberships
    - ISO9011, AS9120, IDEA-1010, ERAI or IDEA Members
  - Audit sources
Choose Your Sources Wisely (continued)

- Purchase only from suppliers who have implemented and are committed to counterfeit avoidance practices
  - Ask about counterfeit policy
- Components
  - Understand warranty and payment terms
- Create a list of approved, trusted Suppliers
- Create supplier partnerships and use them
Purchasing Best Anti-Counterfeiting Protection Practices

- Clearly communicate objectives and needs
- Create company policy on counterfeits
- Look for product in stock, not just availability
- Ask if the product is traceable back to the OCM
- Don’t buy COD.
  - Negotiate terms or use escrow services.
  - Allows time for authenticity checks & testing to be performed before paying
- Before buying, ask for photos and evidence
  - Images of the front and back
  - Compare date codes and EOL date for product
  - Compare marking with known-good product
  - Do your research now as it will save you money later
- Understand the product warranty
  - Anything less than 30 days is a RED flag
  - If supplier does not have confidence in the product, why would you?
Broker or Independent Distributor Basics

- Not all Brokers & Independent Distributors are the same
- Many have minimal Quality Systems and no ESD, storage, or handling controls.
- Some have no experience with semiconductors
  - The Internet has created virtual companies
  - Product quality is compromised
- Traceability back to the original OCM is unavailable
  - Limited or no product warranty
  - No product support
- Buying obsolete products requires more diligence, not less
Evaluate & Validate ALL broker material

- Define Test Plan based on your level of risk
  - What is your application? Commercial? Military?
- Define your test plan to meet risk mitigation needs
  - State requirements in writing and be as detailed as possible
- Require documented reports of all validation tests
  - Copy of lot information detailing all tests performed and results
    - Die ID Photos
    - X-Ray Photos
- Choose a reputable Test Lab/Partner based on accreditations and capabilities, not on price alone.
  - Ask for details of test plan prior to starting test
  - Get multiple bids when electrical test is part of your plan
- If your supplier provides Lot Validation Testing in the purchase price:
  - Provide your test requirements to your supplier
  - Compare their test plan against your risk mitigation needs
  - Understand what you are paying for, get competitive bids
  - Ask who will be performing the testing on your material
New & Revised anti-counterfeiting SEMI Standards

- The list of new SEMI Standards includes:
  - SEMI T20.1 - Specification for Object Labeling to Authenticate Semiconductors and Related Products in an Open Market
  - SEMI T20.2 - Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting of Semiconductors and Related Products
  - SEMI E153 - Specification for AMHS SEM (AMHS SEM)

- In addition to the three new standards, three SEMI Standards were completely rewritten:
  - SEMI MS2 - Test Method for Step Height Measurements of Thin Films
  - SEMI MS4 - Standard Test Method for Young's Modulus Measurements of Thin, Reflecting Films Based on the Frequency of Beams in Resonance
  - SEMI T20 - Specification for Authentication of Semiconductors and Related Products

- As part of the July 2009 publication cycle, these three SEMI Standards were released:
  - SEMI D54 - Specification for Substrate Management of FPD Production (SMS-FPD)
  - SEMI E152 - Mechanical Specification of EUV POD for 150 mm EUVL Reticles
  - SEMI PV2 - Guide for PV Equipment Communication Interfaces (PVECI)

- www.semi.org
Complex Supply Chains

• Multiple points of entry
• Porous return policies

MuCircuit Design
Fab
Avionics
OEM
Ass’y
Dist.
Test
Lloyd Condra, Boeing

NEDA targets counterfeit components with return guidelines
NEDA has released its guidelines on returns, aiming to reduce the number of counterfeit electronic parts entering the electronics supply chain.

By Suzanne Deffres, Managing Editor, News – EDN, 2/4/2010

The NEDA (National Electronic Distributors Association) has released its guidelines on product returns, aiming to provide a clear-cut process to ensure the legitimacy of products customers purchase through an authorized distribution channel. According to NEDA, the primary entry of counterfeit electronic parts into the electronics supply chain is purchasing from unauthorized sources, such as brokers and unauthorized distributors. The group’s goal is to strengthen the integrity of the electronics supply chain when customers purchase through authorized distribution.
Counterfeit Sources

- Many unsafe part & supplier sources
  - Online Broker Search Engines
  - Maverick procurement methods or spending limits
  - Google

- These are counterfeit ports of entry
  - Rapid access to millions of parts
  - Minimal membership requirements
  - Quick & easy access to a large audience of buyers
Trusted Supply Chain

- Direct from the Factory (Original Component Mfg: OCM)
  - Approved Vendor / Manufacturer (AVL / AML)
  - Franchised and Authorized Sources
  - Approved Independent Distributors
- ERAI Members
- Qualified Sources of Supply
  - Suppliers
  - Manufacturers
  - Parts (or alternates meeting the above criteria)
Decision Process

- If prevention is not realistic, when to detect?
- How to mitigate?
- Entry for counterfeit components is cost
  - Cost to procure < cost of redesign (+ requal, etc.)
  - If cost to mitigate is too high, then redesign
- How to determine the appropriate cost to detect and mitigate?
  - Driven by probability / mission risk / volume matrix
Threat Evaluation

- **THREAT ASPECTS**
  - Probability
  - Knowledge of Part
  - Timing of Effect
  - Where Part Can be Found
  - Destructiveness

- **OBSERVABILITY**
  - Measureable
  - Accessible
  - No damage
  - Intermittent
  - Unknown Latency
  - Provokeable
Counterfeit Probability

- Probability of counterfeit (per shipment) tends to display order of magnitude dependence on component source
  - May vary based on supply chain and component technology

<table>
<thead>
<tr>
<th>Source of Components</th>
<th>Probability of Counterfeit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Manufacturer</td>
<td>0.02%</td>
</tr>
<tr>
<td>Licensed Distributor</td>
<td>2.0%</td>
</tr>
<tr>
<td>Broker (Known)</td>
<td>20.0%</td>
</tr>
<tr>
<td>Broker (Unknown)</td>
<td>20.0%</td>
</tr>
</tbody>
</table>

Known: Existing business relationship
Unknown: No existing business relationship (e.g., eBay)
Case Study

- Telecom OEM procures one reel of capacitors from known broker
  - End-of-life (EOL) product

**Decision Matrix**

- Probability is 2%  
  Volume is 4000 parts  
  Mission Risk is $5M
  - Eight capacitors per CCA (500 CCAs)
  - $10K cost of quality ($5K COGS + $1K service + $4K loss of market)

- DfR recommended that $10K to $100K should be spent on counterfeit detection and mitigation
  - Industry ROI can be 1:1 to 10:1
Detection of Counterfeits

- Counterfeiters are increasingly sophisticated
- Use of actual parts at the start and end of a reel
  - Challenges sampling techniques
- Inspection and comparison of known-good to possible counterfeits
  - Markings
  - Internal structure
  - Performance measurement
## Detection/Risk Mitigation Methods

<table>
<thead>
<tr>
<th>Counterfeit Concern</th>
<th>Visual / Marking Inspection</th>
<th>Verificati on of Manuf. LDC, SNs, etc.</th>
<th>Material Analysis</th>
<th>Seal Test</th>
<th>Radiographic</th>
<th>DPA</th>
<th>Minimal Electrical Test</th>
<th>Full Electrical Test (Ambient)</th>
<th>Full Electrical Test (Hot / Cold Ambient)</th>
<th>Test &amp; Burn-in and QCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Die / Non-functional</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Material Content</td>
<td>P</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Wrong Die</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Re-used / Repaired / Salvaged</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Scrapped / Reject</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mechanical Damage</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Mis-Handling / Storage</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manufacturer Change</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>Yes</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Less Reliable Parts</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>Reliability / Quality Issue</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
</tr>
<tr>
<td>ESD / EOS Damage</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Counterfeit with functional die</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>No</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Temperature Range Upmarking</td>
<td>No</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>P</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Shading:**
- Green = Low Cost / Easily Accomplished
- Yellow = Moderate Cost / Some time involved
- Red = High Cost / Significant time to accomplish
- Dotted Pattern = Will be found at first electrical test

**Code:**
- No = Unlikely to Find
- P = Possibly Find
- Yes = Probably Find

---

T. Apple 610-531-5484

---

This chart was developed from one created by Mark Marshall of Integra Technologies.
Detection Techniques (cont.)

---

**Detection Techniques (cont.)**

- **Add material check / seal test / radio-graphic or do basic electrical testing**
- **Add full ambient electrical tests**
- **Add QCI and other lot acceptance testing**
- **Add post burn-in full electrical tests over temperature**
- **Add burn-in**
- **Add full electrical tests over temperature**
- **Add DPA**
- **Add material check / seal test / radio-graphic or do basic electrical testing**
- **Add full ambient electrical tests**
- **C of C Only**
- **Check Alerts**
- **Visual Inspection**

---

**Reliability (Probability of Detection)**

- **Low cost / repairable / redundant systems**
- **Moderate cost / repairable-replaceable / non-mission critical**
- **High cost / non-repairable / mission critical**

---

**Item End-Use Requirements**

---

T. Apple 610-531-5484
theodore.s.apple@lmco.com

Case Study – Visual Inspection

- Capacitor Group 1, Fluorescent Light - Dark Brown
- Capacitor Group 2, Fluorescent Light - Pink
- Capacitor Group 3, Fluorescent Light - Greenish Gray
- Capacitor Group 4, Fluorescent Light - Bluish Gray
- Capacitor Group 5, Fluorescent Light - Light Brown

- Five different capacitor types in one reel
Which is counterfeit?

- The one with markings? Or the two that seem to have none?
- Two samples are non-functional and one functions
Customer experienced two failures

- Left: known good part; center and right: bad parts
- Center part: no die; right part: cracked die
Date Code Marking - Differences

<table>
<thead>
<tr>
<th>Surface</th>
<th>Registration (mm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smooth</td>
<td>2.22</td>
</tr>
<tr>
<td>Even</td>
<td>12.00</td>
</tr>
<tr>
<td>Textured</td>
<td>3.18</td>
</tr>
<tr>
<td>Uneven</td>
<td>12.00</td>
</tr>
</tbody>
</table>

Lettering:
- Uniform depth
- Uneven depth
Blacktopping Defined

- Blacktopping is a counterfeiting technique where the counterfeiter:
  - Takes components, usually real, but discarded
  - Sands them to remove the original component marking
  - Blacktops them in order to hide the original marking
  - Prints them with fake markings.
  - Investigators able to dissolve the blacktop with a solvent solution that revealed the true identity of the components.
    - Many blacktopped components can be uncovered by vigorously wiping acetone on the component
    - But, methods used to blacktop sanded parts improve daily
Examples of Blacktopping

L01, remarked date code, VC36 changed to GC33
Just under top surface, date code mismatch and hynix part

L011, hynix part
Blacktopping & Acetone Wipe Test

Appearance After Acetone Wipe: change in texture and finish

Evidence of Sanding: Visible after blacktopping is removed

Photos courtesy of Oxygen Electronics
Visual Inspection Cost vs. Benefit

- $1K to $3K
- Identify color differences in parts
- Ascertain marking imperfections/changes/blacktopping
- Lead finish and variability
- Co-planarity of leads — reused parts
Case Study: Counterfeit FETS-X-Ray

- Customer has an issue with DC to DC converter failures
- Simulation models did not predict the failures
- X-ray inspection of the failed units

Parallel FETS
Loose Parts

Z436, Z536

Z536

Z536

Z536

EZ609
Summary

This is not an STS25NH3LL Part, does not meet resistance specifications.

Its higher drain to source resistance will cause its parallel FET partner to carry all the current. This part is present in the failed KT Master module.

FETs with large die have similar resistances and electrical performance, regardless of lead frame style.
X-Ray Cost vs Benefit

- $1K to $3K
- Verification of die and wire bonding pattern
- Internal construction of component
- Die bonding delamination issues
- Die attach voiding
Case Study – Electrical Characterization

- Suspect capacitor - group 2
  - Capacitance (F)
  - Dissipation factor
  - Temperature (°C)
  - Cap 4 - Bag 10
  - Limit 1
  - Limit 2
  - Top
  - Within spec
  - Bottom
  - Out of spec

- Suspect capacitor - group 3
  - Capacitance (F)
  - Dissipation factor
  - Temperature (°C)
  - C7 SN2854 - 0632
  - Limit 1
  - Limit 2
  - Top
  - Within spec
  - Bottom
  - Out of spec
Electrical Characterization of Counterfeit Diodes

Breakdown:
280V
250V

Breakdown:
50V
420V
Electrical Characterization of Counterfeit Diodes

Recovery measurements

Acceptable Waveform

Counterfeit Waveform
Electrical Characterization Cost vs. Benefit

- $3K to $6K – passives, simple actives
- One temperature for evaluation
- $15K to $80K – characterization of complex IC, fixturing, test equipment
- Potential for circuit board design, layout and fabrication costs to enable testing

COMMENT: You can’t afford the risk associated with buying expensive ICs from unknown suppliers
Case Study – Mechanical Robustness

- Thermal Shock Test (EIA-595 allows for 5 mil depth)
  - 35% of counterfeit caps had had unacceptable chip-outs

Pictures of chip-outs of counterfeit capacitors (left) and OCM capacitors (right)
Mechanical Robustness-Cost vs. Benefit

- $2K to $5K
- Thermal cycling or other testing to verify component is not counterfeit
Destructive Physical Analysis (DPA)

- $7 to $10K passives
- $8 to $12K actives
- Step by Step analytical approach to identifying whether a device is counterfeit using all tools available.
# Samsung Marking Information

1. **SAMSUNG logo**: SAMSUNG or SEC

<table>
<thead>
<tr>
<th>top marking type</th>
<th>mark criteria</th>
<th>package</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAMSUNG marking</td>
<td>&gt;11.2mm</td>
<td>U-BGA, W-BGA, TBGA, FBGA etc</td>
</tr>
</tbody>
</table>

2. **Year & Week**

3. **Part Number**: Refer to Part No. decoder page

4. **Lot Number**

   Country of origin not a standard Samsung marking feature
Example of SAC part labeled SnPb
B136988 - U2 and BU7

Identical part numbers different marking styles
Examples (cont.)

Different die sizes

DfR Solutions
Results

- Memory still on board
  - SN 5400031117 – BU1 and BU7

Possible remark

Hynix part
SN 5400031117 – BU1 and BU7

BU1

Same part but a better remarking, same die sizes

BU7
Results

- Memory still on board
  - SN 5400034068 – BU1 and BU7

![Image of product labels]

No anomalies
SN 5400034068 – BU1 and BU7

Same part but a better remarking, hynix marking visible
SN 5400034216 – BU1 and BU7

BU1

Same part

BU7
Case Studies Conclusion

- Counterfeits are a real threat and growing
  - Complex supply chain provides multiple entry points
- Risk needs to be managed through a decision matrix
  - Probability / Mission Risk / Volumes
- Helps provide clear boundaries and guidelines for mitigation practices
- Costs are not prohibitive and should be chosen as a function of risk mitigation
Part II: Counterfeit Component Inspection & Detection Techniques Explained
Identification of Counterfeits

- Counterfeiters are increasingly sophisticated
- Use of actual parts at the start and end of a reel
- Inspection and comparison of known good to possible counterfeits
  - Markings
  - Internal structure
  - Performance measurement
  - Manufacturers marking on die (destructive)
**Commonly Specified or Desired Inspection & Test Requirements**

- External visual inspection
- Paperwork check
- Marking permanence
- Scanning Acoustic Microscopy (SAM)
- XRF check of terminations
- X-Ray check for internal
- De-cap (Decapsulation) inspection
- Electrical testing
General Parts Analysis Techniques

- Parts failure analysis always starts with Non-Destructive Evaluation (NDE)
  - Designed to obtain maximum information with minimal risk of damaging or destroying physical evidence
  - *Emphasize the use of simplest tools first*

- Generally non-destructive techniques:
  - Visual Inspection
  - Electrical Characterization
  - Time Domain Reflectometry
  - Acoustic Microscopy
  - X-ray Microscopy
  - Thermal Imaging with Infra-red (IR) camera
  - SQUID Microscopy
Part / Failure Analysis Techniques

- **Destructive evaluation techniques**
  - Decapsulation
  - Plasma etching
  - Cross-sectioning
  - Thermal imaging (liquid crystal; SQUID and IR also good after decap)
  - Surface/depth profiling techniques: SIMS-Secondary Ion Mass Spectroscopy, Auger
  - OBIC/EBIC
  - FIB - Focused Ion Beam
  - Mechanical testing: wire pull, wire shear, solder ball shear, die shear

- **Other characterization methods available**
  - FTIR- Fourier Transform Infra-Red Spectroscopy
  - Ion chromatography
  - DSC – Differential Scanning Calorimetry
  - DMA/TMA – Thermo-mechanical analysis
Electrical Characterization: Components

- **Parametric characterization**
  - Comparison of performance to datasheet specifications

- **Curve tracer**
  - Applies alternating voltage; provides plot of voltage vs. current response
  - Valuable in characterizing diode, transistor, and resistance behavior

- **Time domain reflectometry (TDR)**
  - Release and return of electrical signal along a given path
  - Measurement of phase shift of return signal indicates potential location of electrical open

- **Other characterization equipment**
  - Inductance/capacitance/resistance (LCR) meter
  - High resistance meter (leakage current < nA)
  - Low resistance meter (four wire; < milliohms)

- **Use of additional environmental stresses**
  - Semiconductor-based devices
    - Temperature rise or temperature/humidity could trigger elevated leakage current
  - Passive components
Part Analysis Techniques: Visual Inspection

- **Rapid identification of:**
  - Lot ID: Was the sample covered by a previous corrective action? FA complete!
  - Date Code
  - Supplier

- **Naked eye/magnifying glass/hand-held camera**
  - Low cost, limited magnification
  - Results can be documented using a digital camera
  - Do not underestimate the value of this technique!
Curve Tracing

- **Some limitations of physical characteristic testing**
  - Parts may be re-manufactured or factory rejects in what appears to be authentic packaging
  - No conclusive identification information on the die once decapsulated
- **Therefore, some electrical analysis is helpful in determining authenticity.**
  - Although full datasheet testing is highly recommended for high reliability applications, a curve trace on each lead is a very effective way to begin an electrical examination of the parts.
  - A known good or reference component is required.
Higher Risk Non-Destructive Inspection

- NDE sometimes carried out in a semi-automated manner
  - All incoming failures subject to the same series of NDE processes
  - Important to understand that NDE equipment is not completely non-destructive

- Thermal imaging
  - Temperature rise can damage or mask fragile conductive filaments (joule heating, thermal runaway, evaporation of retained moisture)

- Acoustic microscopy
  - Can remove residues/contaminants when product is submerged in water
  - Selection of bath fluid is key (distilled/deionized water; IPA; oil; etc.)
  - Issue for moisture sensitive components

- X-ray microscopy
  - Elevated exposure, especially with laminography, can induce damage in sensitive components (EEPROM)

- SQUID (Superconducting QUantum Interference Device) microscopy
  - Sensitivity allows for use of very low voltages; mostly non-destructive
Acoustic Microscopy

- Method for inspecting internal structures through the application of high frequency (>20 kHz) sound waves
- Requires immersion in water (acoustic signals reflected by air)
  - Allows for very accurate detection of voids and delaminations
- Options
  - Frequency
  - Transmission mode
  - Imaging
Acoustic Microscopy: Transducer Frequency

General rules:
- Ultra High Frequency (200+ MHz) for flip chips and wafers.
- High Frequency (50-75 MHz) for thin plastic packages. (110MHz-UHF) for flip chips.
- Low Frequency (15-30 MHz) for thicker plastic packages.

High frequency
Short focus
1. Higher resolution
2. Shorter focal lengths
3. Less penetration
   (Thinner packages)

Low frequency
Long focus
1. Lower resolution
2. Longer focal lengths
3. Greater penetration
   (Thicker packages)
Acoustic Microscopy: Transmission Mode

Pulse-Echo: One Transducer
- Uses ultrasound reflected from the sample
- Can determine which interface is delaminated
- Requires scanning from both sides to inspect all interfaces
- Provides images with high degree of spatial detail
- Peak amplitude, time of flight (TOF), and phase inversion measurement

Through Transmission: Two Transducers
- Uses ultrasound transmitted through the sample
- One scan reveals delamination at all interfaces
- No way to determine which interface is delaminated
- Less spatial resolution than pulse-echo
- Commonly used to verify pulse-echo results
Acoustic Microscopy Imaging

Through transmission

Peak amplitude image of die top

Phase inversion image of die top

Peak amplitude image of die attach
Acoustic Microscopy

- Used when delamination or voiding is suspected
  - Electrical shorting within the package (delamination, electro-chemical migration)
  - Electrical opens (delamination, wire bond failure)
  - Insufficient thermal performance detected (i.e. die attach)

- Some value for ceramic BGAs
  - Attenuation due to multiple interfaces prevents imaging of interconnects under PBGAs
X-Ray Microscopy

- Allows for internal inspection through the use of X-ray energy
- Latest innovations
  - Digital detectors
  - Laminography ('virtual' cross-sectioning)
    - 3D reconstruction
  - Nanofocus resolution
  - Oblique viewing
X-Ray Microscopy

- Digital detector
  - Provides greater contrast through wider range of grayscale (elemental differentiation)
  - Prerequisite for 3-D imaging

- Laminography
  - Provides X-ray sectional images and slice in any direction as well as three-dimensional visualizations of the specimen

- Types of laminography
  - Agilent 5DX
    - Best setup for inline inspection; moderate FA capabilities
  - Everyone else (computed tomography)
    - Allows for ‘virtual cross sectioning’ and 3-D reconstruction
    - Requires rotation of the sample (limited sizing) and extensive exposure time

- Resolution
  - Sub-micron

- Oblique viewing
  - Increases capability of 2-D viewing
  - 60 to 80 degree capability
X-Ray Inspection

- Inspect for:
  - Extra wire bonds
  - Wrong configuration of bond pads
  - Larger die than expected
  - Extra heat capacity (large paddle)
X-Ray Fluorescence Spectroscopy

- X-ray emission signature from x-ray source
- Portable models now available
- Crystallographic analysis of solid samples
X-Ray Fluorescence (XRF) Analysis

- X-ray fluorescence widely used to determine the elemental composition of the components and to determine the lead content for compliance to the RoHS directive.
- A new use for XRF to compare a known good component to a suspect component by comparing the elements of the leads as well as the packaging.
- Software developed to compare the two in order to assist in authenticity verification.
Scanning Electron Microscopy

- Sample rastered with an electron beam
- Emitted electrons sorted by delay and quantity
Scanning Electron Microscopy

Secondary electron detection yields topographic information

Backscattered electron detection also used for topography and elemental analysis
Energy Dispersive X-Ray Spectroscopy (EDS)

- Used with SEM
- X-ray emission signature from electron source
- Elemental analysis of solid samples
- Identification based on multiple emission lines (K, L, M)
- Can’t detect light elements: H, He, Li, Be
- Emission from subsurface “tear drop”

EDS scan of elemental copper

Monte Carlo simulation of Si K-α X-rays in an SiO2 matrix at 5 keV (Vanderlinde, 2004)
Circuit activation tracking

- Using SQUID or Infrared to identify the active parts of an IC
  - Send test signal through IC that selectively activates one region
  - Monitor where current is flowing
  - Identify any current activity in unexpected regions
Current monitoring

- SQUID and IR
- Allows identification where currents are on an IC or assembly
SQUID Microscopy: Superconducting Quantum Interference Device

- Current flow in devices produce a magnetic field
  - SQUID uses a highly sensitive magnetic detector (superconductor) to resolve these fields
  - Magnetic field image is converted to a current density image, allowing for fault location

- Resolution
  - 500 nA, 300 nm
  - Dependent on working distance (requires a flat sample)
SQUID Microscopy

- Critical technology for detecting package level electrical shorts
  - Much more rapid failure site resolution
  - Absolute confirmation of shorting path
  - Thermal imaging induces damage
SQUID Microscopy

- Extremely effective in locating failure site
Current Monitoring: Infrared Imaging

- Thermography is the use of an infrared imaging and measurement camera to "see" and measure thermal energy emitted from an object.
  - Provides precise non-contact temperature measurement capabilities.
  - Spectral range can be broken into one of four ranges, near IR: 0.75-3 microns, middle IR: 3-6 microns, far IR: 6-15 microns, and extreme IR: 15-30 microns.

- Important parameters include measurement temperature range, spectral range, accuracy, resolution, and steady state vs. real-time
  - Resolution for PCBA: 15 microns
  - Resolution on-die: 1 micron

- Excellent for:
  - Electrical shorts
  - Power components
Infra-Red Thermal Evaluation

Thermal Anomalies Detected

- Q16 producing heat when is it supposed to be in an off state - sneak circuit detected
- D11 detected a hot spot that exceeded thermal limit

Resulted in overheating nearby capacitors
Decapsulation

- Decapsulation is a very valuable tool for determining authenticity of difficult parts.
  - After performing all of the simple non destructive tests, the part may be opened and the die can be verified.
  - This does not guarantee all of the parts in the lot are the same, but it is a useful tool and is typically cheaper than electrical testing.
Cross-Sectioning

- **Standard method for destructive subsurface evaluation**
  - Used to isolate single IC layers for defect inspection
  - Top surface optical/SEM images can be correlated with top or bottom surface thermal/electrical/optical images (see subsequent techniques)
  - Special fixtures and CMP methods used for maintaining parallelism

- **Method:**
  - Cleaving/sawing to approximate area of interest
  - Potting in epoxy resins to aid polishing
  - Polishing medium dependent upon materials: typically diamond, SiC, or alumina suspensions & embedded polishing cloths
  - Coarse to fine (600 grit to 0.05 um) grinding sequence to eliminate damage from previous step
  - Final etch often used for microstructural relief
  - Optical/electron microscopy techniques used for inspection thereafter
Decapsulation and Cross Sectioning

- Allows direct inspection of circuits and identification of
  - Extra circuitry
  - Extra layers
  - Extra interconnects
Examples of Device Level Countermeasures

- Encryption on a chip
  - Often cited as one of the answers to cybersecurity woes
  - Difficult for small components to handle
  - Intel announced it has *come up with a process* that would allow the random-number generator, which is the basis for encryption, to be made with the same semiconducting material and at the same feature size now used for modern processors. The generators would also be all digital, rather than the current generation of hard-to-handle analog components.

- Smart Marking
  - INK CONTAINING DNA OR OTHER BIOLOGIC MARKER FOR PREVENTION OF COUNTERFEITING AND PRODUCT DIVERSION PERCEPTIBLE WITH INFRARED LIGHT

- RF tagging
  - Package Authentication - This method makes it extremely difficult to counterfeit the data on RFID tags
  - Data acts as an electronic security marker to automatically authenticate genuine product packaging.

- Shipment tracking
Manufacturers Countermeasures

- Complex markings on the package
- Ultra-violet ink in package marking
- Symbols or identifiers etched in the die
Countermeasures (cont.)

- Latest technique involves etch depth analysis
- Use of digital light processing (DLP) to rapidly scan surfaces for highly accurate depth measurements
- Compare to either manufacturer’s spec or known good part
Avoiding Counterfeits

- Custom fabrication ($$$$)
- Lifetime buy ($$-$$$$
- Modernize frequently ($$$$$$$$$$$$$$)$$
- Screen every incoming component ($$
- Screen outgoing components ($-$$$)
- Buy from original sources – and verify ($)
Mitigating Effects of Counterfeits

- Full performance screen
  - Test to or beyond spec
- Test should detect fraudulent parts
  - I.e., empty packages or wrong functionality
  - Factory-failed parts
- Competitors parts may prove to work
- Will not detect parts with latent defects or those with additional circuitry
Prevention

- Comprehensive audit of the distributor based on their quality system
- Risk assessment to the program
- Development of an inspection / test plan
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
Contact Information

- **Questions:**
  - Contact Tom O’Connor, toconnor@dfrsolutions.com
  - 301-474-0607
  - askdfr@dfrsolutions.com
  - www.dfrsolutions.com

- Connect with me in LinkedIn as well!
- Join LinkedIn Counter Counterfeit Group