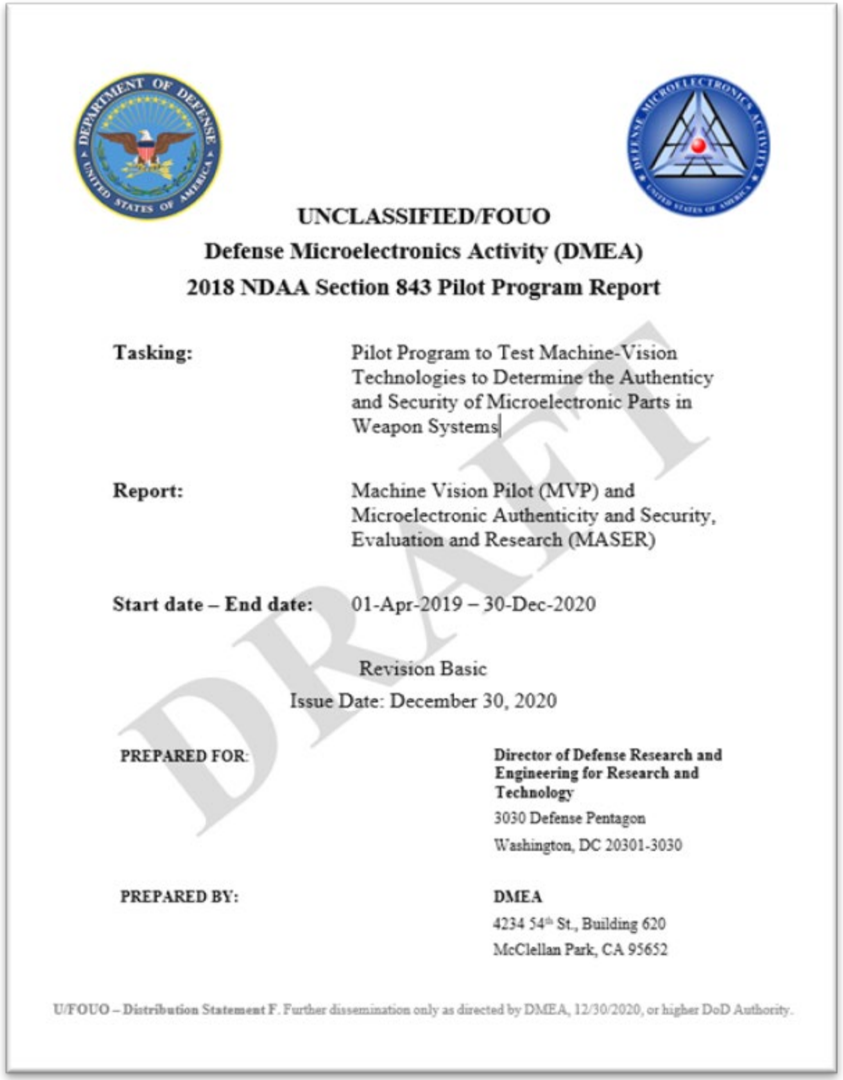
Counterfeit Detection using Side-channel and Machine-Vision Tools

Dr. Diganta Das (diganta@umd.edu)
Dr. Michael H. Azarian
Team: Devon Richman, Dr. Robert Utter, Jesse Hearn, Peter Kuffel
CALCE, Univ. of Maryland

2021 Components for Military and Space Electronics Conference

CALCE Concludes Machine Vision Pilot Study for DoD



UNCLASSIFIED/FOUO

Defense Microelectronics Activity (DMEA)

2018 NDAA Section 843 Pilot Program Report

Tasking: Pilot Program to Test Machine-Vision Technologies to Determine the Authenticy and Security of Microelectronic Parts in Weapon Systems

Report: Machine Vision Pilot (MVP) and Microelectronic Authenticity and Security, Evaluation and Research (MASER)

Start date – End date: 01-Apr-2019 – 30-Dec-2020

Revision Basic

Issue Date: December 30, 2020

PREPARED FOR:

Director of Defense Research and Engineering for Research and Technology
3030 Defense Pentagon
Washington, DC 20301-3030

PREPARED BY:

DMEA
4234 54th St., Building 620
McClellan Park, CA 95652

U/FOUO – Distribution Statement F. Further dissemination only as directed by DMEA, 12/30/2020, or higher DoD Authority.

- CALCE performed a 21 month study in 2019-20 for the Defense Microelectronics Activity (DMEA). The study included:
  - Review of emerging counterfeit detection systems and technologies, and comparison with SAE AS6171 standards-based testing, with a blind study of effectiveness with real counterfeits, including clones.
  - Review of existing legislation, standards, requirements, and policies (led by University of Maryland Carey School of Law)
- CALCE worked with ten technology organizations and SMT Corporation to assess the maturity of their technologies and their ability to detect counterfeit parts.
- The study provided a set of long and short term recommendations to the US DoD regarding technology adoption and procurement policies.

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.

Sood. B, Das. D, Pecht. M (2011): Screening for counterfeit electronic parts, Journal of Materials Science, Materials in Electronics 22:1511-1522
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.

Types of Counterfeits

- Counterfeit parts, based on AS6171, include:[1]
  - **Recycled:** Reclaimed/recovered then misrepresented as new.
  - **Remarked:** Part markings replaced with forged markings.
  - **Overproduced:** Authorized part from contracted facility fab cated ou contract.
  - **Out-of-Specification/Defective:** Identified nonconforming p ated as conforming.
  - **Provided with forged documentation:** Associated docum
  - **Cloned:** A reproduction of an authorized pa
  - **Tampered:** Modified for sabotage or malfunction.
- All counterfeits except for clones originate from an OCM part.
- Conventional counterfeits refer to all except cloned and tampered parts.

Conventional

Advanced Counterfeits

[1] SAE AS6171 Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts, 2016.

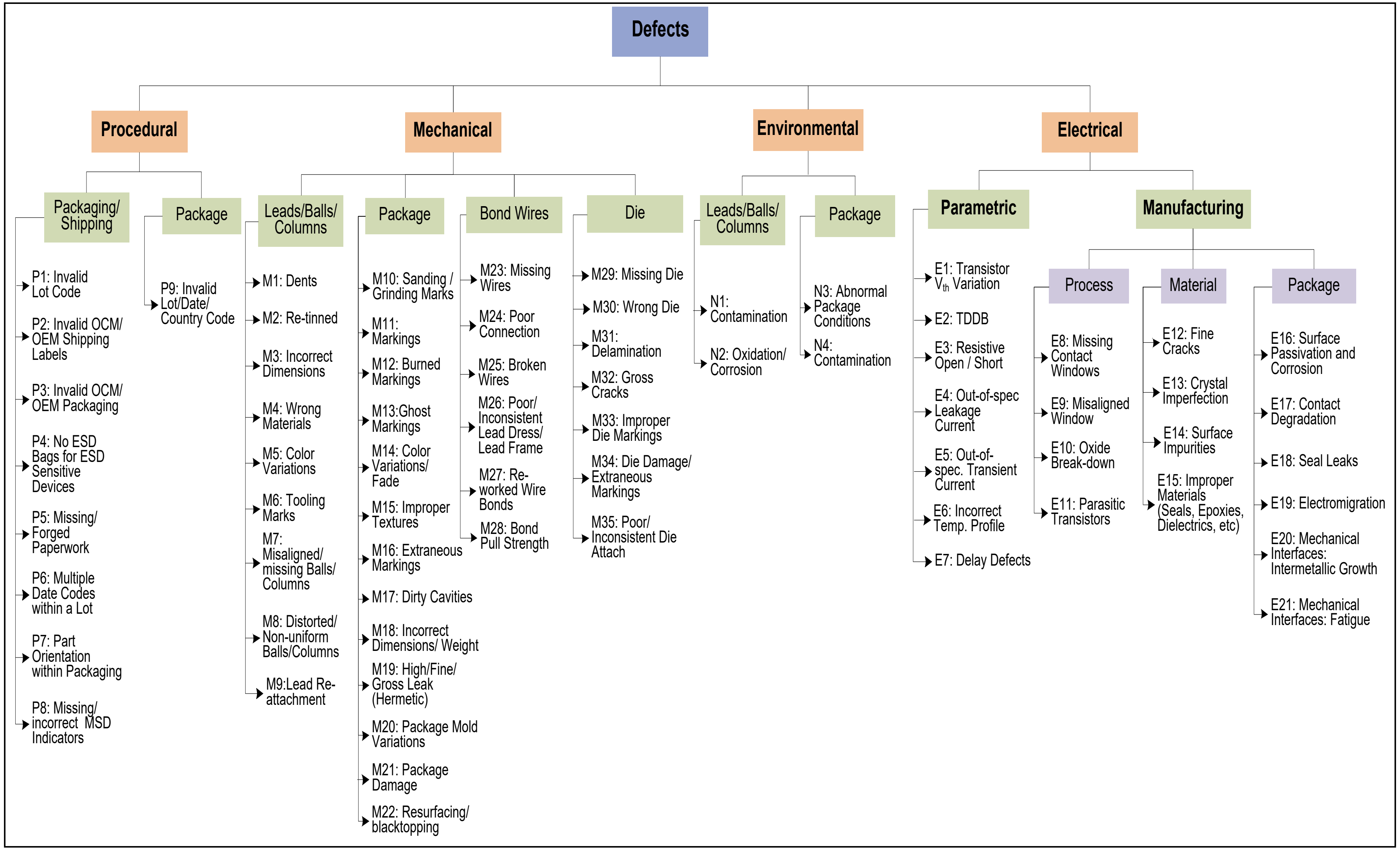
AS6171 – Test Methods Standard

Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts	
Purpose	• Standardize practices to detect suspect counterfeit EEE parts and to ensure consistency of test techniques and requirements across the supply chain
Target Audience	• Independent Testing Facilities • Distributors & OEMs (in-house testing capability) • OEMs, Integrators, and End-Users flowing down test requirements
Uses	• Test Methods for risk-based counterfeit detection • Proficiency for counterfeit test & evaluation • Intended to be used for accreditation of Independent Test Laboratories or Distributors
Status	• Published

Standards Based Testing

- This testing refers to the use of well-established characterization and measurement tools based on SAE AS6171 (such as external visual inspection, X-ray imaging, and electrical testing) to identify defects.
- A defect, in the context of counterfeits, refers to an anomaly in a part. Defects are features or characteristics that are not consistent with expectations for an authentic part or a specific part.
  - Example: The lead finish is different from that listed on material declaration.
- Conventional test methods include both destructive and non-destructive methods.

Taxonomy of Defects
(Device Types Identified in the AS6171)



- Defects
  - Procedural
    - Packaging/ Shipping
      - P1: Invalid Lot Code
      - P2: Invalid OCM/ OEM Shipping Labels
      - P3: Invalid OCM/ OEM Packaging
      - P4: No ESD Bags for ESD Sensitive Devices
      - P5: Missing/ Forged Paperwork
      - P6: Multiple Date Codes within a Lot
      - P7: Part Orientation within Packaging
      - P8: Missing/ incorrect MSD Indicators
    - Package
      - P9: Invalid Lot/Date/ Country Code
  - Mechanical
    - Leads/Balls/ Columns
      - M1: Dents
      - M2: Re-tinned
      - M3: Incorrect Dimensions
      - M4: Wrong Materials
      - M5: Color Variations
      - M6: Tooling Marks
      - M7: Misaligned/ missing Balls/ Columns
      - M8: Distorted/ Non-uniform Balls/Columns
      - M9:Lead Re-attachment
    - Package
      - M10: Sanding / Grinding Marks
      - M11: Markings
      - M12: Burned Markings
      - M13:Ghost Markings
      - M14: Color Variations/ Fade
      - M15: Improper Textures
      - M16: Extraneous Markings
      - M17: Dirty Cavities
      - M18: Incorrect Dimensions/ Weight
      - M19: High/Fine/ Gross Leak (Hermetic)
      - M20: Package Mold Variations
      - M21: Package Damage
      - M22: Resurfacing/ blacktopping
    - Bond Wires
      - M23: Missing Wires
      - M24: Poor Connection
      - M25: Broken Wires
      - M26: Poor/ Inconsistent Lead Dress/ Lead Frame
      - M27: Re-worked Wire Bonds
      - M28: Bond Pull Strength
    - Die
      - M29: Missing Die
      - M30: Wrong Die
      - M31: Delamination
      - M32: Gross Cracks
      - M33: Improper Die Markings
      - M34: Die Damage/ Extraneous Markings
      - M35: Poor/ Inconsistent Die Attach
  - Environmental
    - Leads/Balls/ Columns
      - N1: Contamination
      - N2: Oxidation/ Corrosion
    - Package
      - N3: Abnormal Package Conditions
      - N4: Contamination
  - Electrical
    - Parametric
      - E1: Transistor V_{th} Variation
      - E2: TDDB
      - E3: Resistive Open / Short
      - E4: Out-of-spec Leakage Current
      - E5: Out-of-spec. Transient Current
      - E6: Incorrect Temp. Profile
      - E7: Delay Defects
    - Manufacturing
      - Process
        - E8: Missing Contact Windows
        - E9: Misaligned Window
        - E10: Oxide Break-down
        - E11: Parasitic Transistors
      - Material
        - E12: Fine Cracks
        - E13: Crystal Imperfection
        - E14: Surface Impurities
        - E15: Improper Materials (Seals, Epoxies, Dielectrics, etc)
      - Package
        - E16: Surface Passivation and Corrosion
        - E17: Contact Degradation
        - E18: Seal Leaks
        - E19: Electromigration
        - E20: Mechanical Interfaces: Intermetallic Growth
        - E21: Mechanical Interfaces: Fatigue

The “Tampered” category is not addressed in the current release of AS6171, but will be included in future releases

Conventional Test Methods

- **AS6171/2: External Visual Inspection (EVI)**
  (general, detailed, remarking, resurfacing, weight, dimensions, SEM)
- **AS6171/3: X-Ray Fluorescence (XRF)**
  (lead finish, external, internal)
- **AS6171/4: Delid/Decapsulation Physical Analysis (DDPA)**
  (decapsulation, internal inspection)
- **AS6171/5: Radiological Inspection (RI)**
- **AS6171/6: Acoustic Microscopy (AM)**
- **AS6171/7: Electrical Test AS6171/9: Fourier Transform Infrared Spectroscopy (FTIR)**
- **….**

Second Order Effects

- Electronic parts may exhibit emissions or signatures that include, but are not limited to:
  - 1. Electromagnetic Radiation
  - 2. Conducted Radio Waves
  - 3. Magnetic Characteristics
  - 4. Power Behavior
  - 5. Thermal Profile
- These are the basis for side channel attacks in which information is extracted from physical functions of the device, and for authentication or counterfeit detection methods using side channels.

Side Channel Based Counterfeit Detection Methods

- Side channel refers to methods for extracting part functional information that are external to the part.
- Power consumption analysis
  - Idle or in operation
  - Examples: Battelle, PFP Cybersecurity
- Analysis of emitted electromagnetic radiation
  - Example: Nokomis
- Side channel methods are meant to be non-destructive in nature while also being relatively fast.

Machine Vision Based Counterfeit Detection Methods

- Machine vision involves the collection and analysis of images such as those from cameras, microscopes, or other forms of electromagnetic radiation (e.g., X-rays).
- Machine vision can be used to identify and "track" a registered part.
  - Registered parts are those that have been added to a system or part registry (i.e., database).
  - Registration methods are sometimes referred to as tracking, as they do not distinguish or compare parts, but rather identify those that have been seen previously.
- Machine vision may also be used to detect a potential counterfeit by comparison to an exemplar, defect identification, or lack of consistency within a lot.

Participants in the Study

UNITED STATES CONGRESS

SMT Corporation

DEFENSE MICROELECTRONICS ACTIVITY UNITED STATES OF AMERICA

calce

Machine Vision

Creative Electron

COVISUS

ALITHEON

Conventional

micross
one source. one solution.

INTEGRA TECHNOLOGIES

Side Channel

Sandia National Laboratories

BATTELLE

PFP CYBERSECURITY

NOKOMIS

Technology Evaluation Considerations (1/2)

- What is the product that you are selling to customers?
- What is the critical technology element?
- How many units are manufactured?
- Are units in stock or are they built against order?
- Do the units include software and database? Do the users have to subscribe for getting those features?
- Do you have a product data sheet?
- Do you offer support service?
- Do you offer repair or upgrades?
- Are the units built outside of the company?
- What is the plan for ramping up production in the event that demand increases?

Technology Evaluation Considerations (2/2)

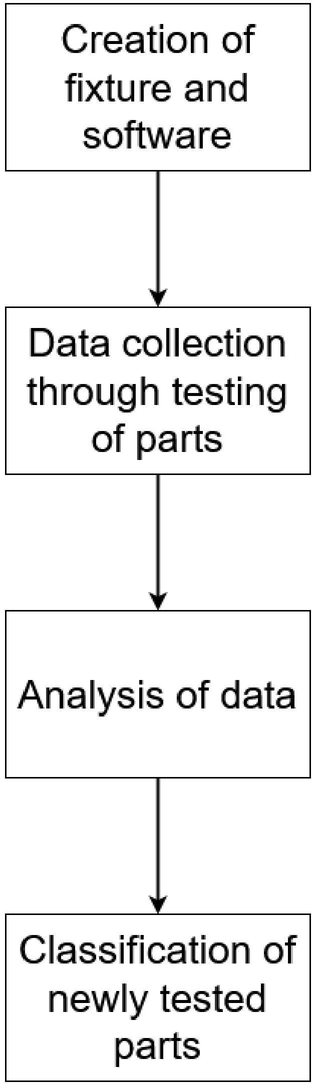
- What is the lead time to buy a unit?
- What is the price of the unit?
- Is the infrastructure in place to support and service 100 fielded units? 1000 fielded units?
- Do the units include both software and a database of signatures of authentic parts? Do users have to pay extra or subscribe for software or database features?
- What is the typical preparation time to test a new part/package type (including fixturing, testing, and training)?
- Have units been qualified for office/laboratory use, including measurement quality and reliability?
- Have units been qualified for outdoor/uncontrolled environment use, including measurement quality and reliability?

Blind Testing Program

- **Parts:**
  - A selection of advanced counterfeits (clones) and conventional counterfeits, with varying package type and original component manufacturer (OCM), along with corresponding authentic parts
- **Testing:** Performed by SMT, CALCE, and a variety of partner organizations using one of the following three approaches:
  - Conventional Techniques
  - Side Channel Methods
  - Machine Vision Technology

Part Classification Using Side Channel Methods

- Setup and planning for side channel methods includes the production of fixtures, and programming of software for collecting and analyzing test data.
- Depending on the nature of available information on the parts, data can be used to cluster or classify parts, or for tracking.
- Clustering (unsupervised learning) involves grouping parts with similar behavior together.
- Classification (supervised learning) requires training on known parts, followed by assignment of tested parts to labeled groups (e.g., authentic, counterfeit).



Creation of fixture and software

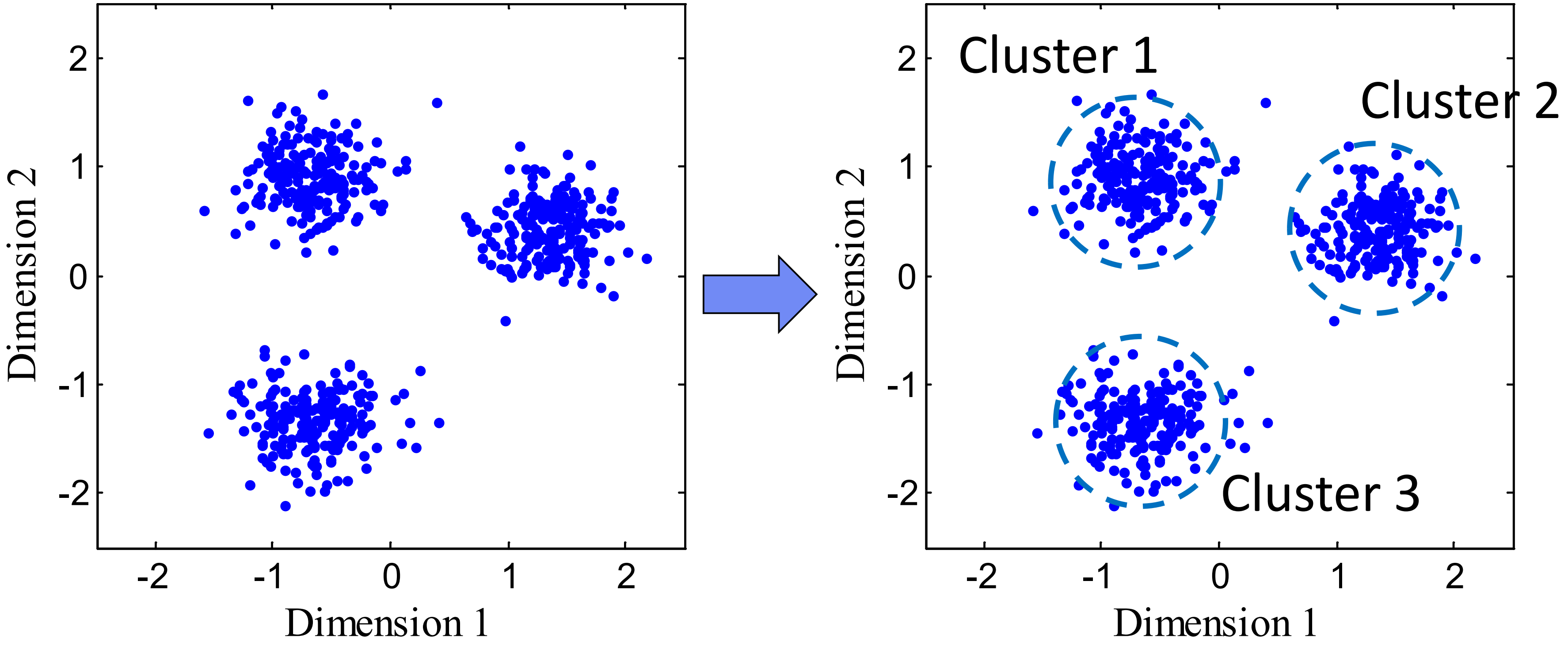
Data collection through testing of parts

Analysis of data

Classification of newly tested parts

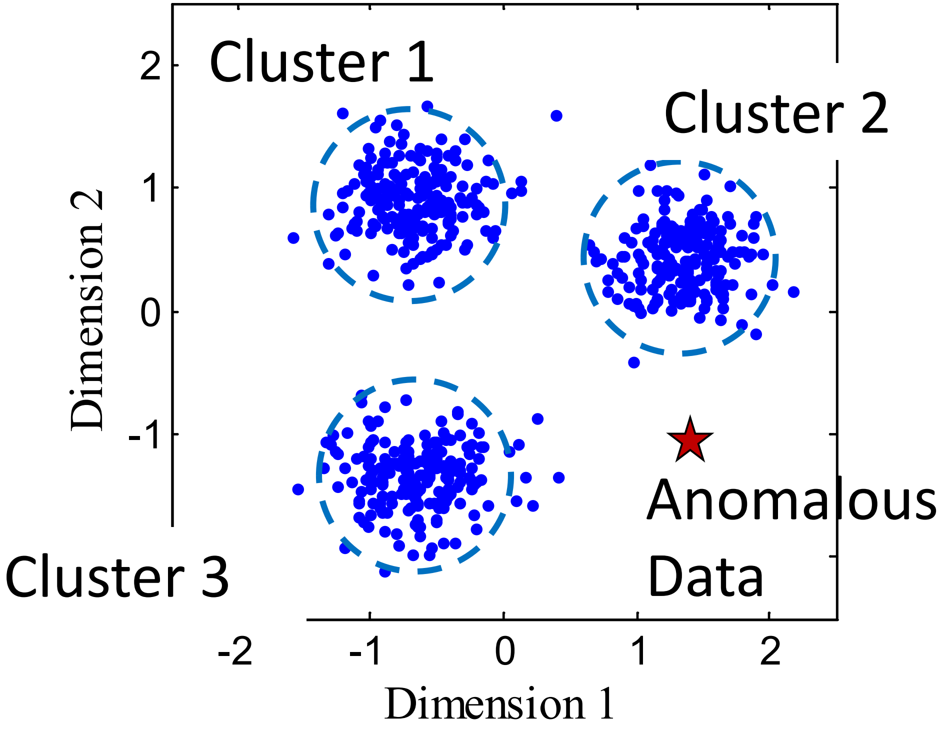
Clustering

- Without parts of known provenance (i.e., unlabeled data), patterns in the data can be used to group parts with similar characteristics.



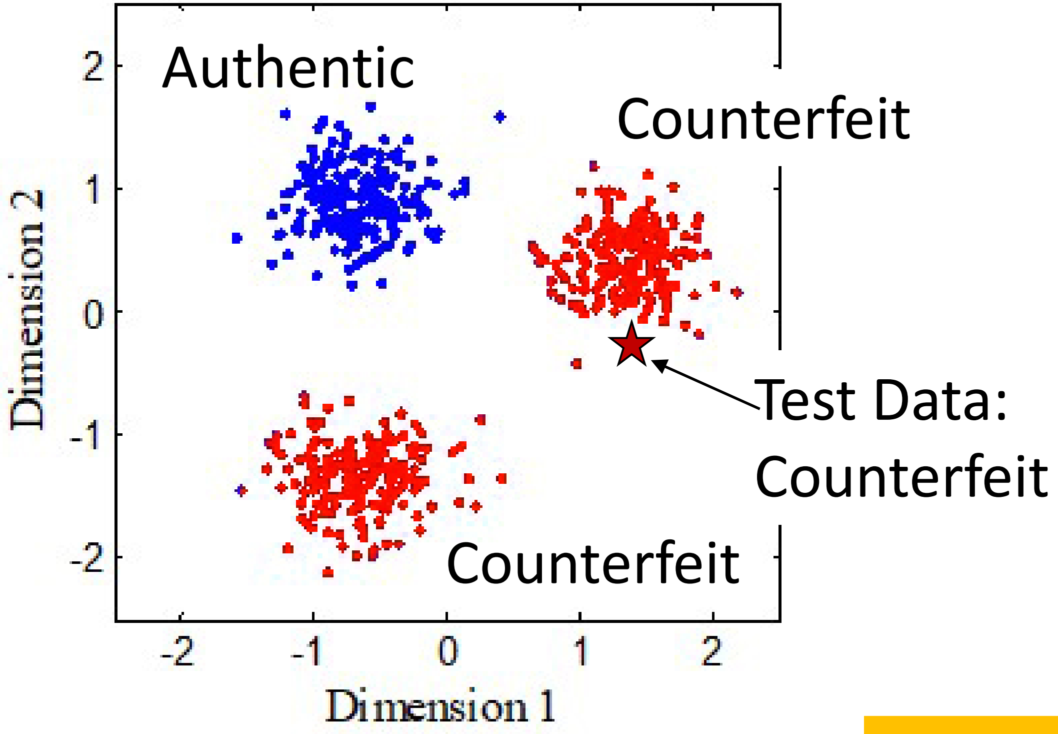
Clustering-Based Anomaly Detection

- Even with unlabeled data, anomalies can be identified based on distance from clusters.



Classification

- With parts of known origin used to *train* an algorithm, unknown *test* parts can be categorized according to the similarity of their characteristics to the training data.



Use of Acquired Images via Machine Vision

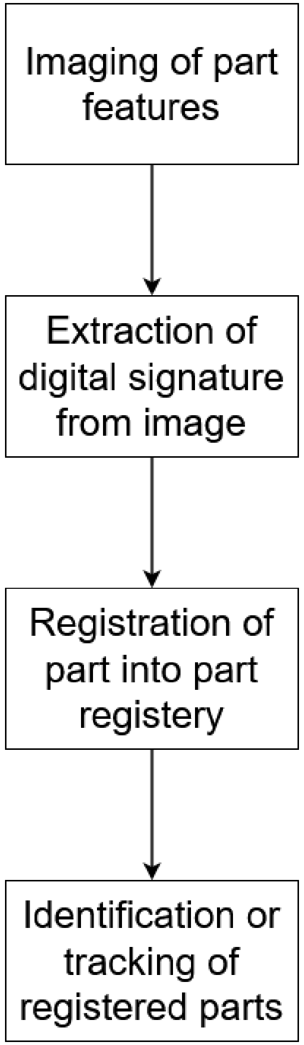
- Identifying relevant features in the image (which could be as simple as geometric shapes or as complex as abstract patterns or spatial wavelengths of color or contrast using machine learning and artificial intelligence tools); and/or
- Extracting information by analyzing the features (e.g., performing quantitative measurements such as size or shape, comparing to reference data or criteria of acceptability, documenting defects).

Thinking Beyond Visible Part of EM Spectrum

- It is useful to consider authentication technologies that are based on techniques for extracting features or images of microelectronic devices using energy outside of the visible part of the electromagnetic spectrum.
- Examples include X-ray radiography, magnetic resonance imaging, terahertz imaging, and imaging or mapping of signals using infrared radiation (e.g., infrared thermography or Fourier Transform Infrared Radiation mapping).
- X-ray radiation generated by interaction with electrons (Energy Dispersive X-ray Spectroscopy, or EDS) or through fluorescence of incident X-ray radiation (X-ray Fluorescence Spectroscopy, or XRF) are also potential candidates.

Identification and Tracking Using Machine Vision

- Registration is performed on parts of known provenance (e.g., at the original component manufacturer or OCM).
- Once a part is registered it may move into the supply chain.
- At any point in the future, the part may be imaged again and checked against the part registry.
- Comparison to the database may use machine learning methods to establish similarity to prior data.


Imaging of part features
Extraction of digital signature from image
Registration of part into part registery
Identification or tracking of registered parts

What are Needed for the Tools to Succeed

- Classification ability by product (beyond tracking)
- Original component manufacturer participation
- Integration with production process and ability to use for inline, real-time decision making
- Defect identification to satisfy requirements of industry standards for visual inspection
- Data security and efficiency of database access and search with scaling of implementation
- Business stability (e.g., change of focus, merger/acquisition, or financial insolvency)
- Adaptability to data acquisition technology changes

Adoption of Machine Vision Technology Recommendations

- Machine vision technologies should be developed further to comply with industry standards on general external visual inspection of electronic parts.
- The customers need to develop a better understanding of the costs and benefits of machine vision and how it can best be implemented.
- A strong business case for adoption of machine vision technologies needs to be made.
- Consideration should be given to the costs of adopting machine vision technologies, including capital investments, administrative overhead, security, and potential licensing costs.

Conclusions

- Standards-based testing for counterfeit detection remains the most practical and effective tool.
- Both side-channel and machine vision technology based counterfeit detection tools have shown ability to classify components into groups with high degree of accuracy and these can supplement the standards based methods.
- The side-channel and machine vision tools are at technology development level and need more maturity before becoming acceptable as commercial stand-alone counterfeit detection tools.

2021 Symposium on Counterfeit Parts and Materials: Virtual Event on August 3-5 (https://smta.org/counterfeit)

SMTA

A Global Association Working at a Local Level

- This long-running symposium continues to provide relevant information that can solve problems today while planning for a different business and technology environment in the future.
- Abstract Submission Deadline: Monday, May 10, 2021 (https://smta.org/mpage/counterfeit-call-for-abstracts/)
- A workshop on modeling of supply chain to disrupt entry of counterfeit items into supply chain for high reliability products will be help on August 5 in conjunction with this event.
- Contact Dr. Das (diganta@umd.edu) or Prof. Sandborn (sandborn@umd.edu) for more information on the symposium and the workshop.