
Counterfeit Detection and Avoidance

Mark Tehranipoor

**Introduction to Hardware Security & Trust
University of Florida**

Why Counterfeiting?

❑ **Lucrative business**

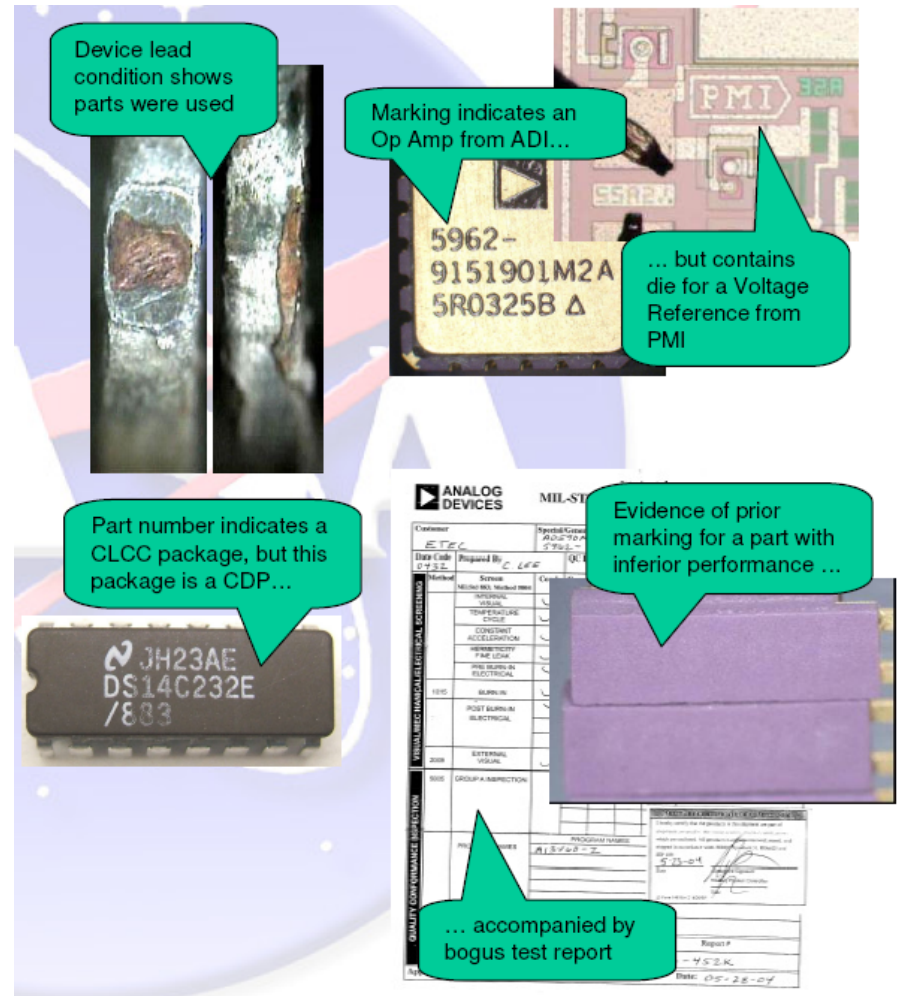
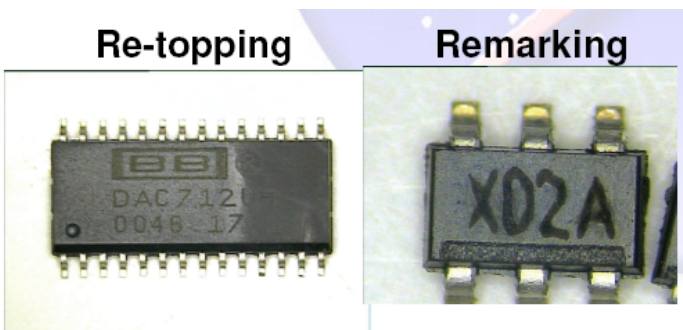
- Easy money, floating everywhere in the world
- Easy to make counterfeit components
- Enough raw material
 - ❑ E.g. ever increasing electronic waste.
- Copy one's design and fabricate components without paying royalty or any R&D costs

❑ **Criminal Activity**

- To cripple the supply chain of one countries defense system.
- To contaminate one company's reputation.
- To kill the market share of one company.
- More ...

Counterfeit Electronic Parts

- Parts remarked or re-topped
- Defective parts scrapped by the OCM (Original component manufacturer)
- Previously used parts salvaged from scrapped assemblies
- Devices which have been refurbished, but represented as new product.
- Overproduced parts by the foundry
- Cloned IP → IC
- Forged Documentation – Misrepresentation of an IC
- Manufacturer Reject



Counterfeit Electronic Parts

- A counterfeit component [1] [2]
 - ❑ is an unauthorized copy,
 - ❑ does not conform to OCM design, model, or performance standards,
 - ❑ is not produced by the OCM,
 - ❑ is out-of-specification, defective, or a used OCM product sold as new,
 - ❑ has incorrect or false markings or documentation, or
 - ❑ is produced or distributed in violation of intellectual property rights, copyrights, or trademark laws.

OCM: Original Component Manufacturer

Examples

- Leads:



Examples- Cont.

- Incorrect device leads:

Non-gold leads



Gold leads on real device



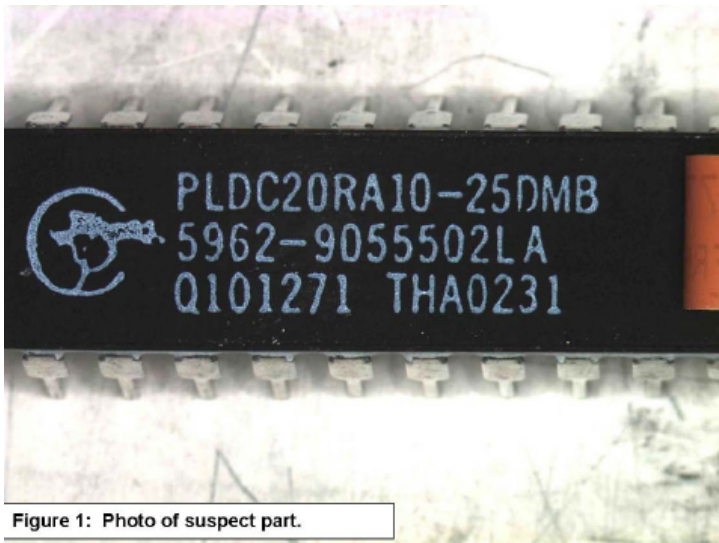
Examples- Cont.

- Dual Marking:

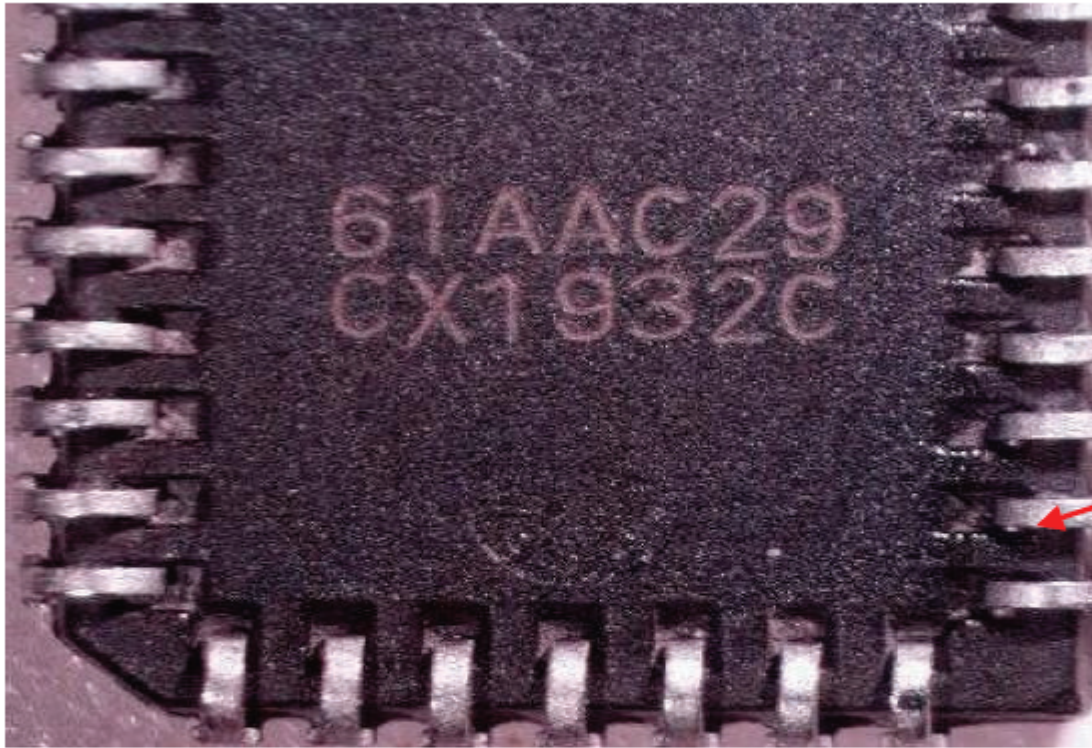


Examples- Cont.

- Good part has only two lines of marking

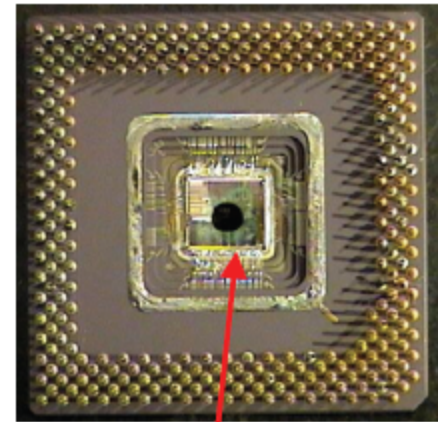


Examples- Cont.

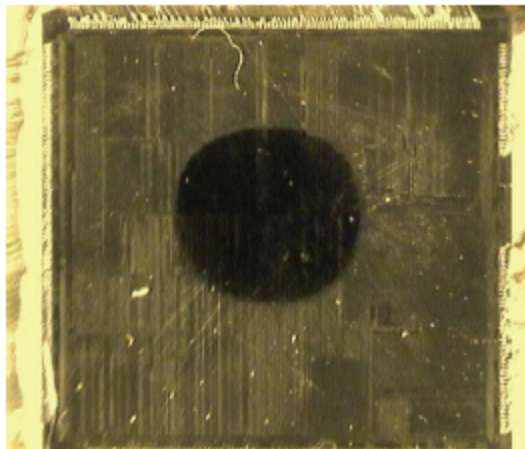


Backside, look at the black shiny paint like substance in the lower right side, the mold pin cavity is almost gone, look at the bent leads, looks like it may have been painted over to hide sanding marks and then fraudulently remarked

Examples- Cont.



Looks simple enough Intel device, marking not too bad, OH OH!!

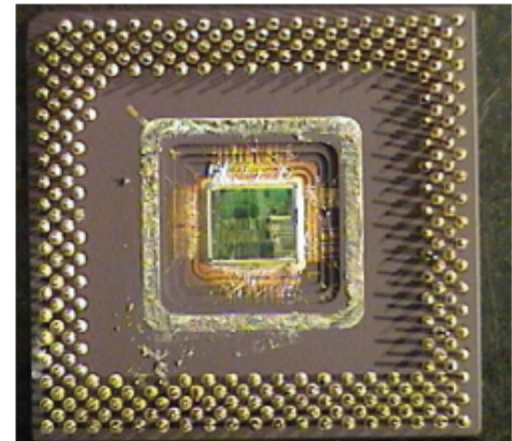


The ink dot that identifies a reject from wafer sort.



Here is the chip ID found after decap, looks good and matches the package marking

Examples- Cont.

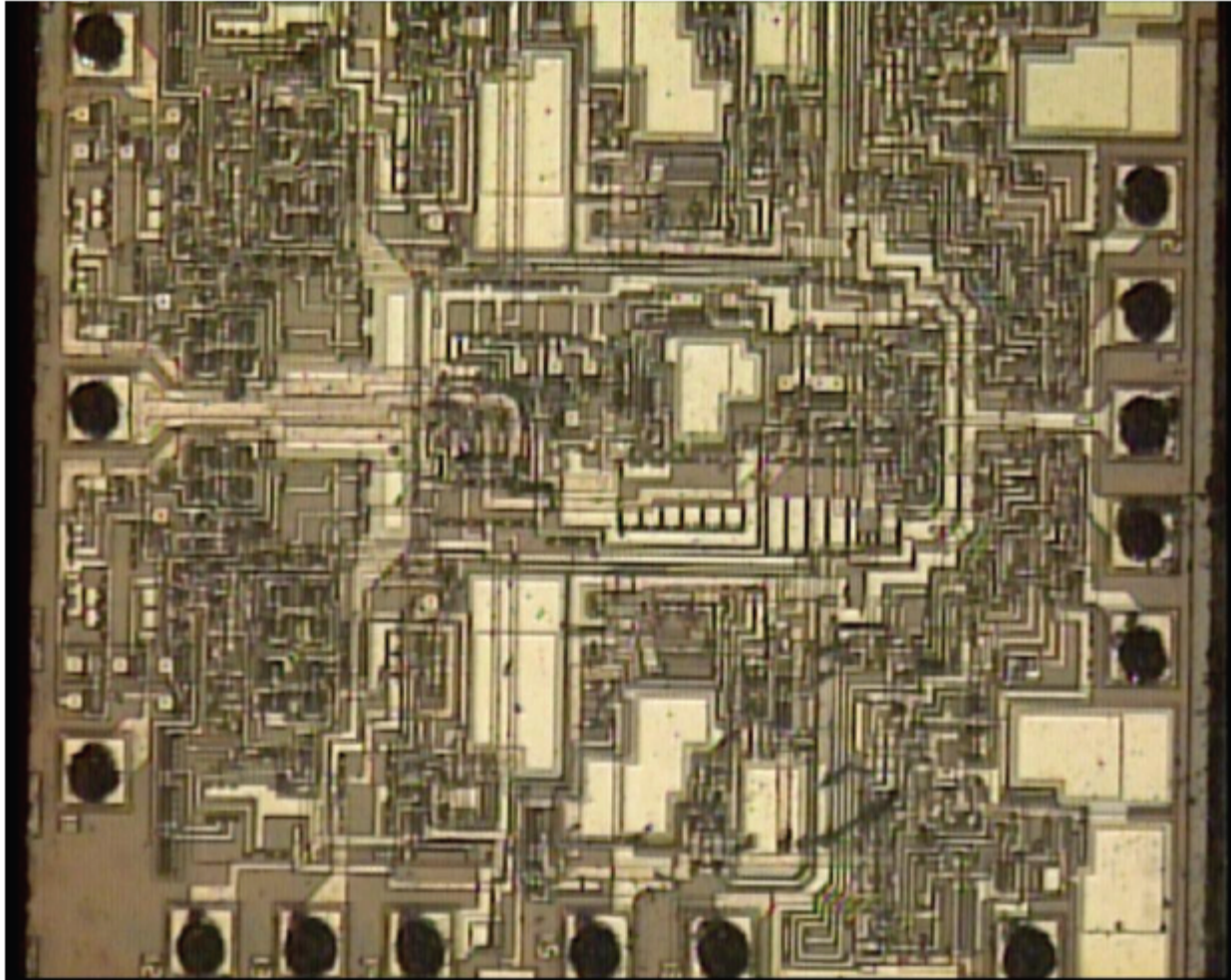


Same lot, same numbers but there is no ink dot



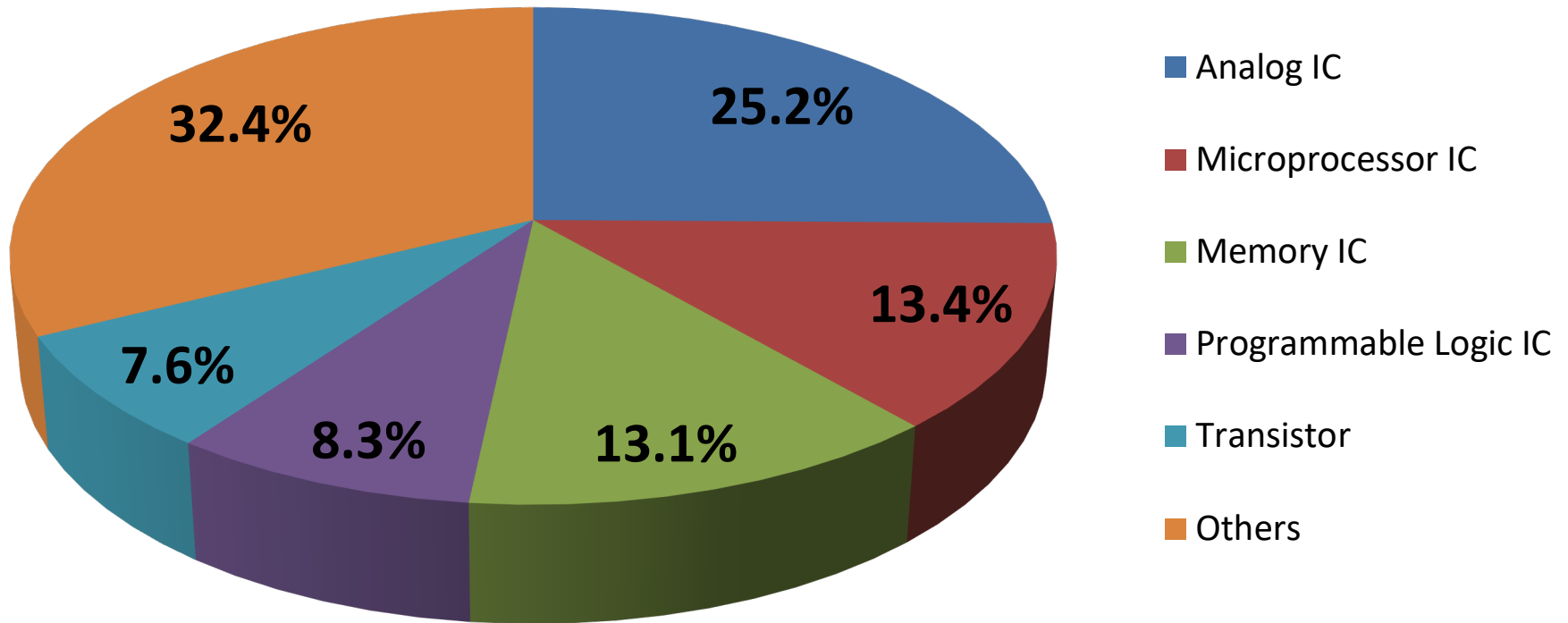
A close look at the characters shows they are backwards

Examples- Cont.



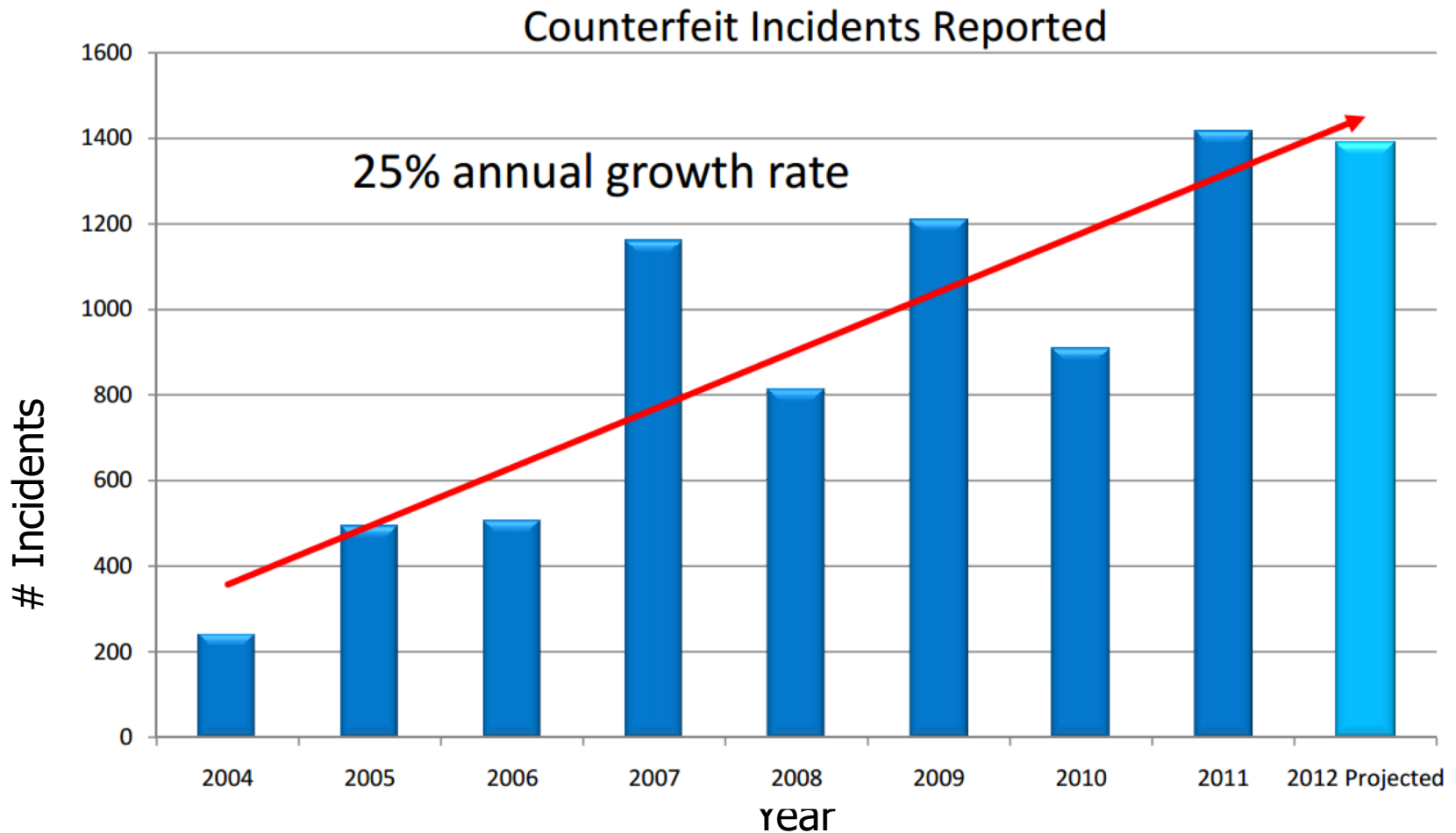
This is a cloned semiconductor chip

Most Counterfeited Parts in 2011 (% Reported Incidents)



IHS reports a \$169B annual risk [3]

Reports of Counterfeits



Counterfeit incidents reported by IHS [4]

Detection Standards

- SAE G-19A Test Laboratory Standards Development Committee
 - ❑ **AS6081** - Counterfeit Electronic Parts; Avoidance Protocol, Distributors
 - ❑ **AS5553** - Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
 - ❑ **AS6171** - Test Methods Standard; Counterfeit Electronic Parts
 - ❑ **ARP6178** - Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors
- CTI CCAP-101
- IDEA-STD-1010
 - ❑ Inspection standard addressing the needs for the inspection of electronic components traded in the open market

SAE G-19A Test Laboratory Subcommittee

Standardize Test & Inspection Requirements Across Industry

Type of Part

Testing Technique

Test Matrix – testing performed by certified test laboratories (AS6171)

Testing Tier

Sampling Plan

Risk Based Recommendations

Application

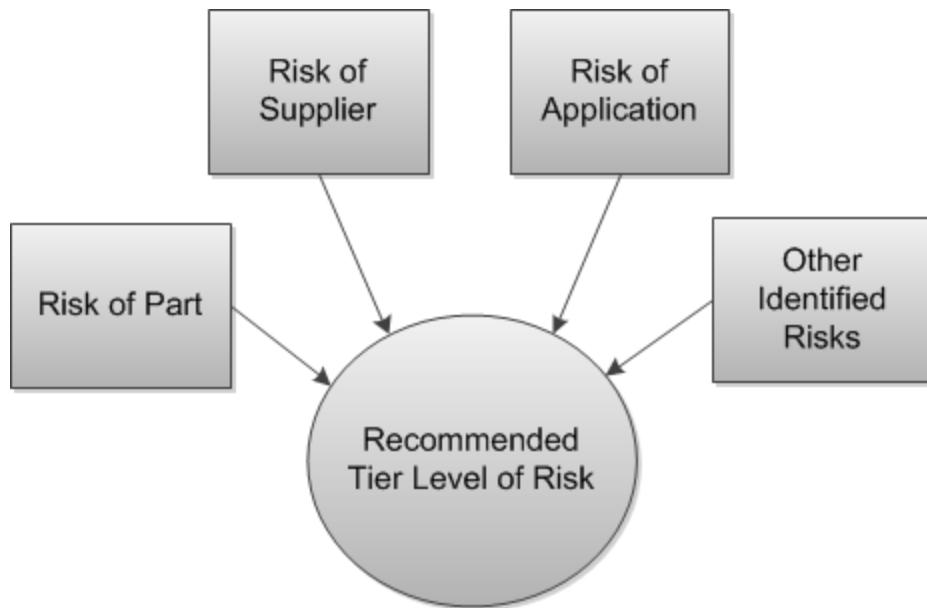
Part

Supplier

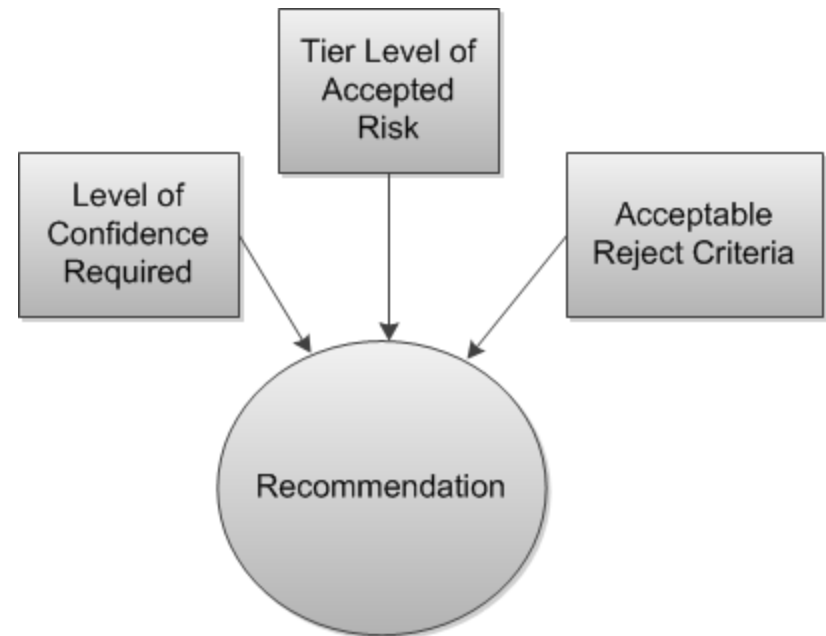
- ***System intended to create standardized testing methodology and consistency throughout industry***

AS 6171 - Aerospace Standard

Recommended Risk Decision Tree



Recommended Sampling Plan



Testing Level Based on Risk

CRITICAL

- Electrical Test: Active Devices- DC, key AC/Switching parameters, and full Functional Test over temperature, Burn-in (240 hrs. for Space Grade Microelectronic products, for other products and applications BI time may vary) and Final Electricals to include limits and delta limits; Passive Devices-Key Electrical Parameters Test over temp., Burn-in (BI time to be specified by Components Engineer for Space Grade Microelectronic products, for other products and applications BI time may vary), Final Electrical including limits and delta limits
- Temp Cycling
- Optional:/Misc. (RAMAN, FDIR, DSC, TMA, etc.)

HIGH

- Key (AC, Switching, functional) At Ambient Temp
- Electrical Test: Active Devices DC, key AC/Switching parameters, and full Functional Test over temperature; Passive Devices-Key Electrical Parameters Test over temperature.

MODERATE

- Basic functional at Ambient Temp
- Electrical Test: Active Devices- DC, key AC/Switching parameters and key Functional, at ambient temperature; Passive Devices-Key Electrical Parameters Test at ambient temperature.

LOW

- Delid Physical Analysis
- Radiographic Inspection/X-RAY
- Acoustic Microscopy (AM)
- Seal (hermetic devices)
- Electrical Test ; Active Devices- DC Test at ambient temperature; Passive Devices- Value measurement at ambient temp.

VERY LOW

- External Visual Inspection, EVI_G, General Inspection
- Remarking & Resurfacing
- XRF, Lead Finish
- External visual Inspection, EVID Detailed Inspection
- Electrical Test: Active Devices-Curve Trace at ambient temperature; Passive Devices-Value measurement at ambient temp

AS6171: Active Device Counterfeit Part Detection Flow

Steps	Mechanical/Environmental/Electrical Inspections/Tests	4 Critical Risk	3 High Risk	2 Moderate Risk	1 Low Risk	0 Very Low Risk
1	External visual Inspection, EVI _G (General, Full Lot)	Y	Y	Y	Y	Y
2	External visual Inspection, EVI _D (Detailed, Sample)	Y	Y	Y	Y	Y
3	Remarking & Resurfacing, p/o EVI Inspection	Y	Y	Y	Y	Y
4	XRF	Y	Y	Y	Y	Y
5	Delid Physical Analysis	Y	Y	Y	Y	
6	Radiological/X-RAY	Y	Y	Y	Y	
7	Acoustic Microscopy (AM)	Y	Y	Y	Y	
8	Miscellaneous	AN	AN	AN	AN	
9	Seal (hermetic devices)	Y	Y	Y	Y	
10	Temp cycling/ End point electricals	Y	-	-	-	
11	DC Curve Trace, Ambient Temp					Y
12	Full DC Test, Ambient Temp	Y	Y	Y	Y	
13	DC, Key (AC, Switching, Functional), Ambient Temp	Y	Y	Y	-	
14	DC, Key (AC, Switching) & full functional Over Temp	Y	Y	-	-	
15	Burn-In & Final Electricals with Limits & Delta Limits	Y	-	-	-	

■ Integrated Circuits

- Digital logic:
 - DC parameters, 25⁰C and min/max temperature
 - Other tests useful to verify authenticity
- Linear, Op Amps & Mixed logic
 - Full power & voltage conditions
 - DC parameters, 25⁰C and min/max temp
 - AC parameters 25⁰C
- Microprocessors, DSPs, Microcomputers & similar
 - Key DC parameters at 25⁰C and min/max temperatures
- Memories, RAM, SRAM, FPGA, etc.
 - Input and output pins, open and short
 - DC parameters at min/max temperature
 - FPGAs are unprogramed
 - Write and read to memory and speed, for RAM and FPGA
 - Other applicable tests
- Other Type Devices
 - Similar parameter verification based upon datasheet

Drawbacks

■ Drawbacks

□ All these **standards**

- Deal only two types of counterfeit parts (recycling and remarking)
- Works on the sampling basis.

□ **Test time** is extremely high (several Hrs/parts).

□ The **test methods**

- can detect only physical defects.

□ **Electrical test methods**

- are too simple to address the detection of counterfeit integrated circuits (ICs).

Components

Types of Components

Digital

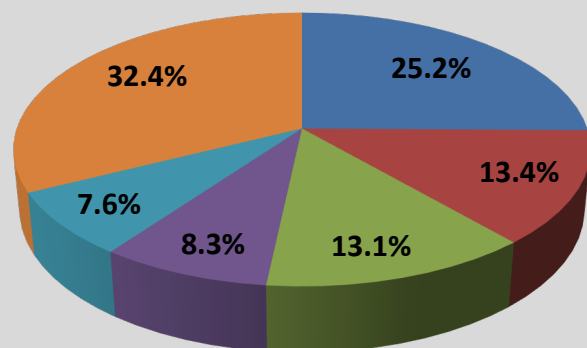
Memory, Programmable Logic Devices, Microprocessor, ASIC, etc.

Analog

Amplifiers, Filters, ADCs, DACs, Mixers, Phase Shifters, etc.

Discrete

Resistors, Diodes, capacitors, inductors, Transistors, sensors, etc.



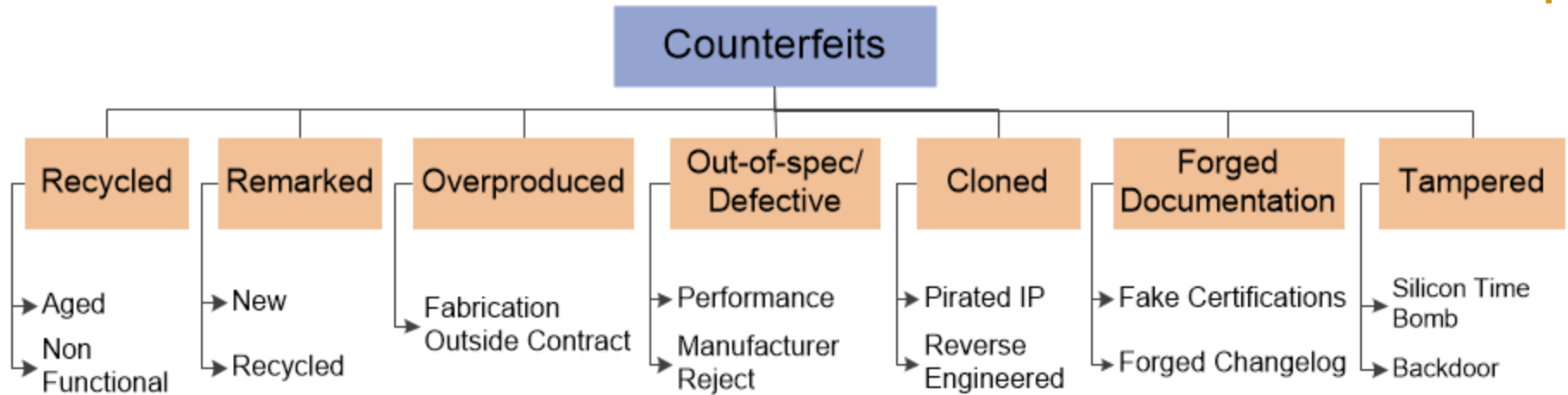
- Analog IC
- Microprocessor IC
- Memory IC
- Programmable Logic IC
- Transistor
- Others

IHS reports a **\$169B** annual risk

Top Part Type Reported in Counterfeit Incidents	Where Used						
	Industrial Market	Automotive Market	Consumer Market	Wireless Market	Wired Market	Compute Market	Other
Analog IC	14%	17%	21%	29%	6%	14%	0%
Microprocessor IC	4%	1%	4%	2%	3%	85%	0%
Memory IC	3%	2%	13%	26%	2%	53%	1%
Programmable Logic IC	30%	3%	14%	18%	25%	11%	0%
Transistor	22%	12%	25%	8%	10%	22%	0%

The top five represent \$169 billion of semiconductor revenue in 2011, according to IHS iSuppli Application Market Forecast Tool (AMFT)

Counterfeit Types



- **Recycled** and **remarked** types contribute to majority of counterfeit incidents.
- Untrusted foundry/assembly can introduce **overproduced** and **out-of-spec/defective** parts
- **Cloning** can be done by a wide variety of adversaries (a small entity to a large corporation)
- **Tampered** parts act as a backdoor where secret information from the chip or sabotage system functionality

Recycled Parts

- More than **80% of the counterfeit** components are recycled [5]
- In 2005, the United States only properly recycled 10-18% of all electronic waste. That number has risen to 25% as of 2009.
- Most of the recycled parts are at the end of life
 - ❑ Damaged considerably due to usage and aging
- **Recycled Parts**
 - ❑ A genuine OCM part is manufactured and used in some equipment, device, or electronic gadget for a period of time
 - ❑ The user discards the device for any number of reasons
 - ❑ Scrap electronics are collected and sold to developing countries or other reclaiming facilities
 - ❑ Scrap devices are broken down into bare circuit boards and components
 - ❑ Components are crudely extracted from circuit boards under very high temperature and prepared for resale

IC Recycling Process

A recycling center



PCBs taken off of electronic systems



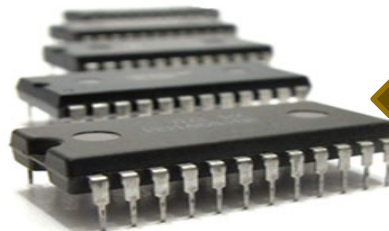
ICs taken off of PCBs



Critical Application



Resold as new



Identical:

Appearance, Function, Specification

Refine recycled ICs



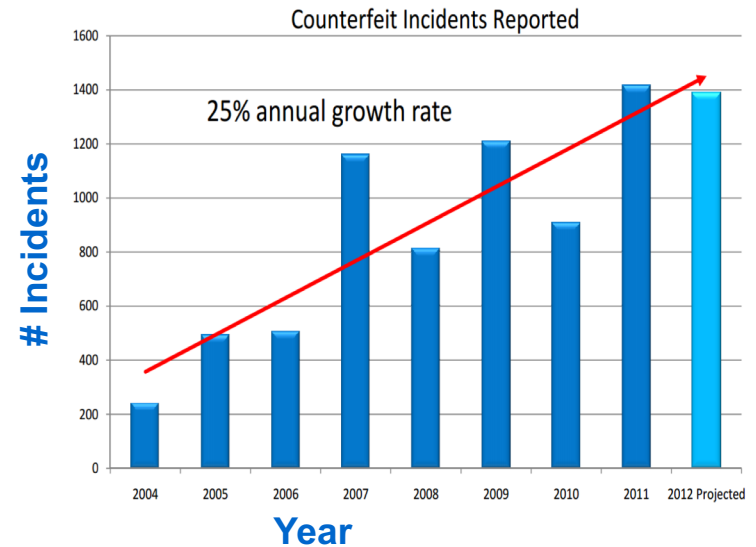
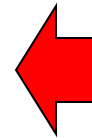
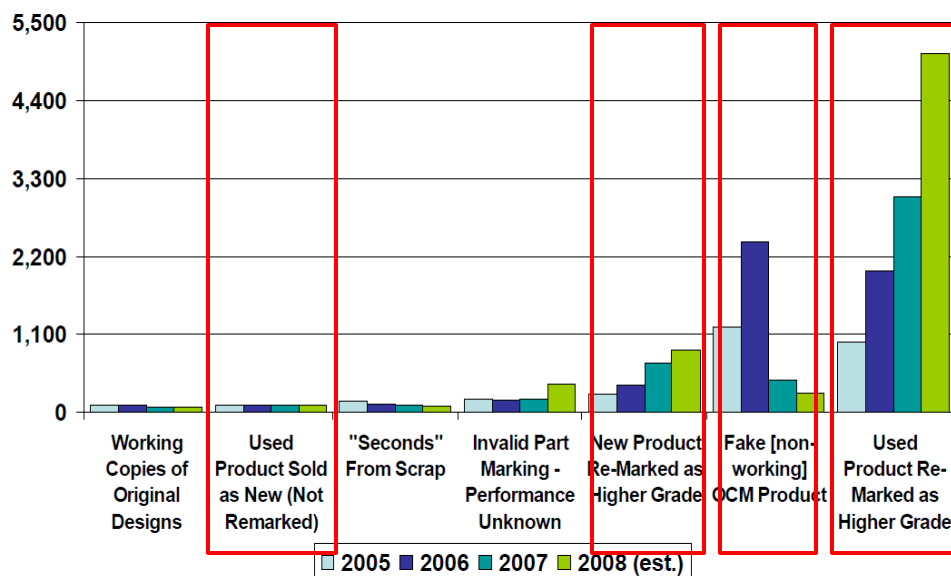
Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Source: Images are taken from google

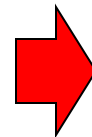
Recycled and Remarked ICs

- Recycling and remarking of ICs have become major security and reliability problems
- IC Recycling: \$9-\$15 billions every year

IHS: All counterfeit Incidents since 2004



Counterfeit type incidents in 2005-2008 reported by US Dept of Commerce Bureau of Industry and Security Office



Remarking

- Recycling and Remarking are the most discussed counterfeit parts
- **Remarking parts are of two types**
 - ❑ Recycled components
 - ❑ New Components
 - ❑ To change the specification of the component (commercial grade → military grade)
- **Remarking Process**
 - packages are sanded or grounded down to remove old markings
 - a new coating is created and applied to the parts
 - thermal or UV-cured epoxy

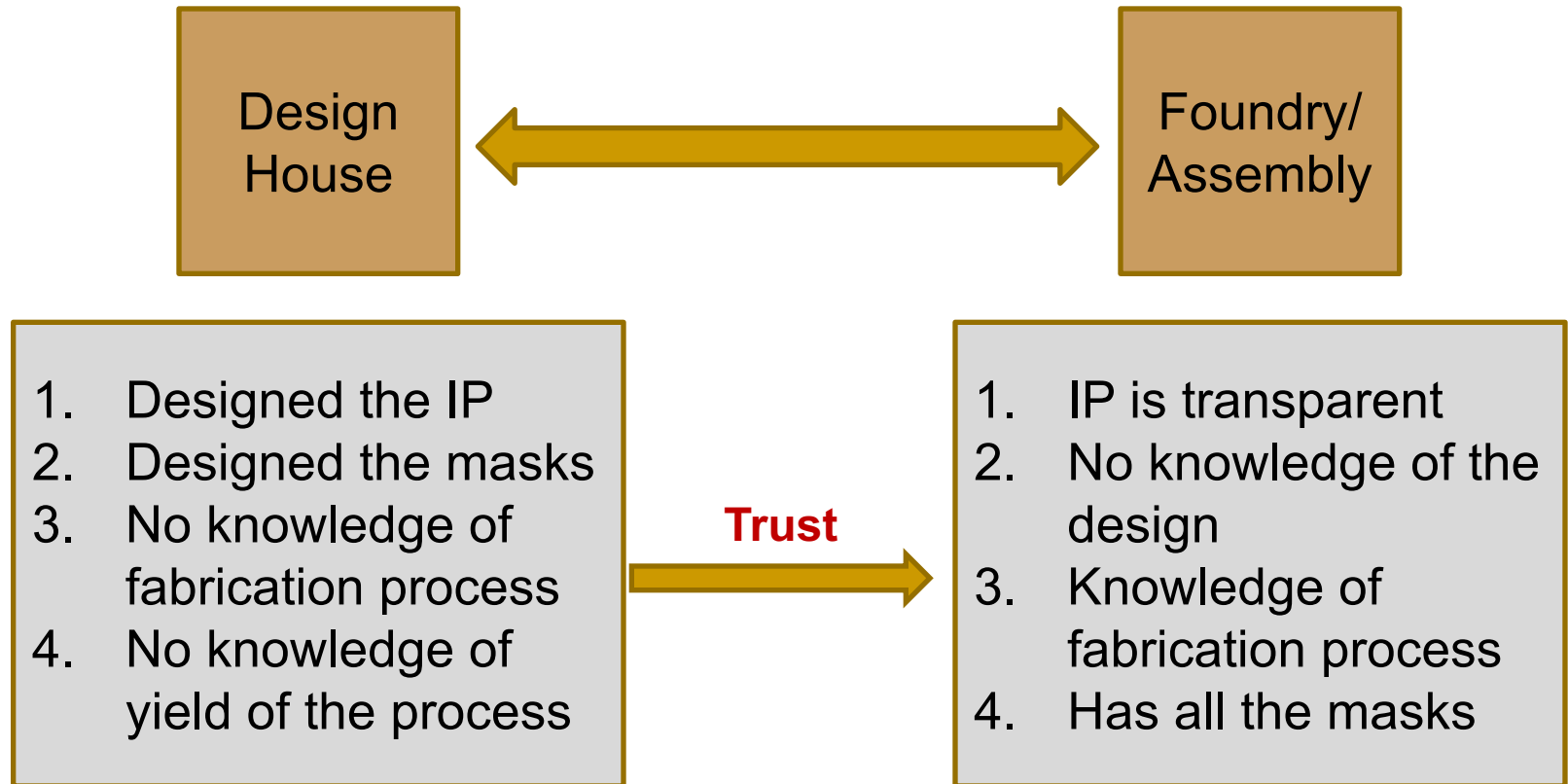
Remarking- Example



Overproduction

- The complexity of the integrated circuits (ICs) goes up exponentially as the feature size scaled down.
- Building and maintaining a modern fabrication unit costs more than \$3B and increasing day by day.
- Semiconductor business model shifted to contract foundry business model (horizontal business model).
- Example:
 - TI and AMD have outsourced their sub-45 nm fabrication to major contract foundries worldwide

Overproduction



■ Foundry can produce more parts

- ❑ Fabricate the yield data and sell the extra chips to the market.
- ❑ Can produce extra chips without sending the information to the design house .

Out-of-spec/ Defective

■ Untrusted Foundry can sell

□ **Defective parts**

- A chip may fail at one particular structural test pattern (The number of test patterns may vary in between several thousands)
- It is highly unlikely that defect will appear in normal operation of the chip in first few hours or days or months.
- Eventually, it will fail at some point of time.

□ **Out-of-spec parts**

- Fail to perform at the design specification (leakage current, dynamic current, performance, etc.)
 - The chip might fail at extreme physical/environmental conditions.
-

Cloned

■ Unauthorized production of a part

- Difference between overproduction and cloned is that cloned parts do not have the authorized IP, could be fabricated in a different foundry

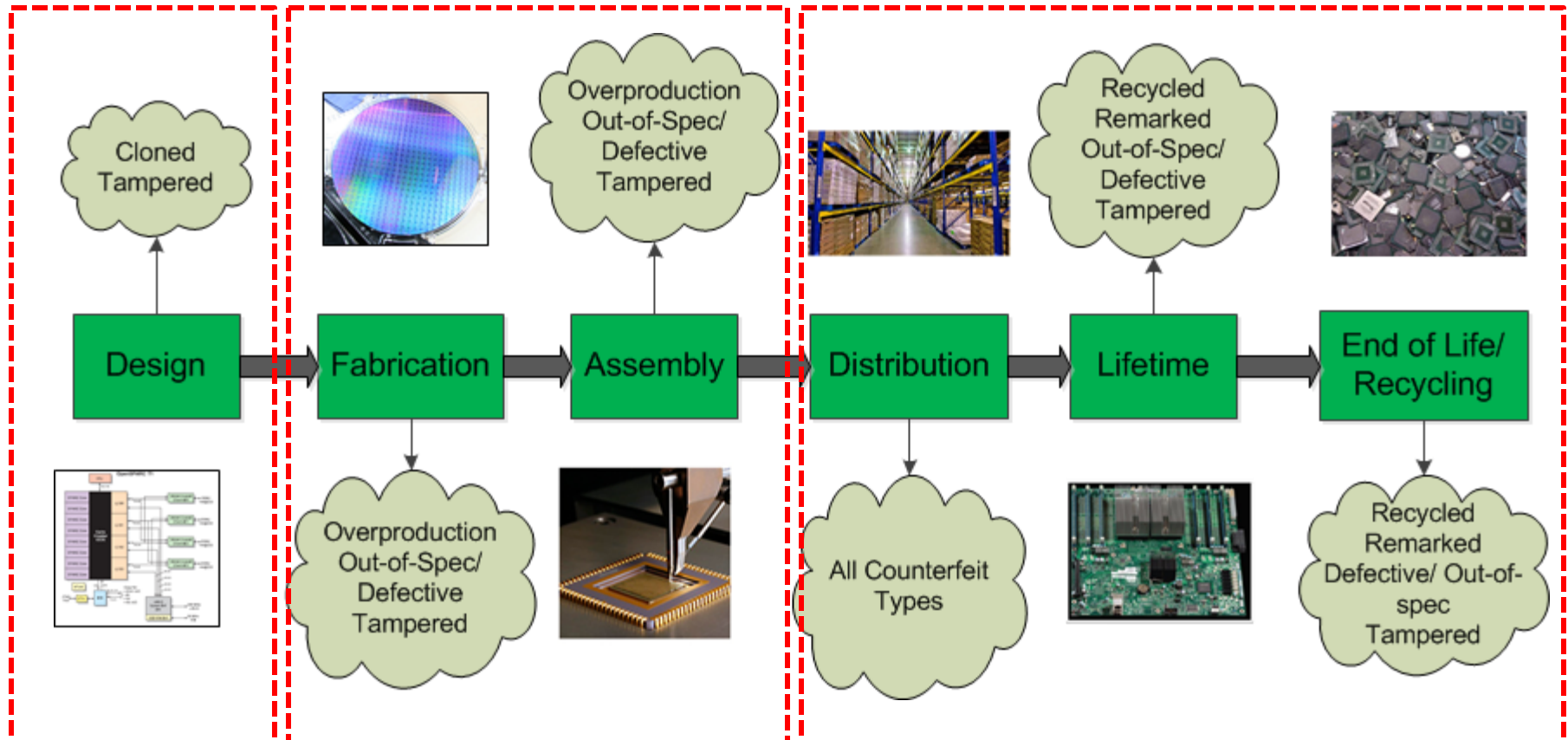
■ Cloned parts

- Pirated IP
 - Counterfeiters acquire the IP in an illegal manner (Saved the design cost of the IP).
- Reversed Engineered
 - Counterfeiters reverse engineer the design and make a new one just like the original design.

Forged Documentation

- The mismatch of specification documents between the purchased parts with the OCM (Original component manufacturer).
- Easy to detect as usually the original documents are present somewhere...
- Old parts (parts in the supply chain for around several years) have the higher probability of getting counterfeited.

Supply Chain Vulnerability



**Untrusted IP
Vendor & Sys.
Integ.**

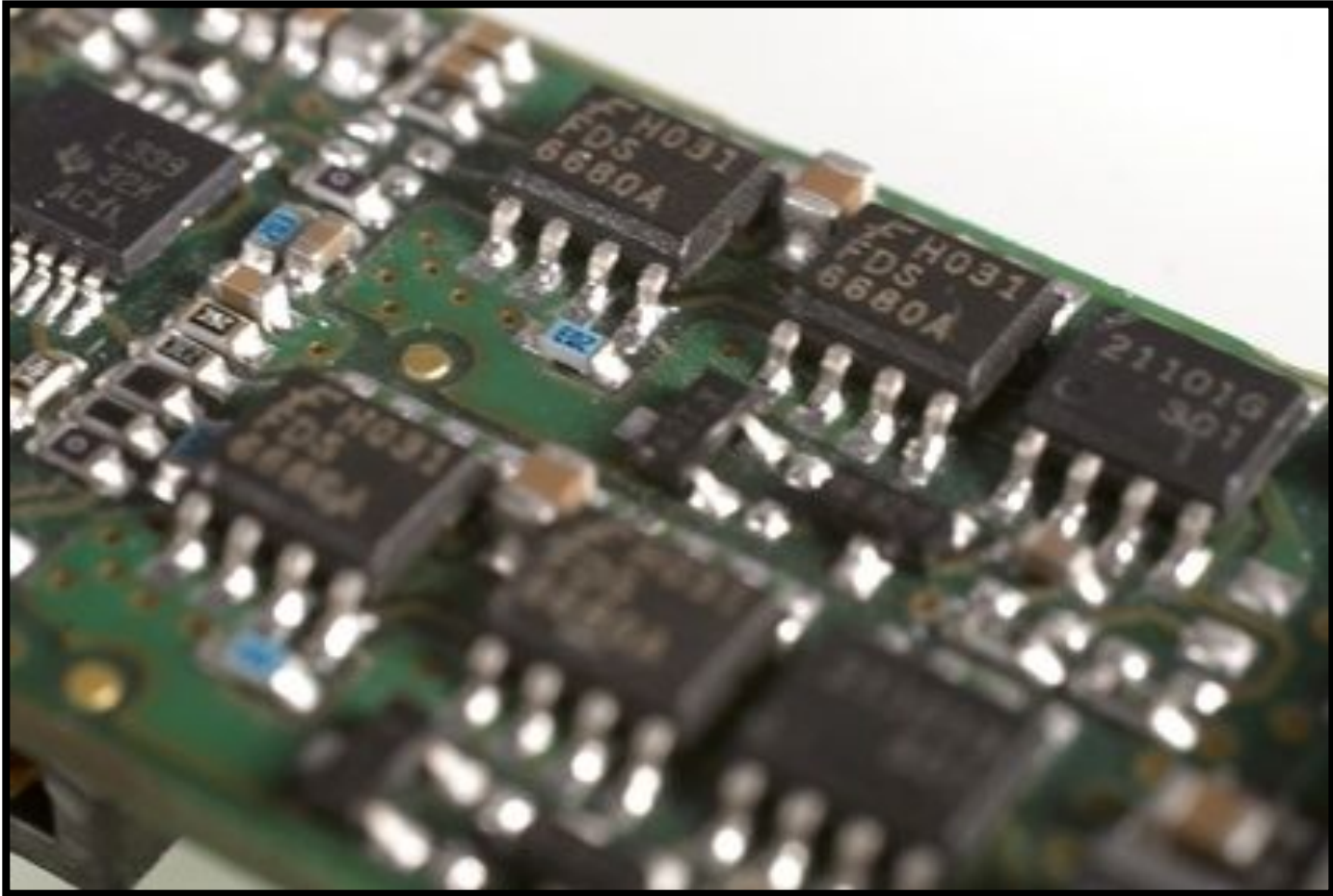
**Untrusted Foundry
& Assembly**

In the Field & Recycling

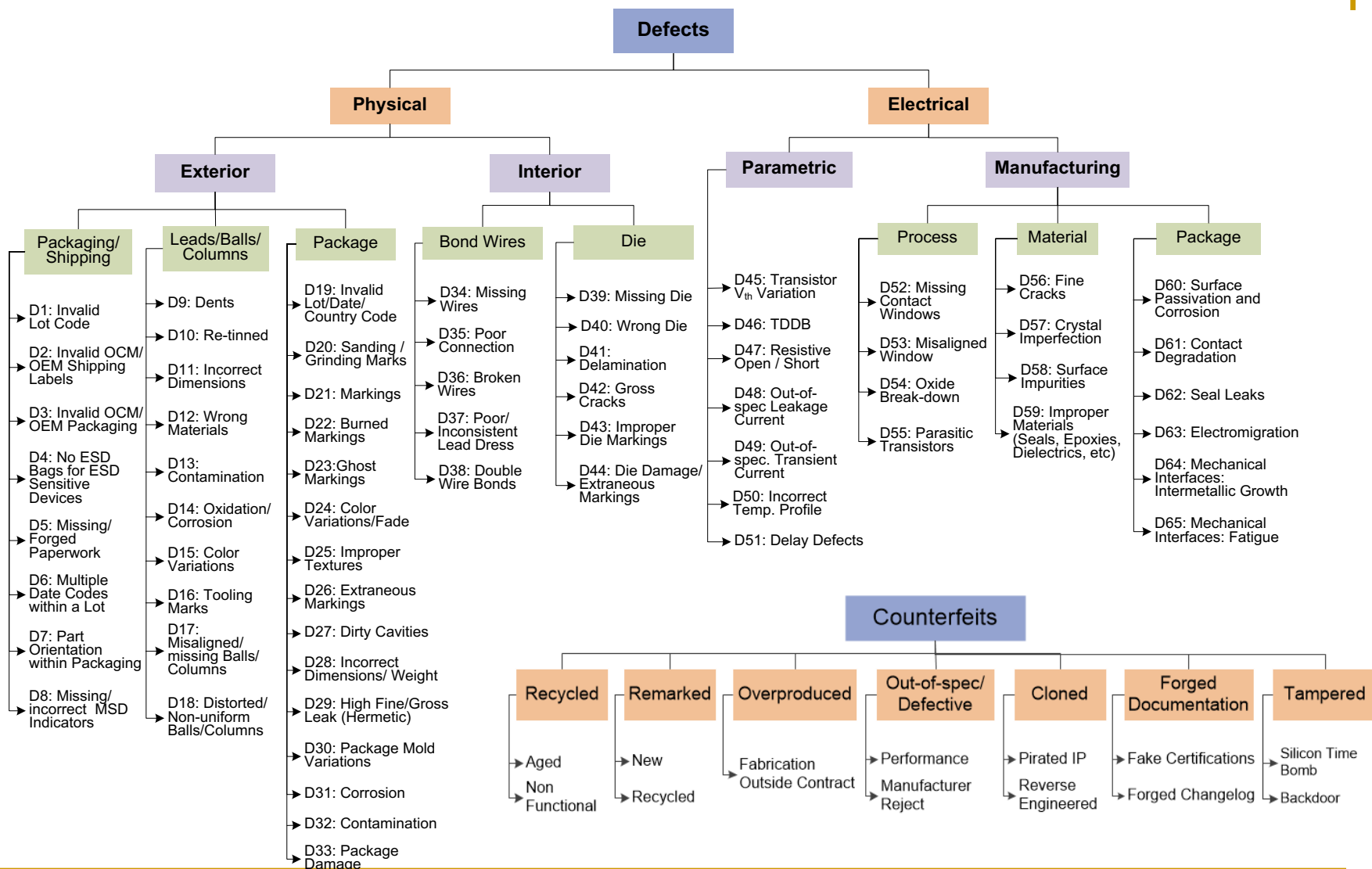
Maximum Flexibility

Minimum Flexibility

Counterfeits are Defective!



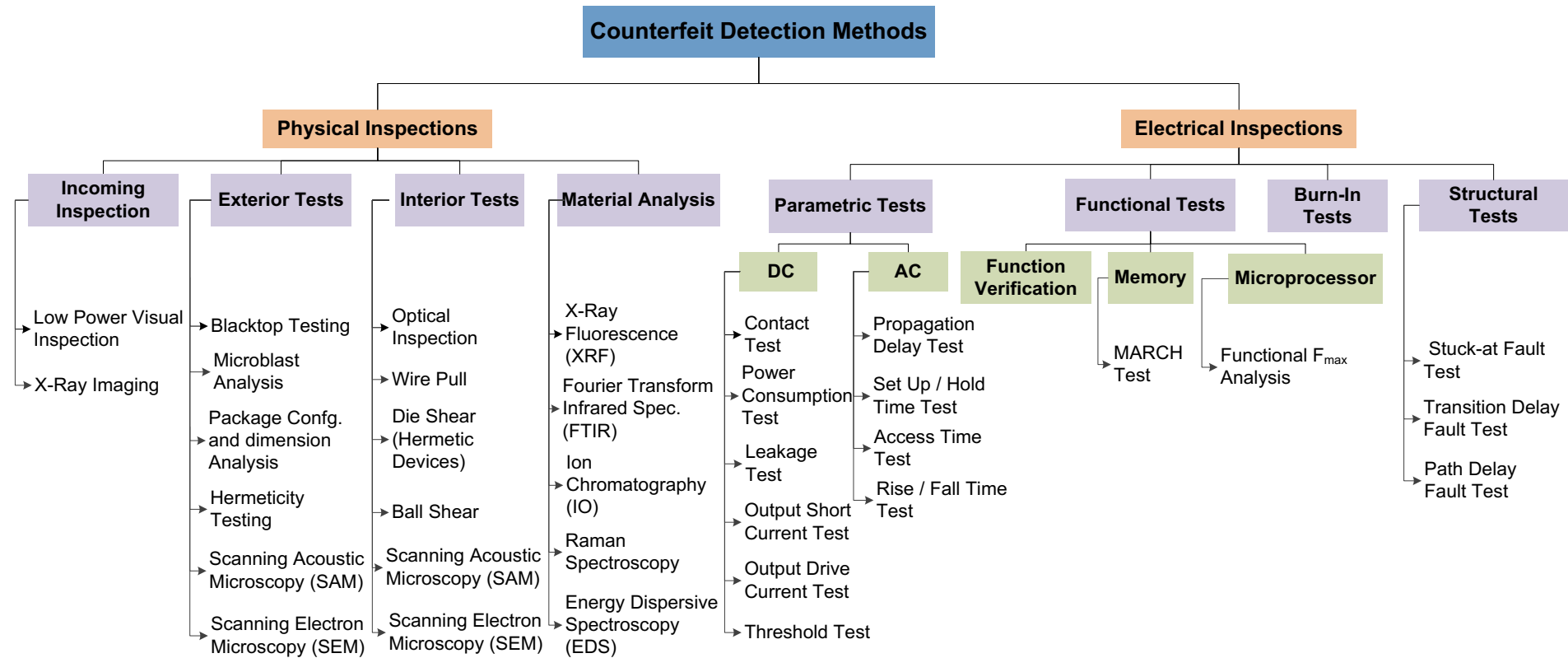
Counterfeit Defect Taxonomy



Testing for Defects



Detection Method Taxonomy



External Visual Inspection (EVI)

EVI:

- All devices shall be optically examined at a suitable magnification (3X to 100X) and with suitable lighting.
- A portion of inspection (sampling) shall be performed at 40X or higher.
- IDEA specification IDEA-STD-1010-A is a good reference.



Burned markings from low quality laser

Detailed EVI Inspection:

- A sample size of 119 devices shall be selected to undergo the detained EVI Inspection. Normally 116/c samples would be inspected to give a 90% confidence that the failures is at most 2%. The additional 3 samples are to be later used for marking permanency, lead finish (XRF), and Delid Physical Analysis (dpa).

Verification of:

- Date and Lot Codes
- Low Power Microscopy
- High Power Microscopy
- OEM Shipping labels
- Lead quality
- Dimensions & Weight
- Marking Quality

EVI Cont.

■ Test for Remarking and Resurfacing.

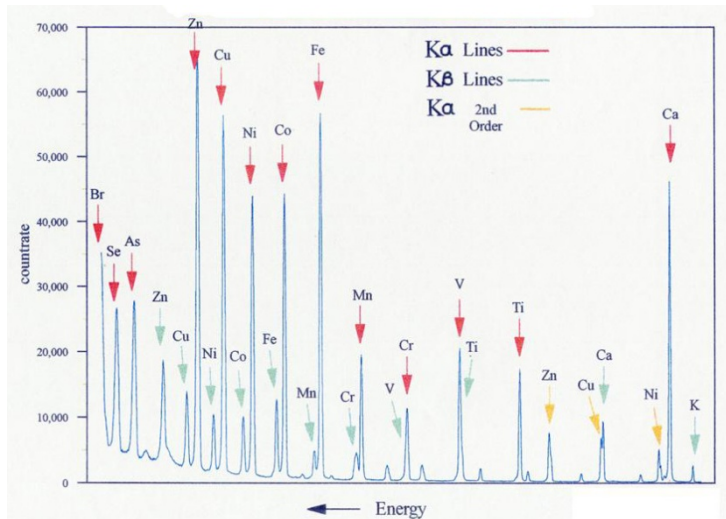
- The first set of tests focus on the part marking and is a resistance to solvents test
 - The markings should not smear or be removed by the solution.

■ Test for Resurfacing

- This test uses the same 3 devices, and consists of three separate chemical tests.
 1. Acetone Test,
 2. 1-Methyl 2-Pyrrolidinone Test, and
 3. Dynasolve 750 Test
- The inspection process is to look for indicators of package resurfacing and recoating.
- The 3 devices that pass this inspection are then to undergo the Delid Physical Analysis Inspection.

X-Ray Fluorescence

- X-ray Fluorescence (XRF) Spectroscopy
 - ❑ Tool for material composition detection
 - ❑ Can be a handheld instrument or a full lab system
 - ❑ Can be on external surfaces or de-lidded/de-capsulated
 - ❑ Non destructive
 - Destructive for internal material composition (e.g., wire bond, passivation, and metallization)
 - ❑ Sampling required.



■ Lead finish examination

- ❑ Shall be performed on the 3 sample devices
- ❑ Examined for Remarking and Resurfacing, to verify that the Lead Finish / Solder Ball & Column composition matches the device specifications or datasheet

■ Plating material(s) identification

- ❑ verify the plating layer thicknesses, presence of barrier materials, and possibly the base material

Delid Physical Analysis

■ The inspection

- ❑ Component's internal structure
- ❑ The top surface of a microelectronic die
- ❑ Metallization traces of a thin-film resistor

■ Apparatus & Equipment

- ❑ Chemical Decapsulation Process
 - Use of hazardous chemicals (Nitric acid and sulfuric acid)
- ❑ Mechanical Disassembly Tools
 - This includes cross-section tables and associates epoxy mounting material and other supplies, fine-tipped picks, x-acto blades, bladed saws, diamond wire saws, etc.
- ❑ Radiographic Tool
 - X-ray images
- ❑ Metallurgical Microscopes and Photodocumentation Equipment
- ❑ Scanning Electron Microscope (SEM), Energy Dispersive X-ray (EDX) tool

Description of the Procedure –Microcircuits, Hybrids, Diodes, and Transistors

- **External Optical Examination**
- **X-ray**
 - Images (top and side surface of the devices)
 - Information to be obtained for decapsulation (x-ray images to be 1:1 ratio – the die location within the case)
- **Decapsulation of Plastic Parts and Delidding of Cavity Devices**
 - Plastic Parts
 - Nitric acid and sulfuric acid
 - Manual delidding of ceramic devices
 - Two types of ceramic devices
 - two ceramic plates sandwiched around a glass seal (“cerdip” tool).
 - hermetically sealed metal cover that is soldered in place over the die area (x-acto knife)
 - Care to be taken to expose the die without damaging the other internal structures (bond pads, bond wires, lead frame, die attach material, substrate, etc.)

Description of the Procedure –Microcircuits, Hybrids, Diodes, and Transistors-Cont

■ Inspection and photodocumentation

- Overall photo of the decapsulated device shall be obtained. Also obtain a higher magnification photo showing only the die (up to a minimum of 500x). Inspect the die for the information listed below.
 - Manufacturer markings
 - Name and Logo
 - Unique Die part numbers
 - Die mask ID numbers
 - Year of design
 - Bond types
 - Any other markings or features that may help in identifying the origins of the die.

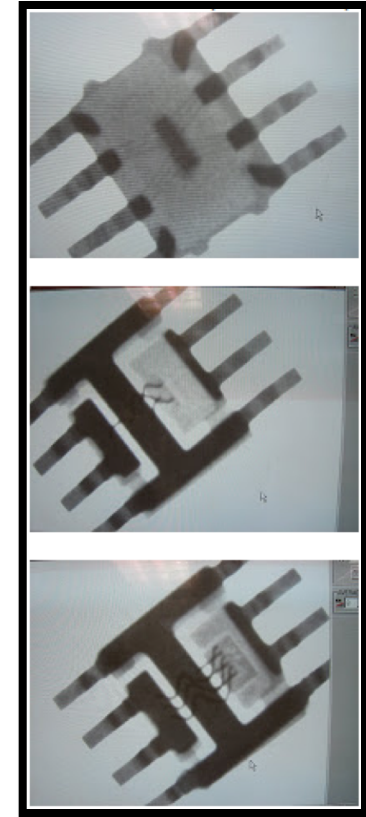
Risk Level Inspection Test

	Critical Risk	High Risk	Moderate Risk	Low Risk
	4	3	2	1
Optically Inspect/Photo document	X	X	X	X
Wire Pull	X	X	X	(optional)
Die Shear (hermetic)	X	X	(optional)	(optional)
Ball Shear	X	X	(optional)	(optional)
SEM Inspection	X	(optional)	(optional)	(optional)
Perform EDX	X	(optional)	(optional)	(optional)
Delayer/Inspect Metalization	X	(optional)	(optional)	(optional)
Glassivation Layer Integrity Testing	X	(optional)	(optional)	(optional)

X-Ray Inspection

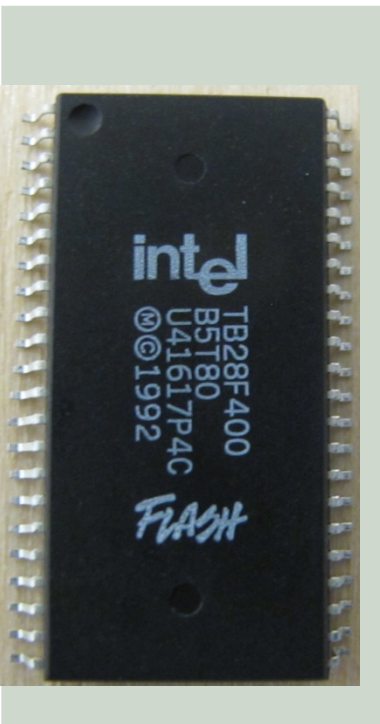

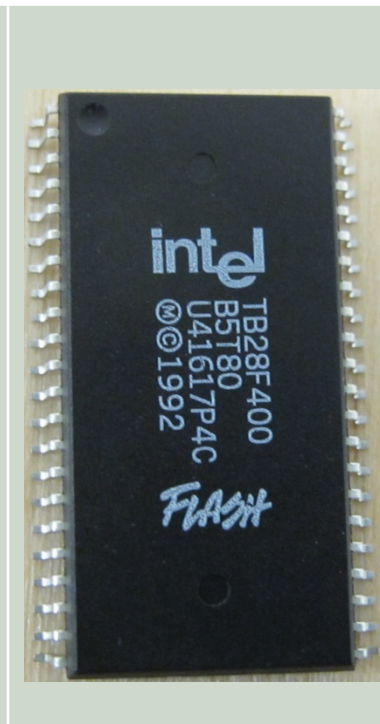
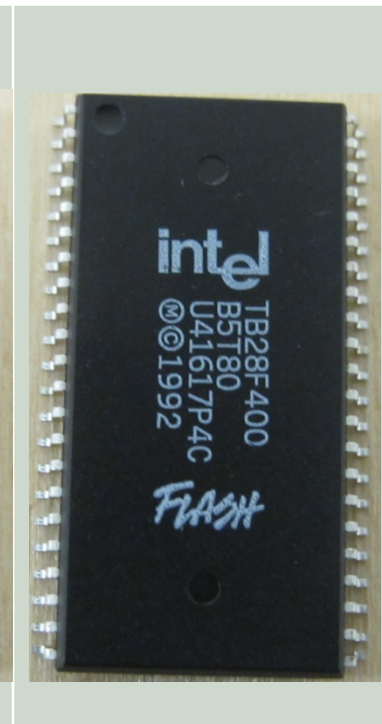
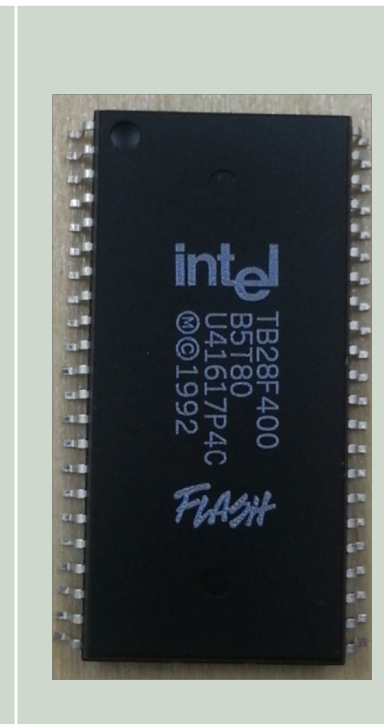
Determines:

- If the package contains a die
- Consistent size/shape of the die
- Consistent internal construction
- If the die has all wire bonds attached
- Exact die and bond wire location
 - To avoid damage during decapsulation



"The value of X-ray is increased when there is a known good OCM device available for comparison of internal details" —CCAP-101 Certified Document Rev D

Low Power Visual Inspection

Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
				

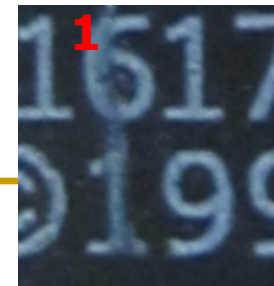
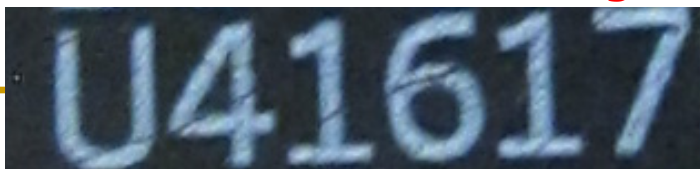
Observations:

All Samples look the same at Camera level

Except for :

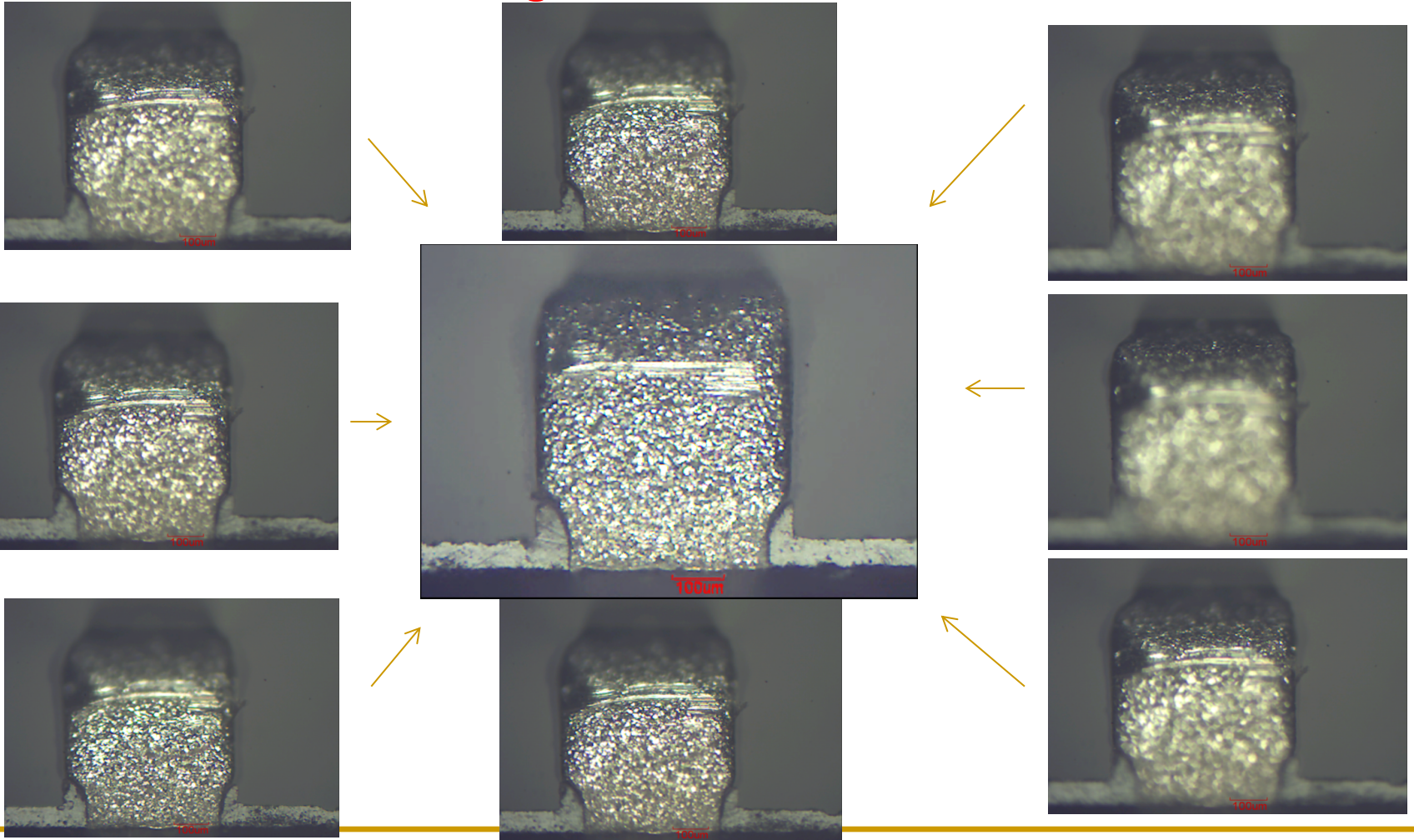
Sample 3 has a scratch on markings starting with U

Sample 2 scratch on marking over numbers 6 and



Optical Microscope + Z stack Improved Depth of field

All optical microscope image shown is the reconstruction of at least 8 images at different focus

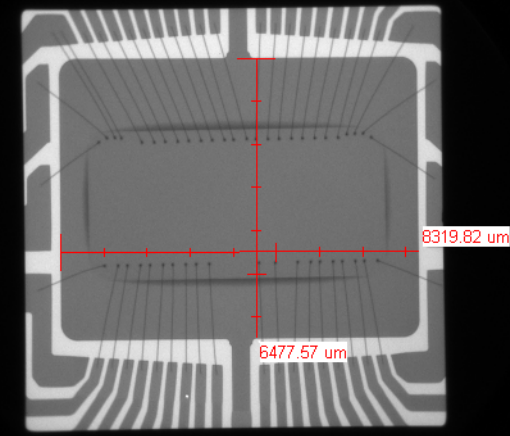
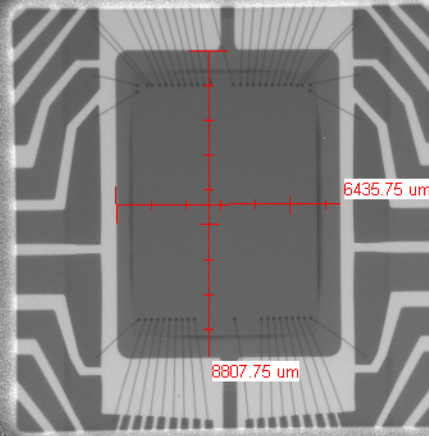
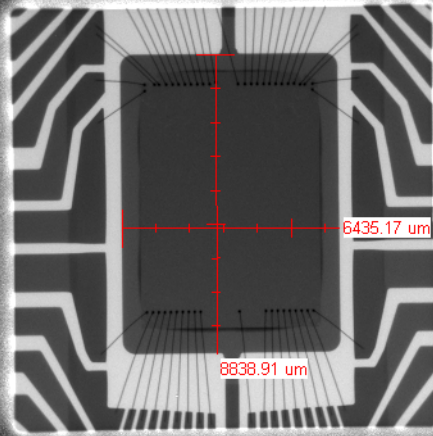


2D X-ray Radiography

Sample 1

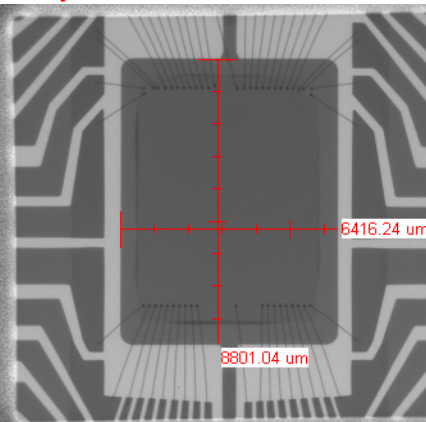
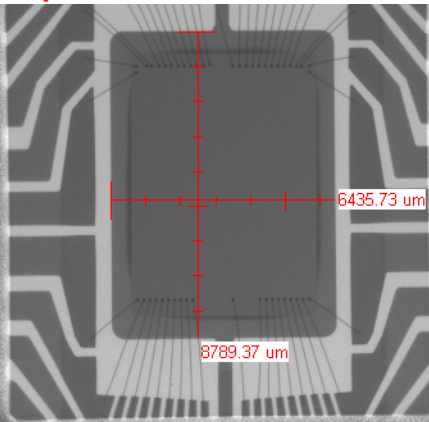
Sample 2

Sample 3



Sample 4

Sample 5



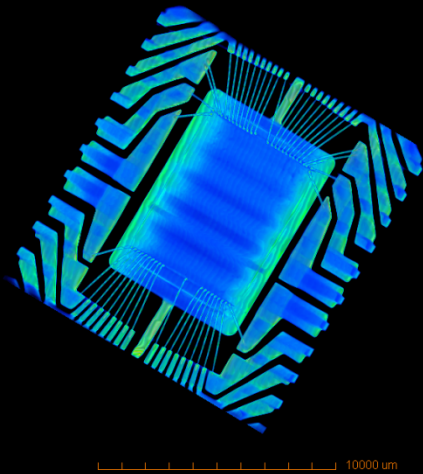
Observation:

Sample 3 has a different Die and bond wires

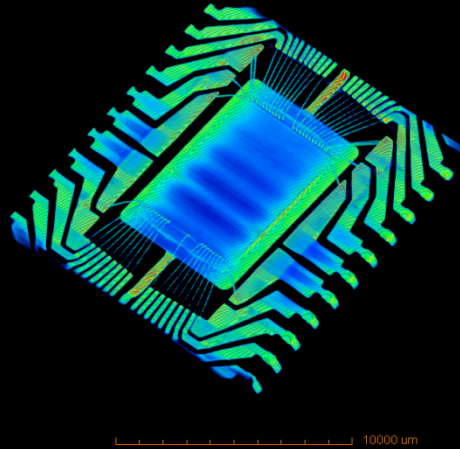
Samples 1,2,4,5 look very similar

3D X-ray Tomography

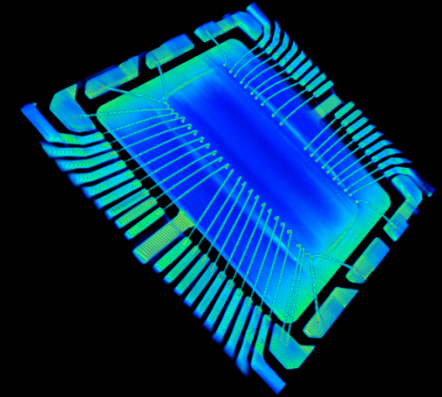
Sample 1



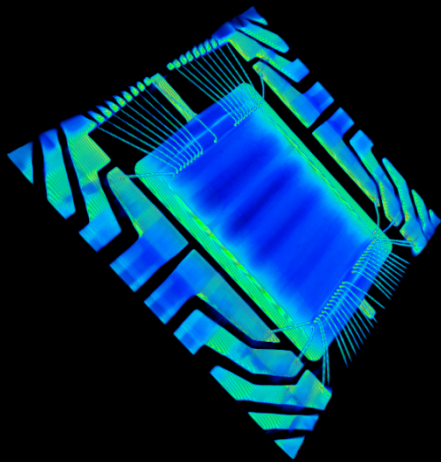
Sample 2



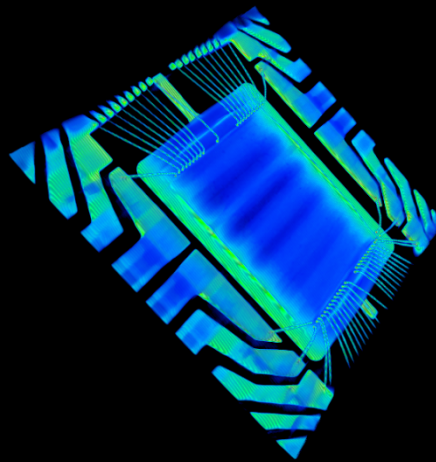
Sample 3



Sample 4



Sample 5



Observation:

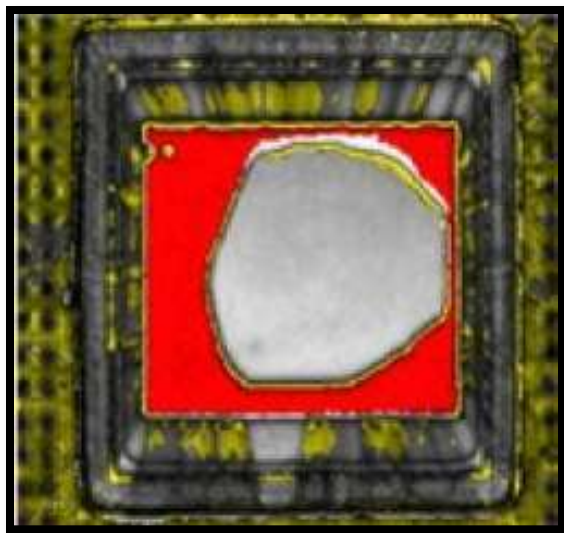
All connections are Checked and look fine on all samples

Sample 3 lacks One connection which is believed to be the ground wire.

(possible grade issue)

Scanning Acoustic Microscopy

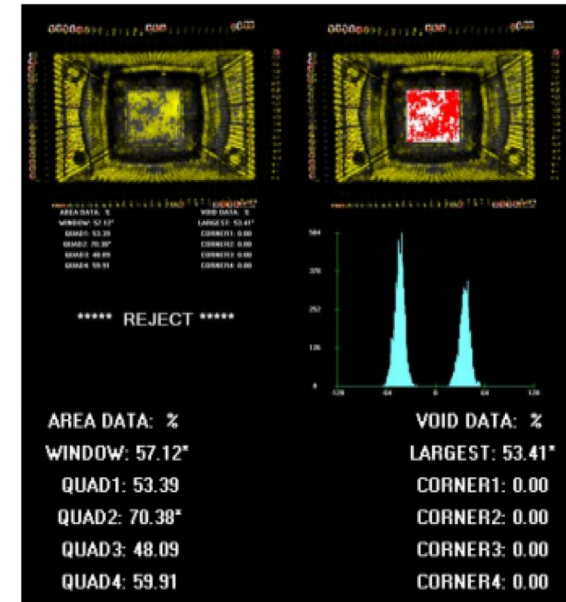
- Acoustic is non-invasive
 - Reveal cracks, voids, and delamination
 - Non destructive die inspection
 - Uses de-ionized water or IPA as medium



Red areas indicate delamination

Sonoscan

C-SAM® Series – Model Gen6™
(Advanced C-SAM® System for Laboratory Environments)



MuAnalysis *look deeper*

Electrical Tests

- Mainly focus on large scale integrated circuits
 - Microprocessor, Memory, and Programmable Logic chips account for almost 35% of counterfeits
- As these are high cost parts, counterfeiter will probably put much effort to counterfeit and physical detection will be extremely difficult (merely impossible)
- No definite test methodology either electrical or physical (without destroying the chip) to detect counterfeit with 100% confidence level.

Electrical Tests

■ Tester

□ ATE (Automated Test Equipment)

■ Specification:

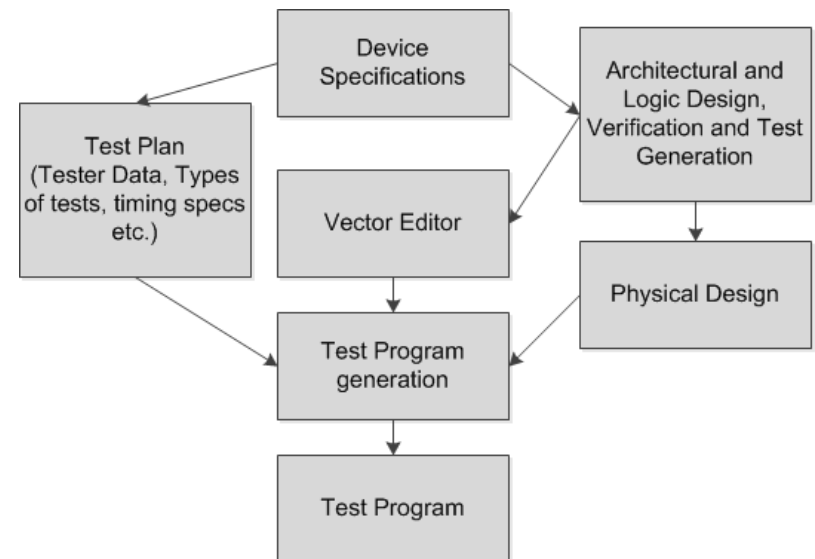
- Speed (clock rate of the device)
- Timing (strobe) accuracy
- Number of input/output pins, etc.



■ Test Programming

■ Limitation

- HDL description of test module must be available to test ICs
- No definite methodology to detect counterfeit ICs



Recycled Parts: Aging

- Recycled parts are around 80% of total counterfeit parts.
- Most of the defects in recycled parts are due to aging.
- Aging
 - Negative bias temperature instability (NBTI)
 - NBTI occurs in p-channel MOS devices stressed with negative gate voltages and elevated temperature due to the generation of interface traps at the Si-SiO₂ interface
 - Hot carrier injection (HCI)
 - HCI occurs in NMOS devices caused by the trapped interface charge at Si=SiO₂ surface near the drain end during switching
 - Time-dependent dielectric breakdown (TDDB)
 - The carrier injection with high electric field leads to a gradual degradation of the oxide properties which eventually results in sudden destruction of the dielectric layer
 - Electromigration
 - Mass transport of metal film conductors stressed at high current densities

Parametric Test

■ DC Parametric Test

- ❑ Contact Test
- ❑ Power Consumption Test
- ❑ Leakage Test
- ❑ Output Short Current Test
- ❑ Output Drive Current Test
- ❑ Threshold Test

■ AC Parametric Test

- ❑ Propagation delay test
- ❑ Setup/hold time test
- ❑ Access time test
- ❑ Rise and fall time test

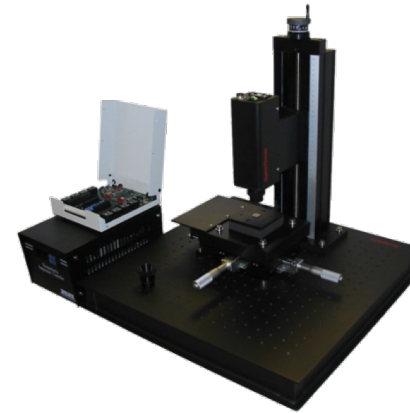
Functional Tests

■ Functional testing

- ❑ The most efficient way of verifying the functionality of a component.
- ❑ Function Verification of a Component
 - Determines whether individual components, possibly designed with different technologies, function as a system and produce the expected response.
- ❑ Memory Tests
 - Read/write operations are performed on a memory to verify its functionality. MARCH tests can be applied for counterfeit detection.
- ❑ Microprocessor Tests
 - Microprocessors are binned in different groups depending on the maximum functional frequency (f_{\max}).

Temperature Cycling/ Burn-In

- Testing the chip at extremes of operating range
- Tester Ranges:
 - ❑ Military Grade: -65°C to 175°C
 - ❑ Industrial Grade: -25°C to 85°C
 - ❑ Commercial Grade: -10°C to 70°C
- Burn-in
 - ❑ The device is operated at an elevated temperature (Stressed condition)
 - ❑ To find infant mortality failures and unexpected failures to assure reliability.
 - ❑ Test methods
 - MILSTD-883 for integrated circuits and
 - MIL-STD-750 for other discrete components.
 - ❑ Very useful as it can easily weed out the commercial grade components marked as military grade.
 - ❑ Can remove defective components or those components that were not designed to perform over the stressful conditions.



OptoTherm

Structural Tests

■ At-speed tests

- ❑ To detect gross and spot delay defects
- ❑ Transition delay fault test / Path delay fault test

■ Stuck-at tests

- ❑ To detect spot delay defects

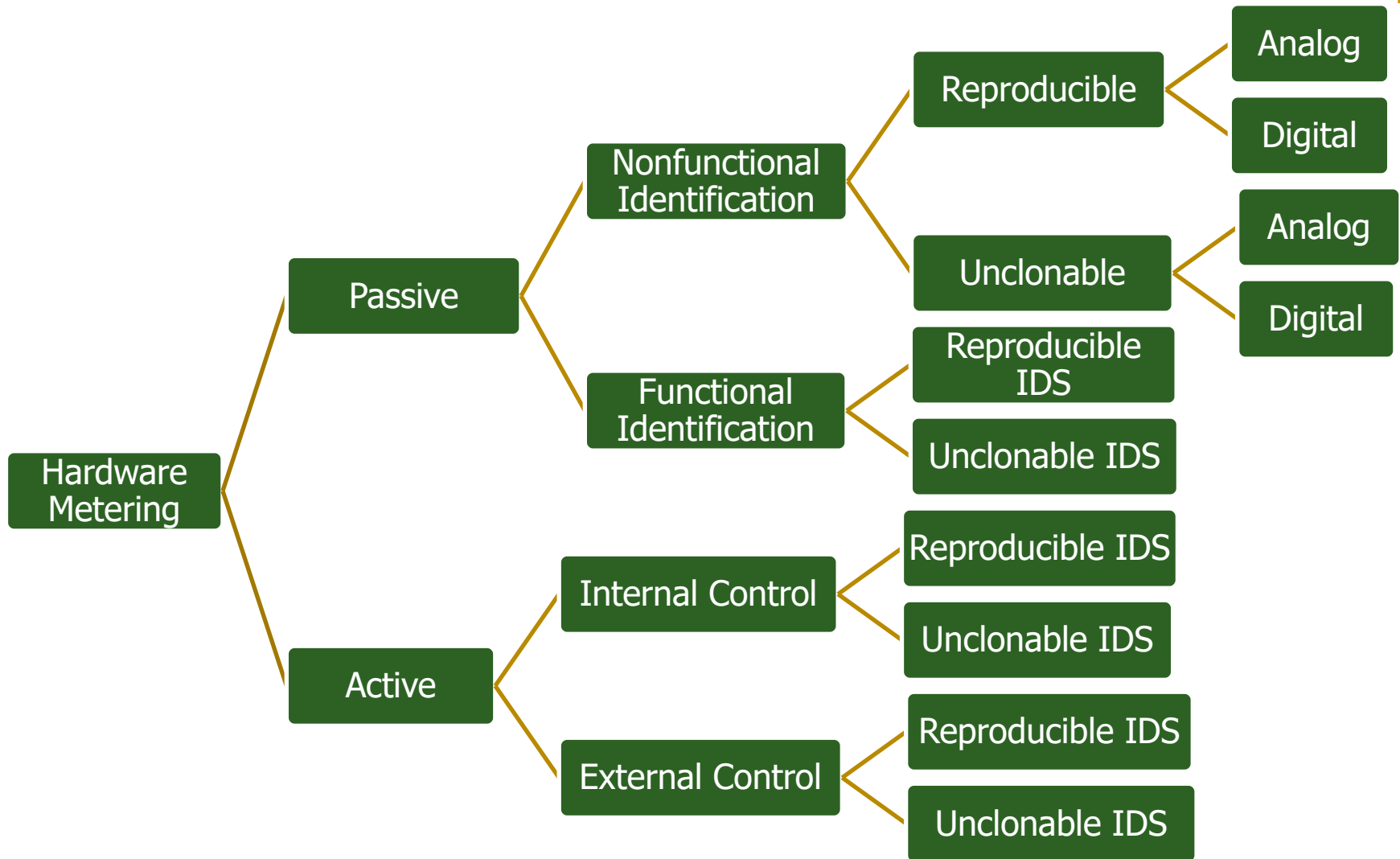
■ Bridging tests

- ❑ To detect physical bridging defects

Hardware Metering

- Is a set of security protocols that enable the design house to achieve post-fabrication control over their ICs.
- Provides a way to uniquely fingerprint or tag each chip and/or each chip's functionality
 - It is possible to distinguish between the different chips manufactured by the same mask.
- First introduced in 2005
 - To uniquely tag each ICs functionality

Taxonomy [6]



Hardware Metering

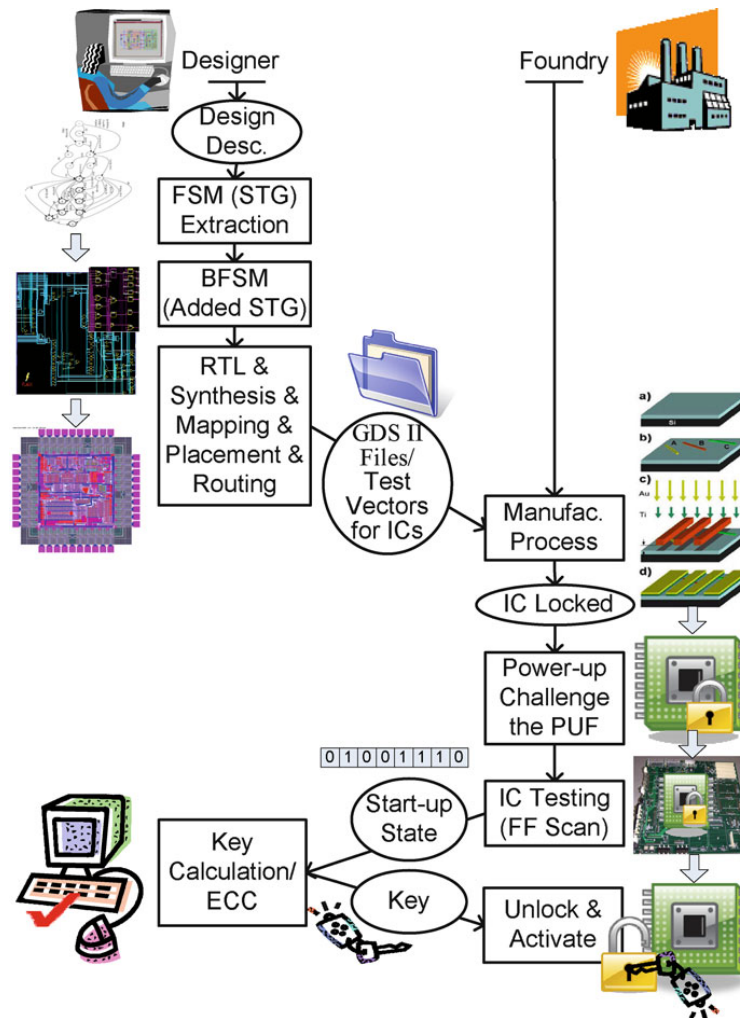
■ Passive IC Metering

- ❑ IDs on the package
- ❑ IDs stored in memory
 - Intel Pentium III Processor (PSN: Processor Serial Number)
- ❑ Unclonable Identifiers
 - Generate IDs utilizing process variations

■ Active IC Metering

- ❑ Uniquely and unclonably identifies each chip
- ❑ Provides an active mechanism to control, monitor, lock, or unlock the ICs after post fabrication

IC Enabling by Active Metering



Physical Unclonable Functions (PUFs)

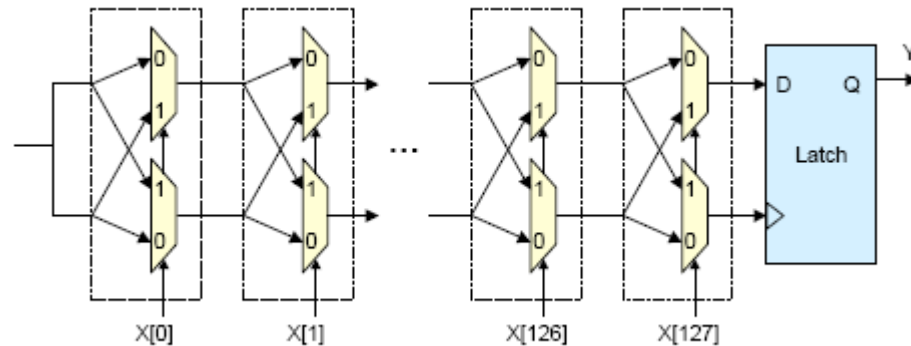
- To derive secrets from complex physical characteristics of ICs rather than storing the secrets in digital memory.
- Extremely difficult to predict or extract the secret as PUFs utilize the random process variation to generate the secret.
- PUFs generate volatile secrets (only exist in a digital form when a chip is powered on and running)
 - Harder for an invasive attack (must accurately measure PUF delays while power on)

PUF

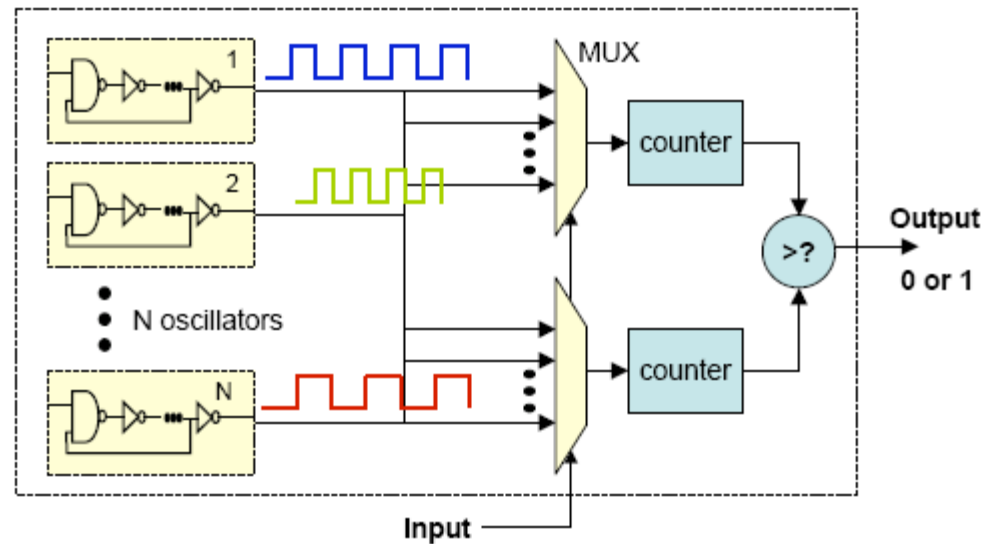
- Is a function that maps a set of challenges to a set of responses based on a complex physical system
- The function
 - Can only be evaluated with the physical system
 - Is unique for each physical system because of random process variation.

PUFs

Arbiter PUF



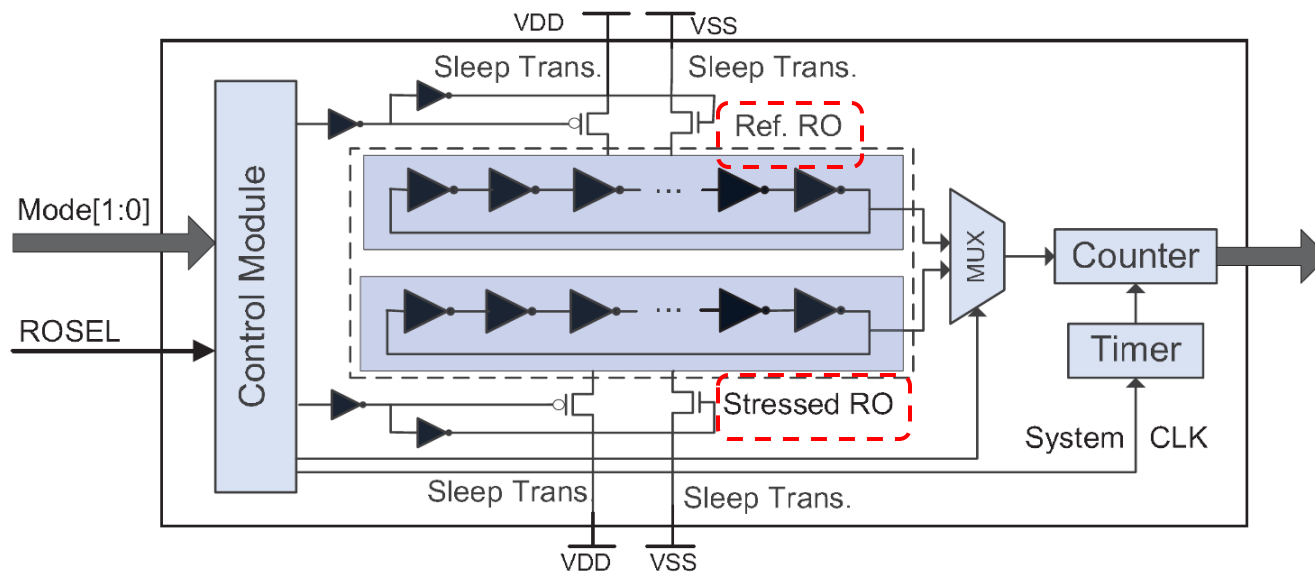
RO PUF:



CDIR Sensor

■ Combating Die/IC Recovery (CDIR) sensor

- Ref. RO and Stressed RO
- Test Mode: Ref. RO and Stressed RO are both off
- Function Mode: Ref. RO is off while Stressed RO is on
- Measurement Mode: RO and Stressed RO are both on



Baseline CDIR Structure

References

- [1] National Defense Authorization Act. United States Congress, 2011.
- [2] R. K. Lowry, “Counterfeit electronic components – an overview,” Presented at the Military, Aerospace, Spaceborne, and Homeland Security (MASH) Workshop, 2007.
- [3] “Top 5 Most Counterfeited Parts Represent a \$169 Billion Potential Challenge for Global Semiconductor Market,” <http://press.ihs.com/pressrelease/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha>.
- [4] “IHS,” April 2012,
<http://www.era.com/presentations/General%20Session%201/Leading%20up%20to%20HR%201540%20National%20Defense%20Authorization%20Act%20for%20Fiscal%20Year%202012.pdf>
- [5] L. W. Kessler and T. Sharpe, “Faked Parts Detection,” 2010,
<http://www.circuitsassembly.com/cms/component/content/article/159/9937-smt>.
- [6] M Tehranipoor, “Introduction to Hardware Security and Trust”
- [7] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation”, DAC , vol. 6, pp. 9-14, 2007