Limitations of Product Inspection as an Authentication Method

Diganta Das, PhD

Center for Advanced Life Cycle Engineering (CALCE)

University of Maryland, College Park, MD, USA

diganta@umd.edu (www.calce.umd.edu)

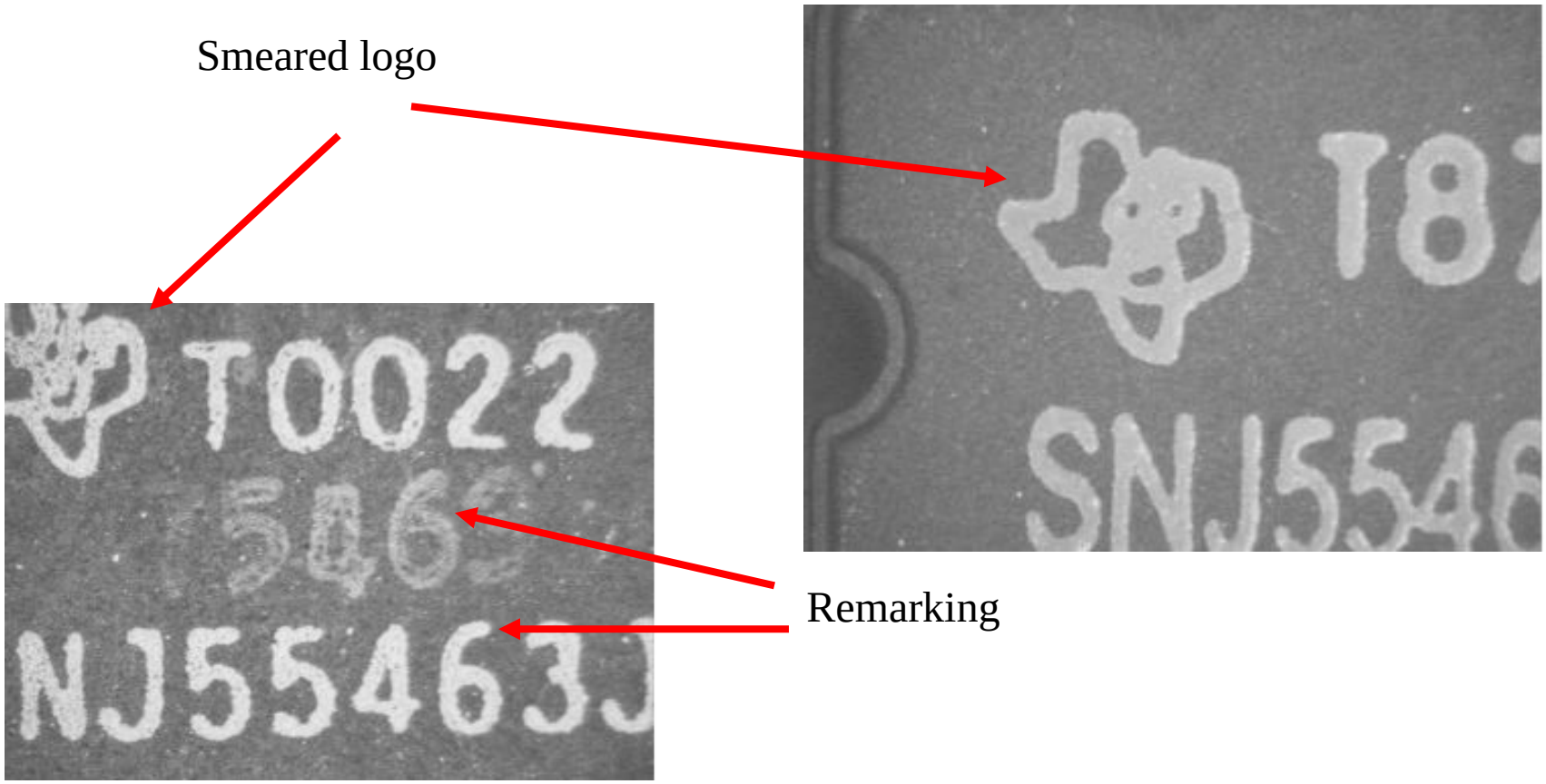
NIST Product Authentication Information Management Workshop
February 17-18, 2009

What is a Counterfeit Electronic Part?

- A counterfeit electronic part is one whose identity has been deliberately misrepresented.
- Identity of an electronic part includes:
  - Manufacturer,
  - Part number,
  - Date and lot code,
  - Reliability level,
  - Inspection/Testing,
  - Documentation.

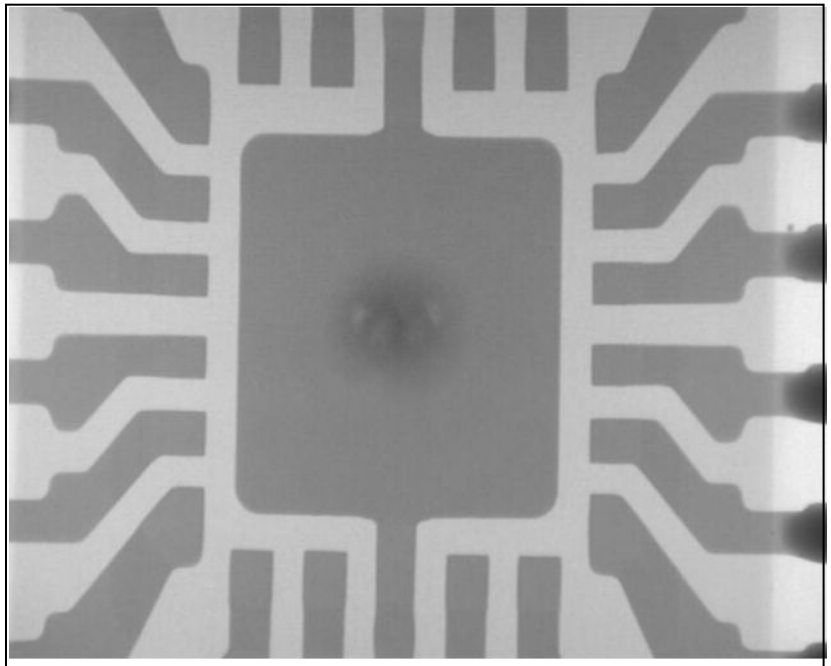
Chatterjee, K. and Das, D., "Semiconductor Manufacturers' Efforts to Improve Trust in the Electronic Part Supply Chain", IEEE Transactions on Components and Packaging Technology, Vol. 30, No. 3, pp. 547 – 549, September 2007.

Evidence of a Part Being Counterfeit may be External to the Packaging and Easy to Find

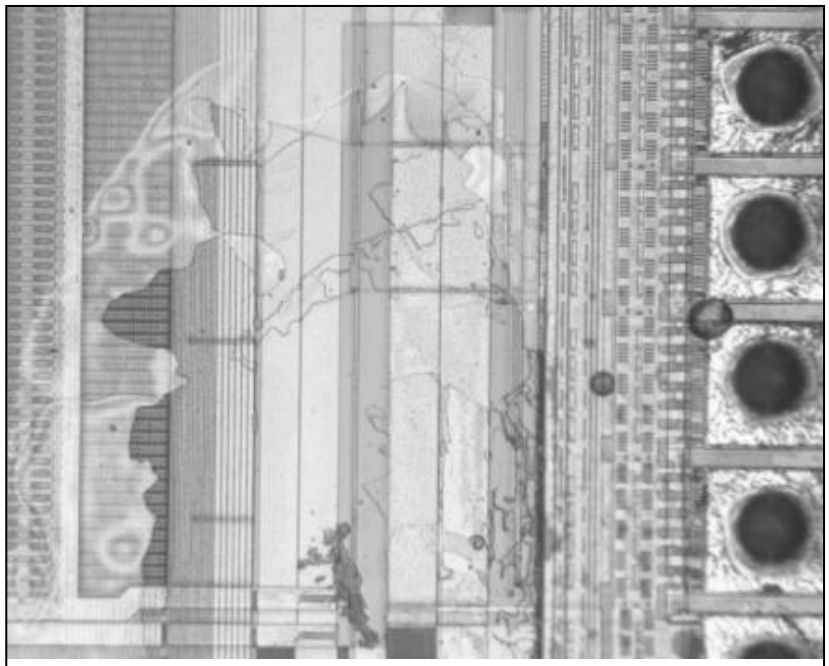


Izzo, J.M., "Counterfeit Risk Mitigation Process for Non-franchised Distributors", CALCE Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts, September 9, 2008.

Or They May be Internal and Require Internal Package Evaluation to Detect



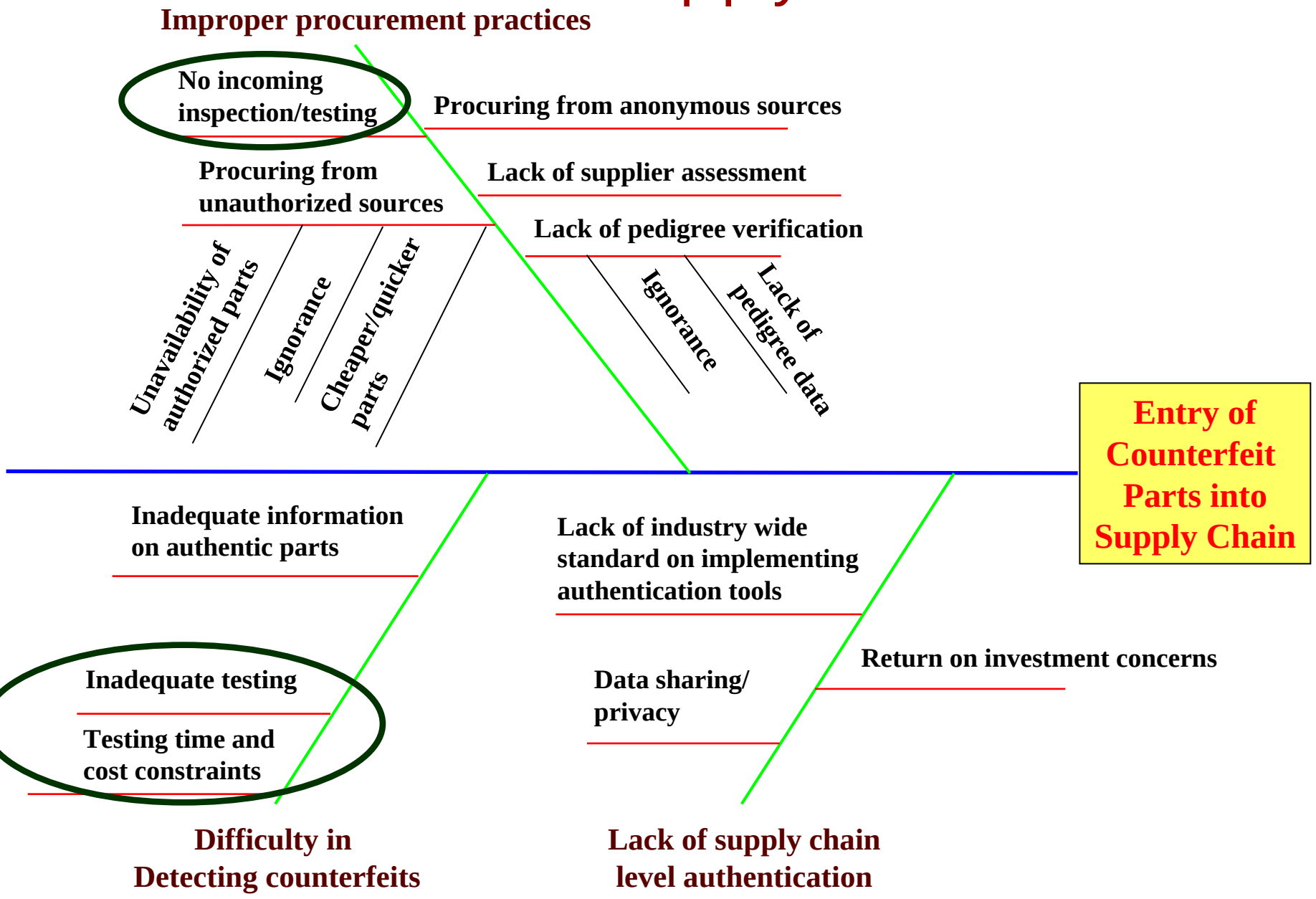
No die[1]



Passivation layer damage[2]

[1]Izzo, J.M., "Counterfeit Risk Mitigation Process for Non-franchised Distributors", CALCE Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts, September 9, 2008.
[2]Gibbs, D., et. al., "Laboratory Tools and Methods for Detection of Counterfeit Components", CALCE Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts, September 10, 2008.

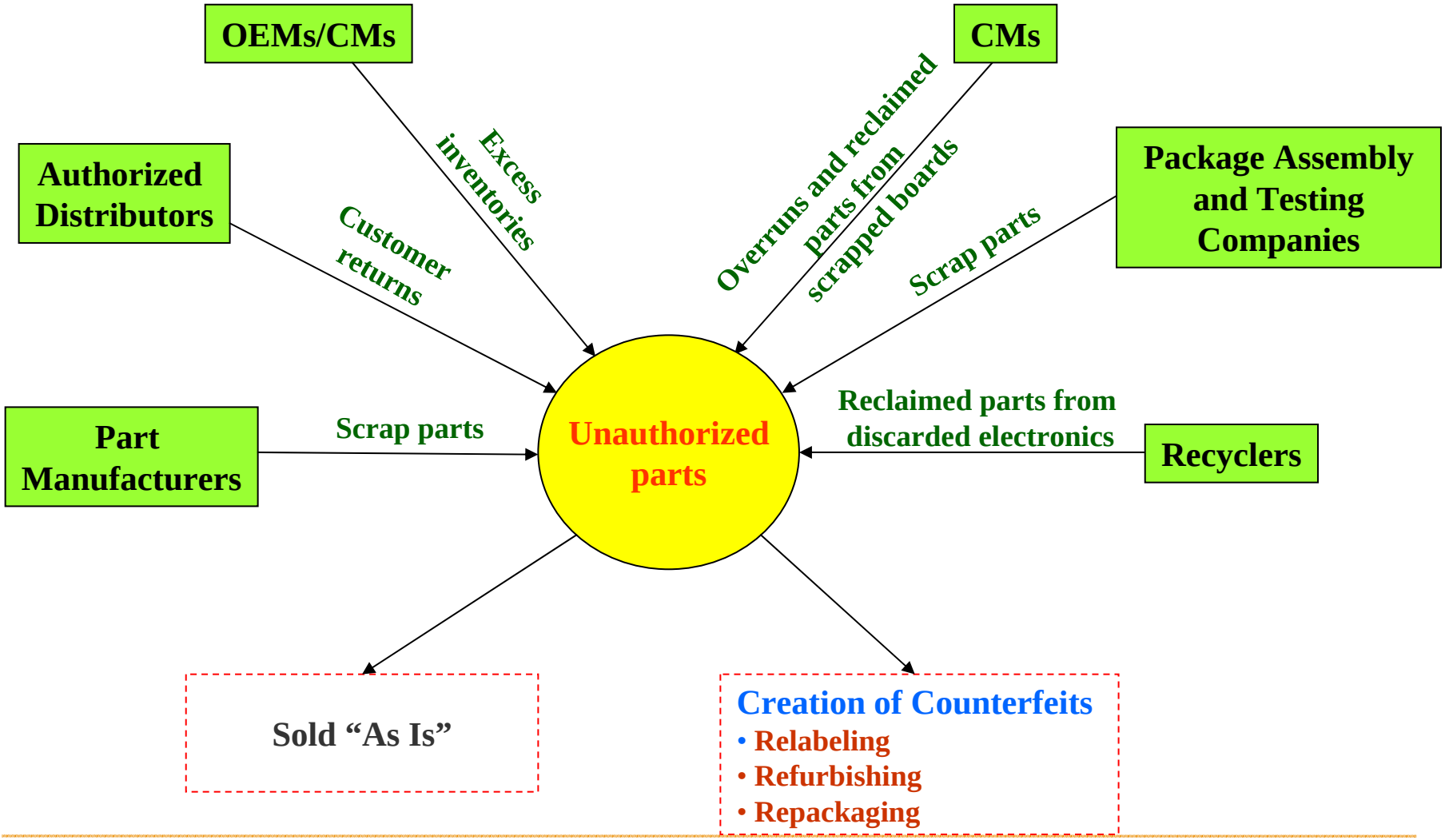
What Allows the Entry of Counterfeit Parts into Supply Chain



Methods of Prevention of Entry of Counterfeit Parts into the Supply Chain

- Supply chain management (proper procurement policies)
- **Supply chain level authentication**
  - **Traceability verification using tools such as serialization codes, tags/taggants**
  - **Counterfeit risk detection (through inspection/testing/characterization)**
- Law enforcement and government policies

Possible Sources of Parts Used to Create Counterfeits



There is Risk Even When Unauthorized Parts are Sold "As Is"

Types of parts	Sources and example attributes
Excess inventories	**Sources:** OEMs, Contract manufacturers **Attributes:** handling, packaging, and storage related damage; defects due to aging.
Scrapped parts	**Sources:** part manufacturers, testing companies, contract manufacturers **Attributes:** internal quality problems such as missing die or bond wires; die contamination; part termination damage, EOS/ESD damage.
Reclaimed parts	**Source:** recyclers **Attributes:** damaged terminations and body; inherent defects induced during reclamation.

Creation of Counterfeits: Relabeling

➢ Definition:

Relabeling is the process of modifying or altering the markings (e.g., part number, date code) on a part to make it appear as a different part.

➢ Example anomalies and defects:

- Marking irregularities (e.g., invalid date code, spelling errors, older marking showing through)
- Poor quality marking material
- Filled – in, unclean, or missing mold cavities
- Discrepancies between die and package
- Surface texture anomalies (linear scratches)

➢ Example of processes used:

- Erasing the original marking by methods such as black topping or sandblasting and applying a new marking using ink or laser to create a different part.
- Sandblasting is the process of smoothing, shaping, or cleaning the top part surface by forcing solid particles across that surface at high speeds.
- Blacktopping may be performed after sandblasting to cover the old marking on top part surface with a new layer material.

Creation of Counterfeits: Refurbishing

➢ Definition:

Refurbishing is a process in which parts are renovated in an effort to restore them to a like new condition in appearance.

➢ Example anomalies and defects:

- Improperly aligned or bridged terminations
- Internal defects such as interfacial delamination, metallization deformation, and cracks in passivation layer
- Differences in termination plating materials with original part

➢ Examples of processes used:

- Realignment (e.g., straightening) of leads often carried out on reclaimed or scrapped parts that have bent or non-aligned leads
- Refinishing processes such as solder dipping and reballing
  - Solder dipping is used to change the lead finish and improve or restore the solderability of the parts, and can act as the primary finish for the terminations.
  - Reballing is carried out on ball grid array (BGA) parts to replace damaged balls or to change the termination finish.

Creation of Counterfeits: Repackaging

➢ Definition:

Repackaging is the process of altering the packaging of a part to make it appear to be a different part with a different pin count and package type.

➢ Example of processes used:

- Recovery of die (by removing the original packaging) and molding the die into the desired package type
- Packaging procedures, tools, and materials used for repackaging the die lead to defects or degradations in the repackaged parts

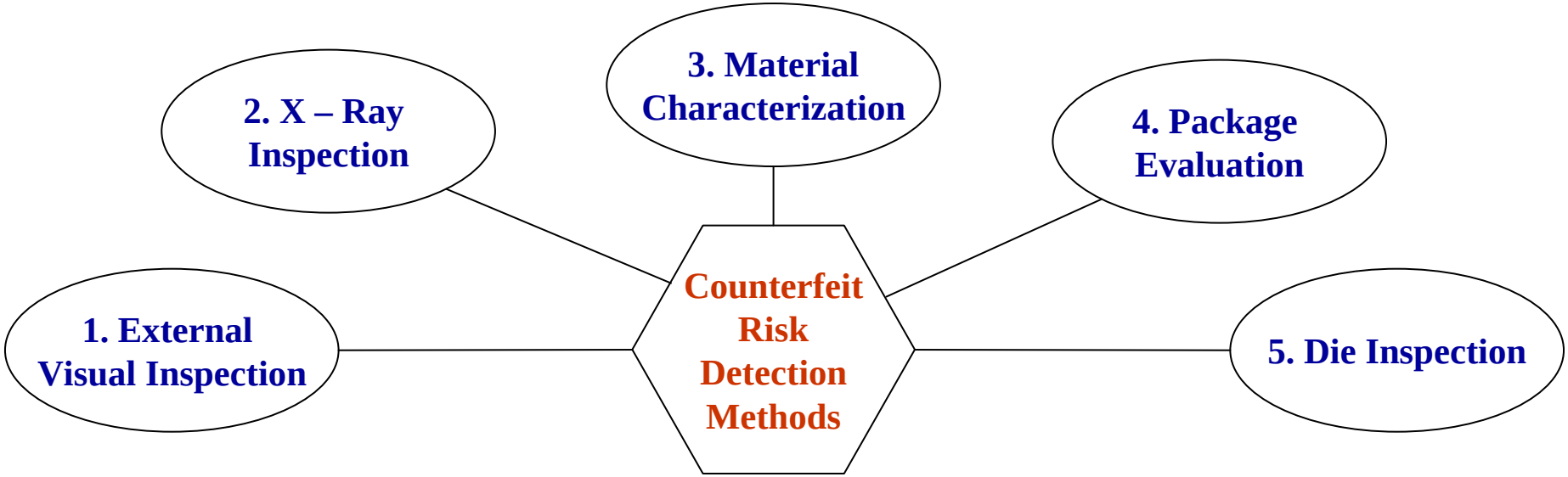
➢ Example anomalies and defects:

- Missing bond wires, missing die, bond wire misalignment, or poor die paddle construction
- Discrepancies between die and package
- Marking irregularities such as spelling errors, discrepancies in part number, or an incorrect logo
- Different mold compound or die package materials

Summary: Example Anomalies and Defects

Processes of counterfeiting	Example anomalies and defects
Relabeling	Marking irregularities, poor quality marking, filled-in, unclean, or missing mold cavities, discrepancies between die and package, Surface texture anomalies
Refurbishing	Improperly aligned or bridged terminations; internal defects such as interfacial delamination and cracked passivation layer induced during processes such as solder dipping, reballing, and realignment of terminations; differences in termination plating material with original part
Repackaging	Discrepancies between die and package; workmanship issues such as missing bond wires or poor die paddle construction; internal defects such as moisture induced interfacial delamination; poor materials used

Counterfeit Risk Detection Methods



Individual detection method outcomes:

- **Positive:** high probability (large number of anomalies and defects present) of part being counterfeit. May proceed to next method to confirm the outcome or exit at the current method and take necessary steps (e.g., reject parts, report to GIDEP).
- **Uncertain:** low probability (small number of anomalies, may be due to manufacturing changes or poor handling) of part being counterfeit. Proceed to next method (to reduce uncertainty level) depending on application risk tolerance level or exit at current method.
- **Negative:** tolerable probability (no anomalies and defects present) of part being counterfeit. Proceed to next method. Accept parts based on outcomes of all methods.

External Visual Inspection

- **Definition:**
  External visual inspection is a process of verifying the attributes of parts such as package and part markings (part number, date code, country of origin marking), part termination quality, and surface quality.

- **Example anomalies or defects to inspect:**
  Spelling errors in part markings or labels; validity of logo, part number, lot code, date code, and/or Pb-free marking; marking technique; quality of marking; mold cavities; straightness, coplanarity, scratches, bridging or other defects in terminations; surface texture

- **Severity:**
  Non – destructive, may induce handling related damage such as ESD if precautions are not taken

- **Tools/Equipment:**
  Optical microscope, solvent for marking permanency tests, part datasheet information

- **Industry standards:**
  JESD22 – B(101, 107A, 108), MIL – STD – 883 M(2009, 2015), IDEA – STD – 1010A, PEM – INST – 001

- ✓ **Note:**
  External visual inspection should not be used as a standalone counterfeit detection process.

Limitations of Using Visual Inspection Alone for Detecting Counterfeits

Types of counterfeit parts	Examples of limitations of visual inspection
Relabeled	Fails if markings on counterfeit parts are good quality Need access to datasheets or support from original manufacturer
Refurbished	Cannot verify RoHS compliance claims Cannot detect termination plating discrepancies with original parts Cannot detect internal failure mechanisms induced during the refurbishing processes such as interfacial delamination
Repackaged	Cannot detect internal discrepancies such as bond wire misalignment or missing bond wires, missing or damaged die Cannot detect die and package marking mismatches

Visual inspection may also fail to detect anomalies and defects in "As Is" parts such as excess inventories, reclaimed, and scrapped parts that are commonly used to create counterfeits. For example, scrapped parts with original manufacturer's markings may have hidden discrepancies such as missing die or bond wires that cannot be detected by visual inspection.

X – Ray Inspection

- **Definition:**
  X-ray inspection is a process used to verify the internal attributes of parts such as dimension, alignment, and other construction and workmanship issues.

- **Example anomalies or defects to inspect:**
  Improper die size; bond wire misalignment; anomalies such as missing or damaged bond wires, missing die, presence of foreign particles.

- **Industry standards:**
  MIL – STD – 2012.7, ESCC 20900,
  PEM – INST – 001.

- **Severity:**
  Non – destructive, may induce handling related damage such as ESD if precautions are not taken.

- **Tools/Equipment:**
  X-ray machine, X-ray images of an authentic part.

- ✓ **Note:**
  Different die size does not necessarily indicate a counterfeit since manufacturers sometimes will institute a process change on a particular product.

Material Characterization

- **Definition:**
  This is a process used to evaluate the material composition of the part by comparing with an authentic part.

- **Example anomalies or defects to inspect:**
  Discrepancies in termination (e.g., leads or balls) plating materials, molding compound materials, leadframe and die attach materials, coatings, laminate materials, dielectric materials (e.g., for capacitors).

- **Industry standards:**
  PEM – INST – 001, MIL – STD – 1580B.

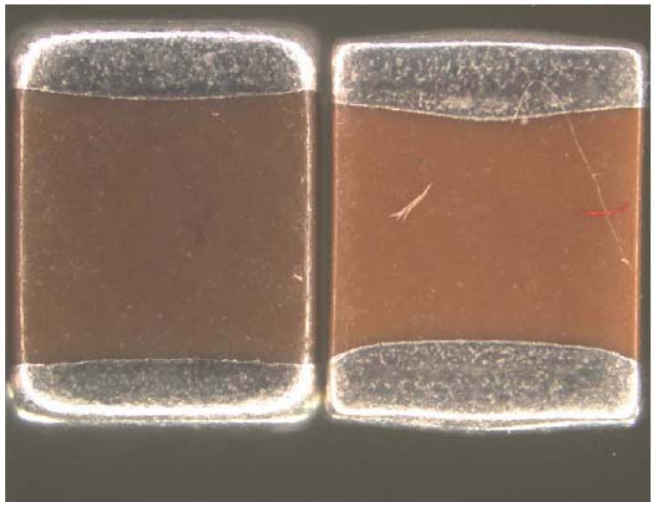
- **Severity:**
  May be destructive or non – destructive depending on the type of equipment used, may induce handling related damage such as ESD if precautions are not taken.

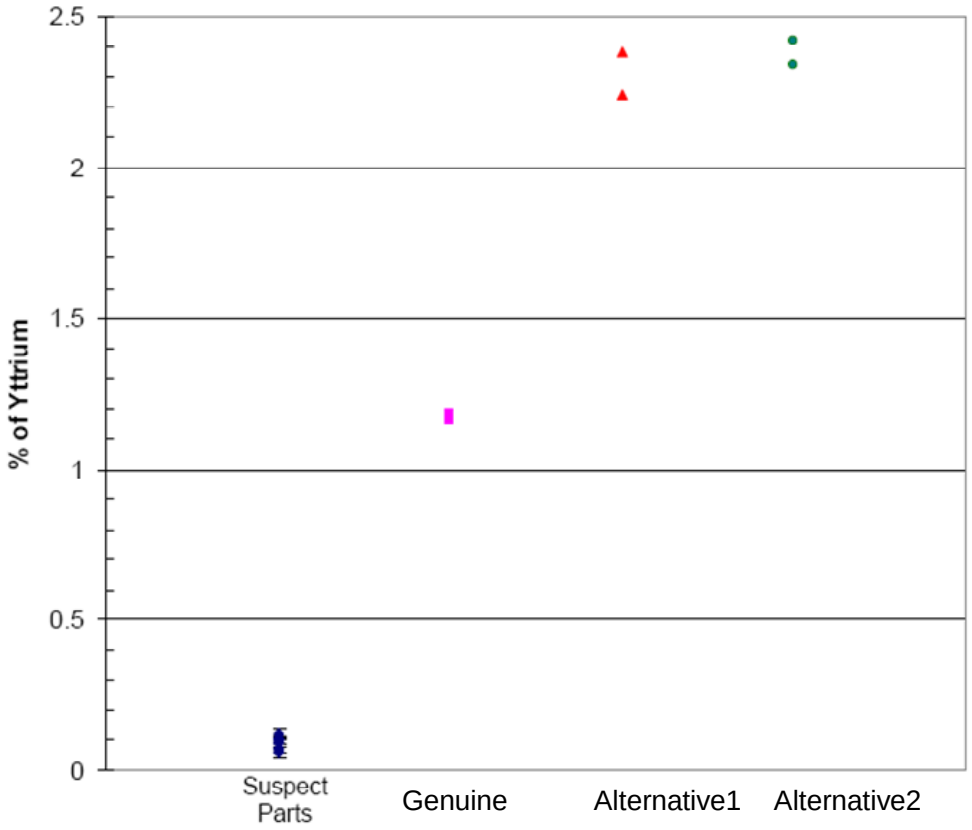
- **Tools/Equipment:**
  Commonly used equipments are X – ray fluorescence (XRF), scanning electron microscope (SEM), electron dispersive spectroscope (EDS), differential scanning calorimeter (DSC), and thermo-mechanical analyzer (TMA).

- ✓ **Note:**
  Information on original part materials may be needed.

Counterfeit Capacitors: Detection Using XRF

CALCE performed material analysis of four different multilayer ceramic capacitors (MLCC) using XRF instrument, in order to identify differences between three parts known to be genuine and a part that had capacitance stability problems.





Plot showing variation in amounts of yttrium in dielectric ceramic materials among various parts

Package Evaluation

- **Definition:**
  This is a process used to identify hidden internal defects or degradations in electronic parts, which lead to failure mechanisms that ultimately result in failures during assembly or field use.

- **Example anomalies or defects to inspect:**
  Delamination, voids and cracks in the molding compound, leadframe, and die – attach material; ionic contaminants in the package.

- **Industry standards:**
  PEM – INST – 001, GEIA – STD – 0006, J – STD – 035, MIL – STD – 2030, IPC – TM – 650 (2.3.28), J – STD – 020C.

- **Severity:**
  May be destructive or non – destructive, depending on type of test. May induce handling related damage such as ESD if precautions are not taken.

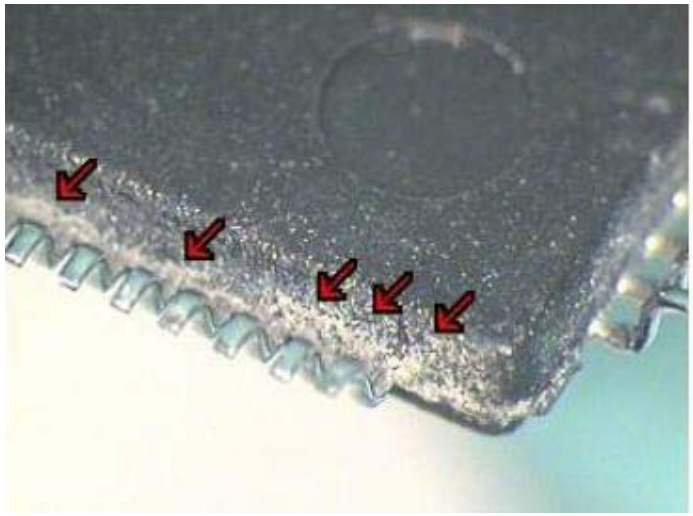
- **Tools/Equipment:**
  C – SCAN, scanning laser acoustic microscopy (SLAM), or C – mode scanning acoustic microscopy (C – SAM), Ion Chromatography.

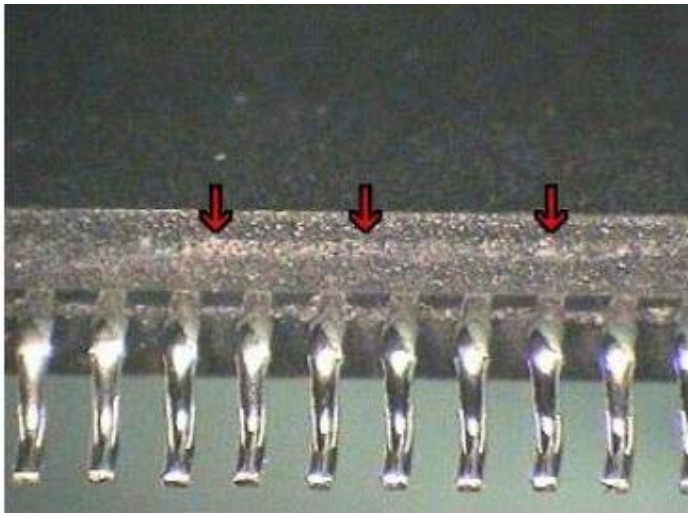
- ✓ **Note:**
  It may be necessary to perform evaluation after environmental exposure (e.g., thermal cycling or temperature, humidity, bias (THB) tests) to precipitate defects and make detection easier.

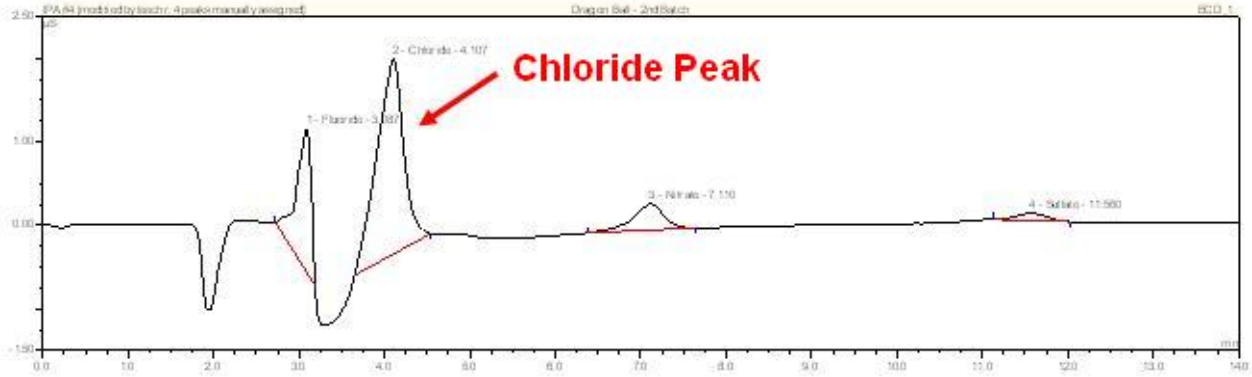
Need for Environmental Stressing

- Some of the processes such as solder dipping used in the counterfeit creation can lead to latent defects.
- Such defects may become apparent only after subjecting the parts to environmental exposure (e.g., thermal cycling, THB tests).
- The GEIA standard* qualification of solder dipped parts require package evaluation before and after environmental exposure of packages – similar methodology can be utilized for counterfeit part detection too.
- The types of exposure, post – exposure inspections and acceptance criteria or risk assignment criteria are to be based on the acceptable risk levels.

Ion Chromatography to Detect Hidden Defects







- White residue on component body
- High levels of chloride noted that are likely sourced from original tin/lead strip process

Gibbs, D., et. al., "Laboratory Tools and Methods for Detection of Counterfeit Components", CALCE Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts, September 10, 2008

Die Inspection

- **Definition:**
  This is a process used to verify the attributes of die (e.g., die marking) and internal defects.

- **Example anomalies or defects to inspect:**
  Discrepancies in the die and package markings (e.g., manufacturer, date code), metallization layer damage (due to EOS/ESD, corrosion), contamination, bond wire defects, and cracks in the passivation layer.

- **Severity:**
  Destructive.

- **Tools/Equipment:**
  Decapsulator (can also be carried out through manual etching), SEM, optical microscope.

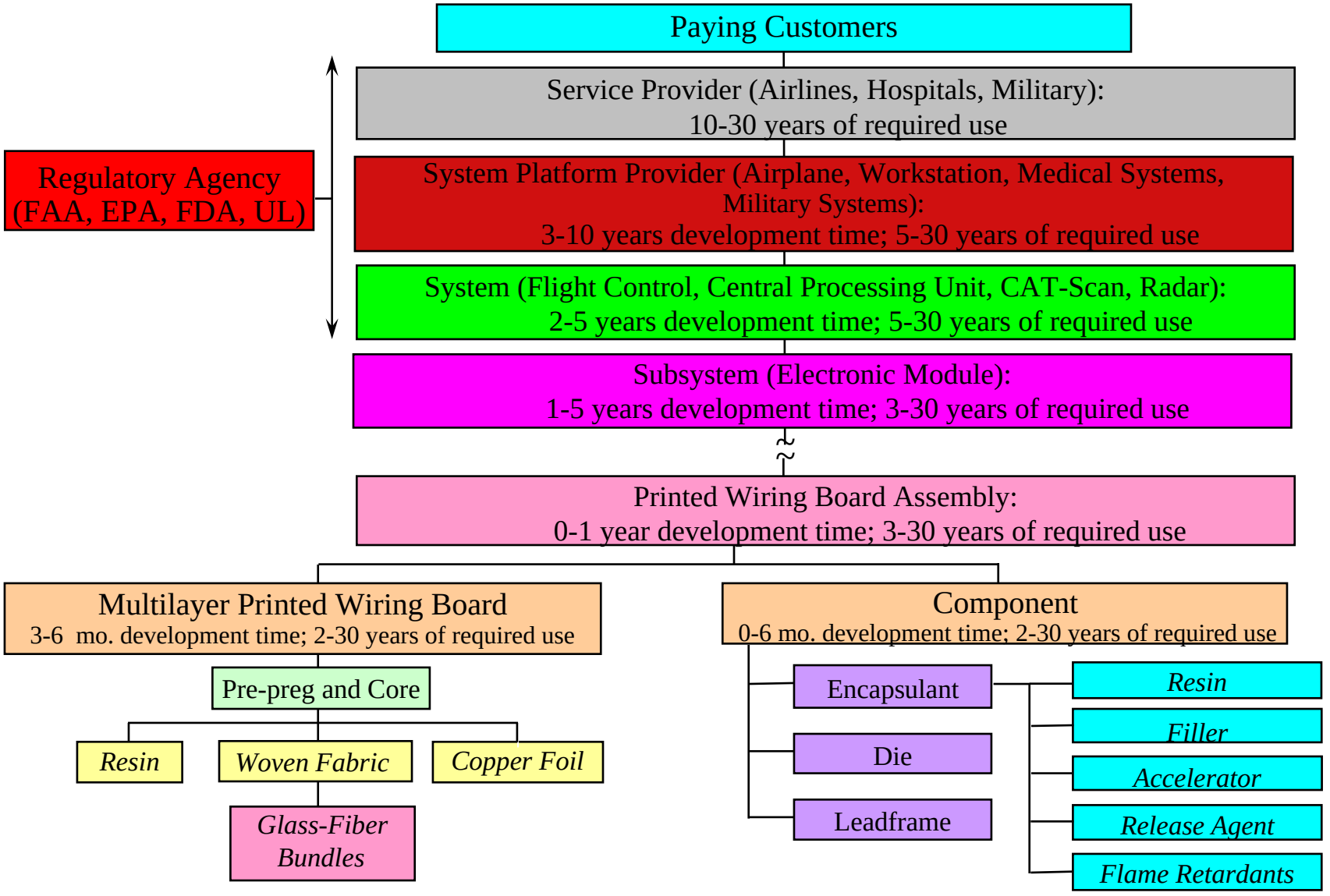
- **Industry standards:**
  PEM – INST – 001, ESCC 25300, MIL – STD – 2021, MIL – STD – 1580B.

✓ **Note:**
Information on original die markings and attributes needed. Performed only on few parts.

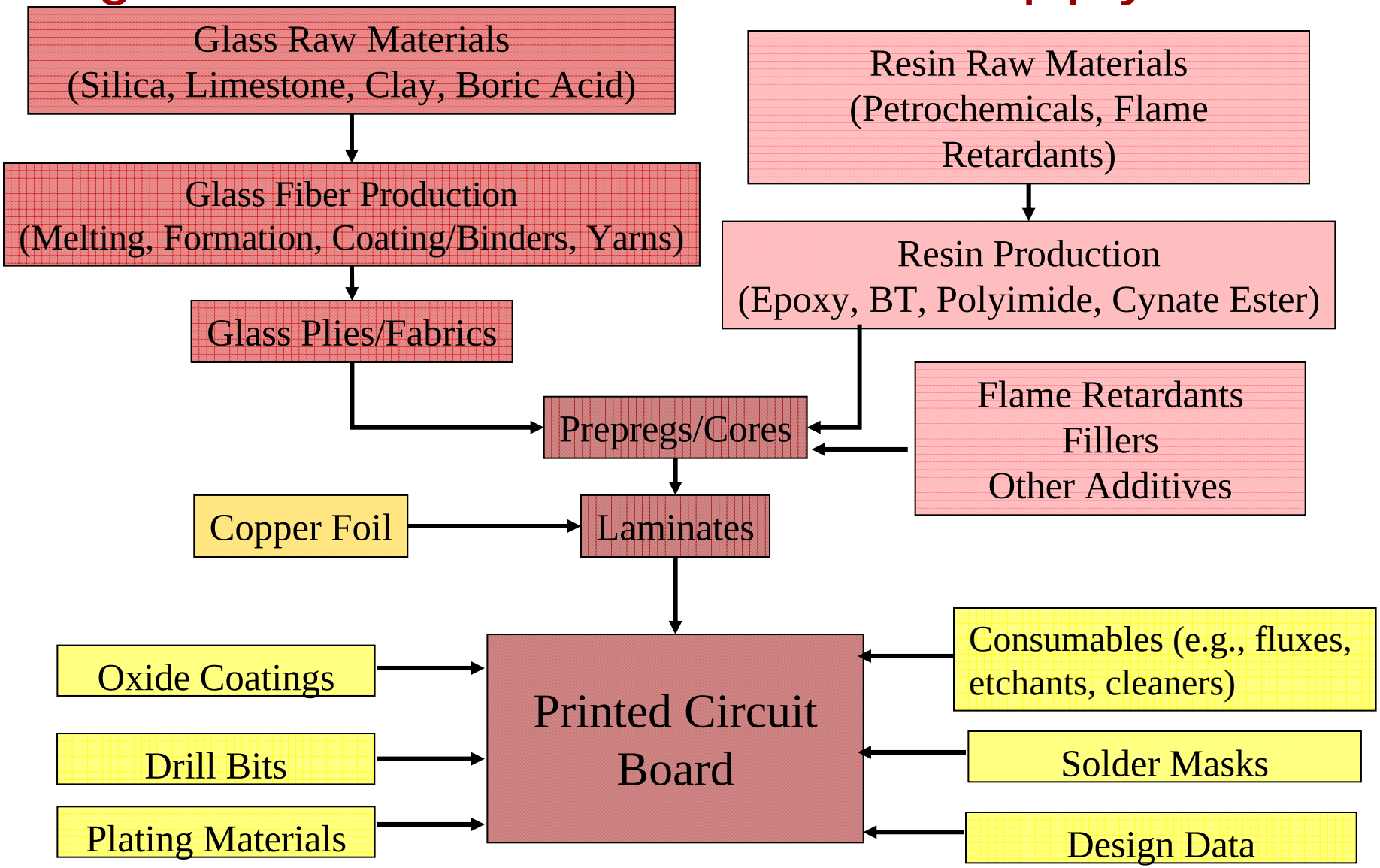
Recommendations

- In order to be effective, the counterfeit risk detection process needs to come to a conclusion within a relatively short period of time and hence a logistics plan of performing the evaluations needs to be in place since all the equipment and expertise may not reside in the same location.
- The attributes of the authentic parts (e.g., part number, date code on the part) should be known before initiating the detection process.
- Counterfeit risk detection process should be applied on actual production shipment and not on samples obtained separately prior to production shipment.
- Counterfeit part risk detection process can be utilized properly only when proper component engineering practices are followed, e.g., process changes initiated by original part manufacturers are tracked, maintained and used.
- Even after all these, inspection still is a reactive method.

Complex Electronic Systems Supply Chain



Organic Printed Circuit Board Supply Chain

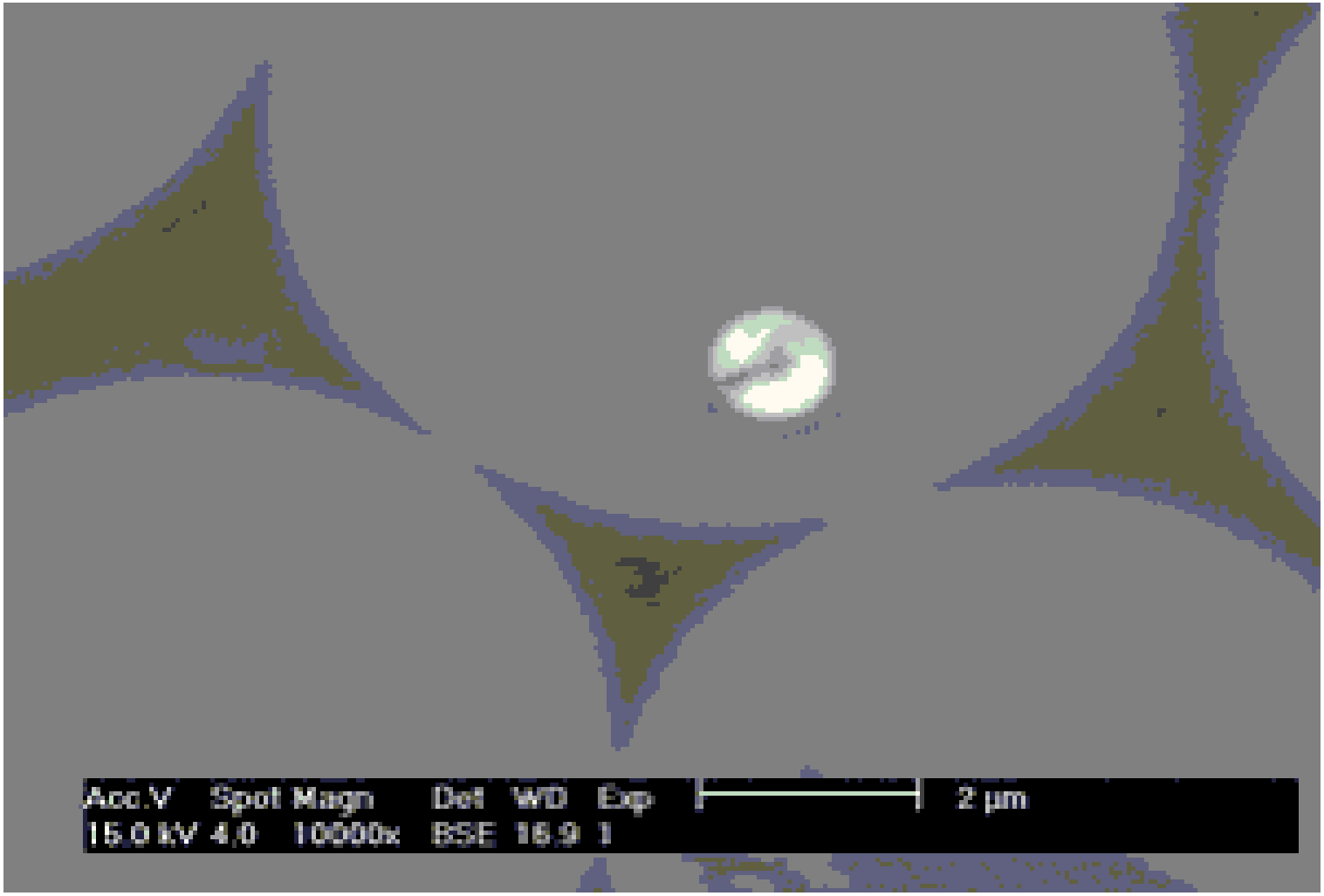


Hollow Fiber Problems: Nov. 16, 2005

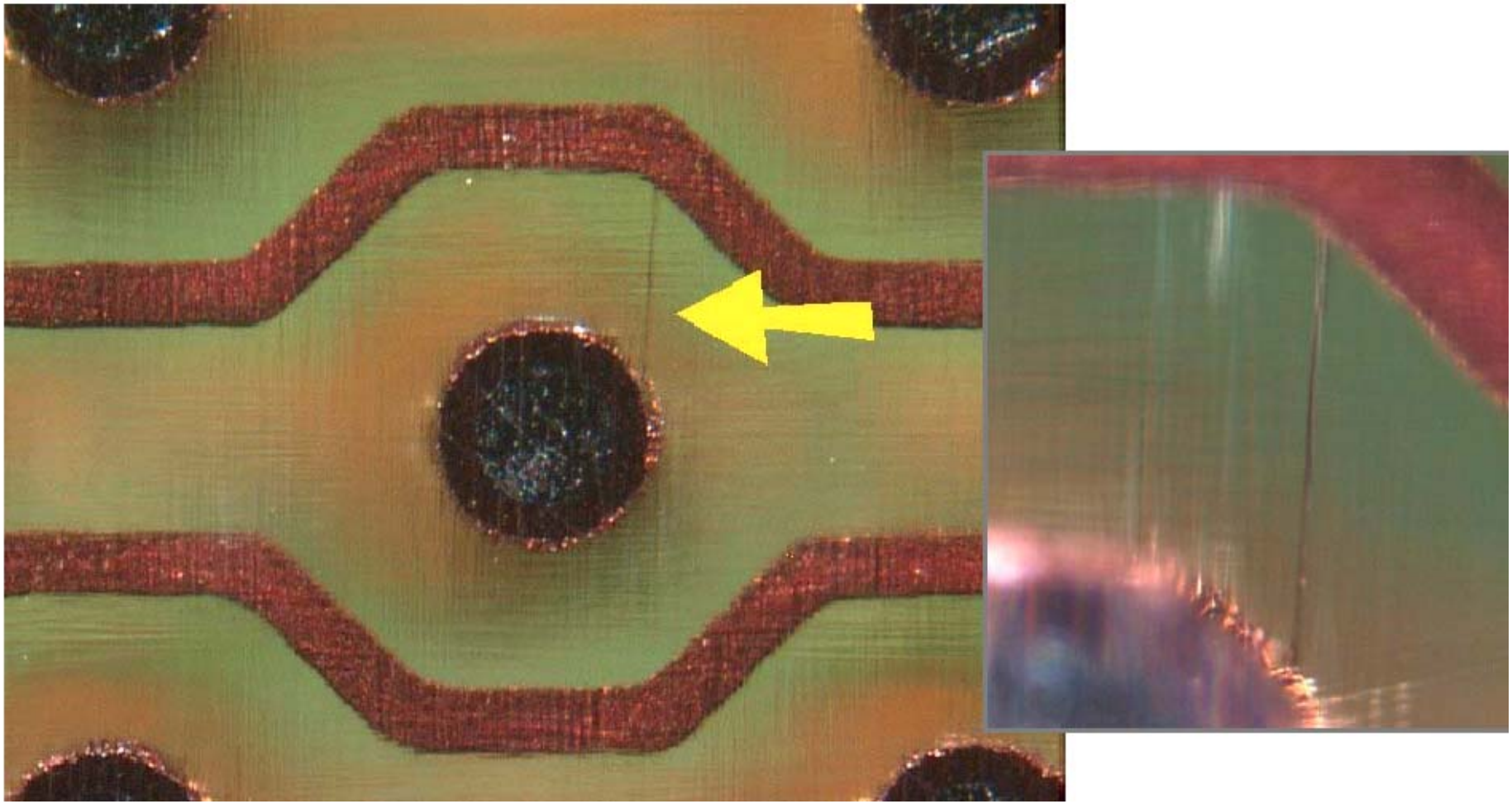
We have recently experienced two CAF (Conductive Anodic Filament) failures with one of our customers that we have been able to conclusively determine were caused by hollow glass filaments.

Scott M. Benedict
Global Supplier Quality Engineer
Polyclad Laminates

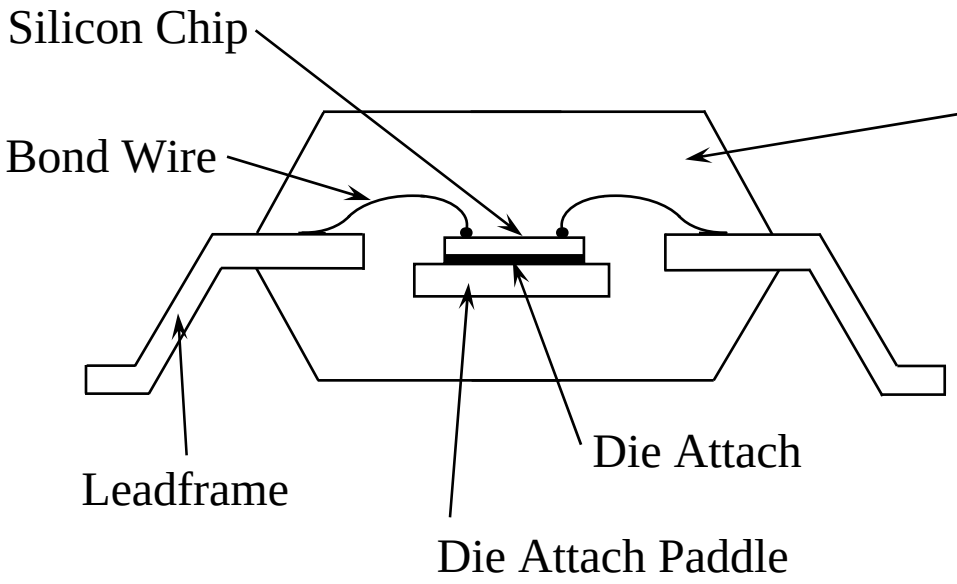
Hollow Fiber



CFF: 100v, Via to ½ Oz Line, Layer 5



Plastic Leadframe Package Construction



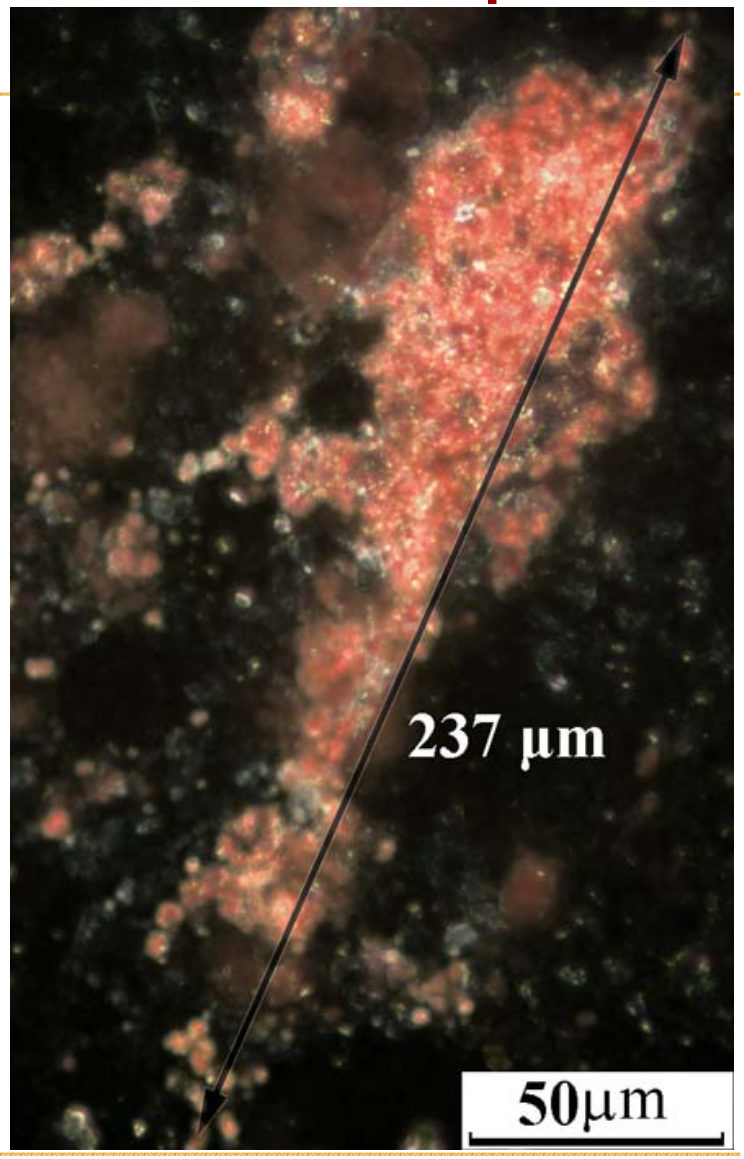
- Filler (65-90%)
- Epoxy resin matrix (10-20%)
- Crosslinker (5-10%)
- Stress relief agents (2-5%)
- Flame retardant (1-5%)
- Mold release agent (0.1-1%)
- Coloring agents (0.2-0.4%)
- Catalyst (0.2-0.3%)
- Coupling agent (< 0.2%)
- Ion trapping agents (< 0.2%)

Semiconductor Device Failure due to Red Phosphorus Flame Retardant

- Flammability of the mold compounds in encapsulated semiconductor devices, is a safety concern traditionally mitigated by adding bromine-based aromatic compounds
- Due to various environmental, health and reliability concerns, brominated flame-retardants (BFRs) are being discontinued
- A new "green" mold compound (EME-U series) was put into production by Sumitomo Bakelite in 1999. It contained red phosphorus as the flame retardant.
- Around 2000, companies started to observe electrical short circuit and leakage current failures. (Some ICs were even observed to burnt)
- This problem occurred in various types of products from different manufactures, for diverse applications.

Sumitomo EME-U Series Mold Compound

- What's different with the new mold compound?
  - Red phosphorus was used as flame retardant, to replace the commonly used brominated material which was considered environmental unfriendly.
- Red phosphorus flame retardant
  - A flame retardant is induced to protect the device against fire. For semiconductor devices, the mold compound must satisfy industry standard (UL-94V0).
  - Red phosphorus particles were coated with an aluminum hydroxide layer and a phenol resin layer, in order to stabilize the red phosphorus content. However, the coating appeared to have broken down.
  - Large particles of red phosphorus flame retardant were found in the molded packages.



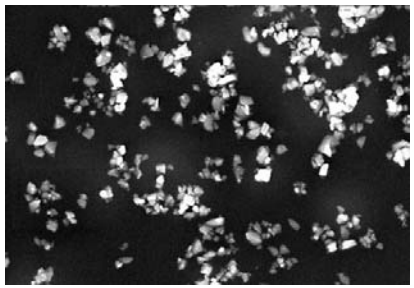
How Could This Happen?

- The parts were all screened and tested in accordance with industry practices
- The parts all passed the specified acceptance tests
- Were these tests not adequate to assure reliable performance?
- What should have been done differently to avoid these catastrophic failures?

These are cautionary tales for introducing material based authentication

Taggants Based Authentication

- Taggants is a covert tool for product authentication. Several different taggants are available.
- The taggants are used to create unique code that can serve as a unique fingerprint for a product.



Rare earth mineral based

Polymer based

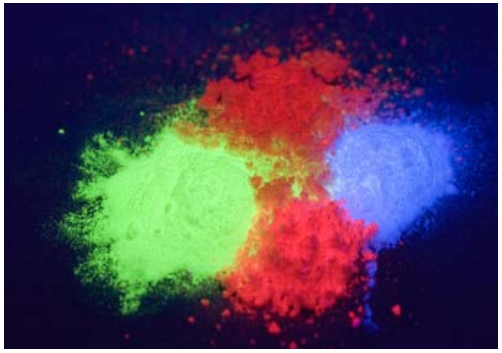
Example of Taggant: Covert Micro Tag

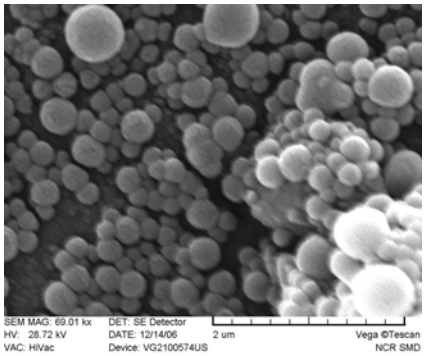
- Some authentication technology uses microscopic markers for integration into the manufacturing process at multiple layers– on the packaging, on the label, or in/on the product itself.
- The covert marker technology can be engineered to contain certain forensic capabilities to confirm if a product has been tampered with or exposed to particular environmental conditions.
- The markers can be constructed with materials which only respond to specific light wavelengths.

Gabrielle, P., "Product Surety, Security, Protection & Safety,"
CALCE Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts, September 10, 2008

Rare Earth Based Taggants

These taggants are sub-micron silica-based particles that are doped with one or more luminescent chemicals (rare earth ions, dyes, or quantum dots).





When exposed to a specific excitation frequency, these silica-based particles create a unique spectral response with sharp, narrow spectral peaks in the visible and/or infrared regions of the electro-magnetic spectrum.

Areas of Research and Implementation to Get Ready for the Future

- The next level of counterfeiting is at the material level which will not allow inspection of piece part for counterfeit detection
- Material level authentication tool implementation including research into manufacturability, quality, and reliability issues associated with the tools
- Identification of failure mechanisms that may be precipitated by inclusion of the authentication material
- Test methods development for evaluation of products for accelerating the failure mechanisms caused by these additions

Third International Symposium on Tin Whiskers

calce™

- June 23-24, 2009 at Technical University of Denmark, Lyngby, Denmark
- Please provide an abstract (within 300 words) on any relevant topics to Dr. Michael Osterman via email to osterman@calce.umd.edu or upload by clicking on the "upload abstract" tab above no later than March 27, 2009
- This symposium will cover case histories, theories of tin whisker growth, experiments and results, risk evaluation methods, and risk mitigation strategies. Attendees will be able to learn about the current state of knowledge regarding tin whisker growth, risk, and mitigation strategies, enabling the development of improved and effective qualification and mitigation procedures.
- Registration will open in March on the SMTA web site

Symposium on Avoiding, Detecting, and Preventing Counterfeit Electronic Parts

calce™

- June 25-26, 2009 at Technical University of Denmark, Lyngby, Denmark
- If you are interested in presenting, submit abstract of proposed talk to Dr. Diganta Das via email to diganta@umd.edu by March 31, 2000 or at SMTA web site (http://www.smta.org/education/education.cfm#counterfeit)
- Topics of interest include:
  - Supply chain management tools to mitigate counterfeit part risks
  - Inspections tools and techniques for detecting counterfeit parts
  - Impact of counterfeit parts on the military and avionics industry
  - Sources of counterfeit parts
  - Authentication techniques for securing electronic part supply chain
- Registration will open in March on the SMTA web site

Workshop on Testing Lead-free Assemblies

- April 14, 2009 University of Maryland College Park, MD
- The ban on the use of lead in the majority of electronic products has raised a number of concern. In particular, the relevance and effectiveness of existing test procedures for lead-free assemblies. To address this issue, GEIA-STD-0005-3, Performance Testing for Aerospace and High Performance Electronic Interconnects Containing Pb-free Solder and Finishes was released June 2008. This workshop is intend to provide a forum to examine testing of lead-free assembles.
- Topics of interest include:
  - Lessons Learned in Lead-free testing
  - Performance data (mechanical, environmental, etc.) of lead-free solders
  - Critiques/comparisons of various test approaches/procedures
  - New/novel test methods
  - HALT/HASS
  - Environmental Stress Screening
  - Challenges in lead-free testing
  - New materials

CALCE and Buehler Offer Short-Course on Failure Analysis of Electronics

Tuesday, April 21 – Friday, April 24, 2009

Course Topics

1. Failure analysis techniques
   - Non-destructive analysis
   - Destructive analysis
   - Inspection and materials characterization
   - Other analytical techniques
2. Failure mechanisms of electronic products
3. Root cause analysis
4. Physics of failure

Course fee: $2500. For more information, please visit:

http://www.calce.umd.edu/facourse/spring2009

Bhanu Sood, (301) 405 3498