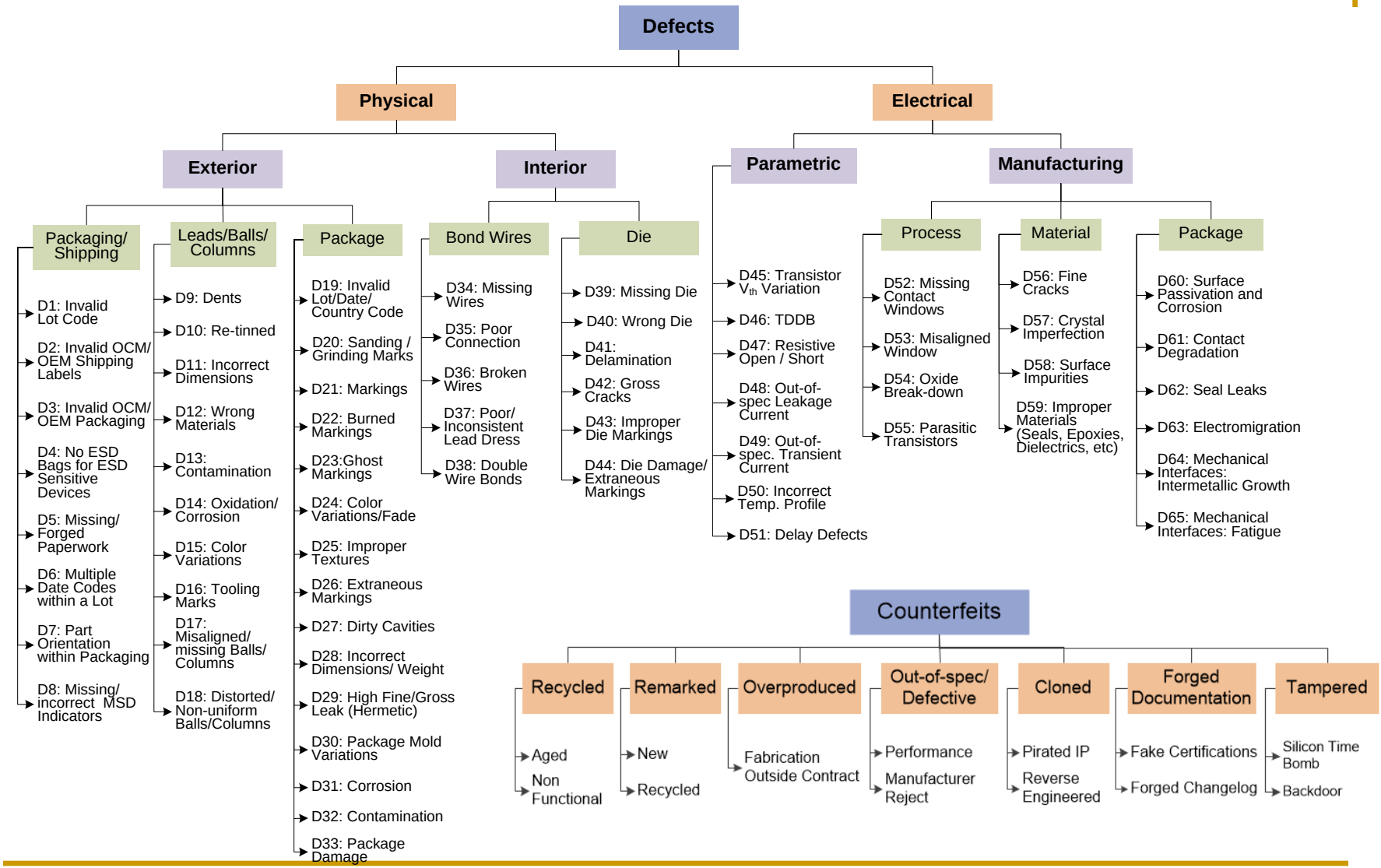
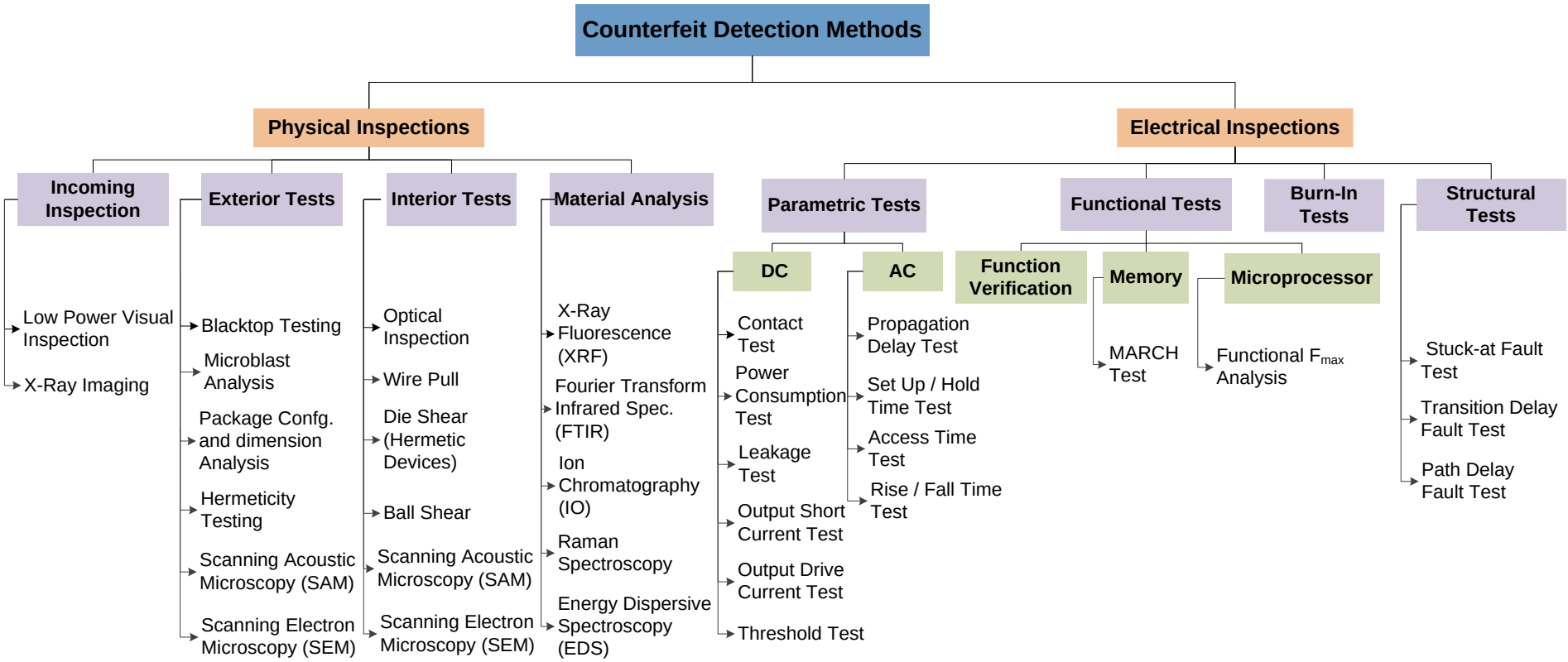
Counterfeit Defect Taxonomy



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:

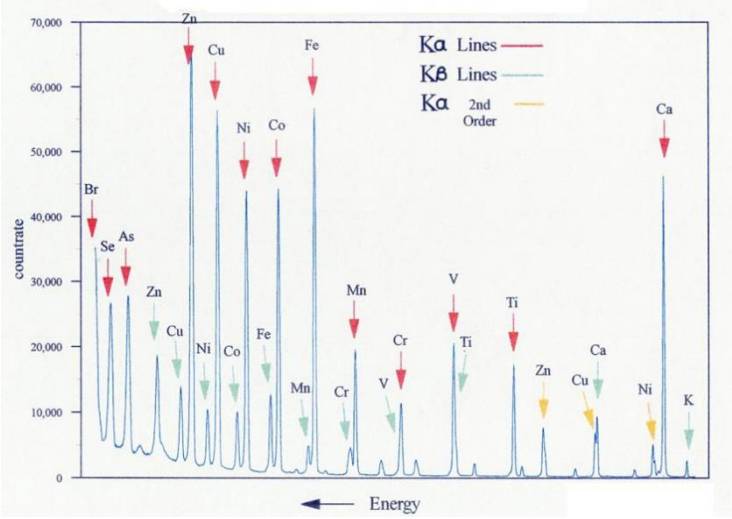
- Date and Lot Codes
- Low Power Microscopy
- High Power Microscopy
- OEM Shipping labels
- Lead quality
- Dimensions & Weight
- Marking Quality

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.



XRF-Cont.

- **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.

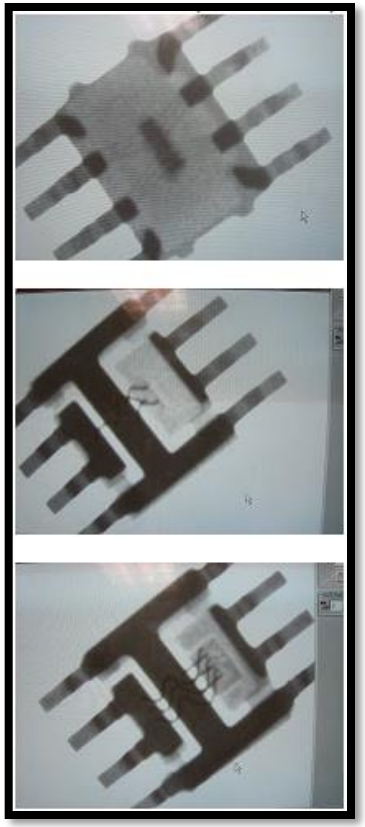
Risk Level Inspection Test

	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

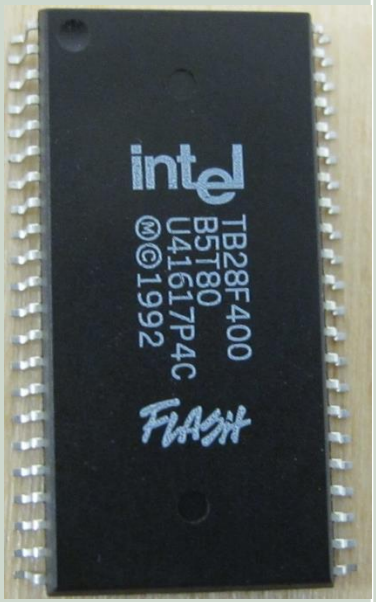
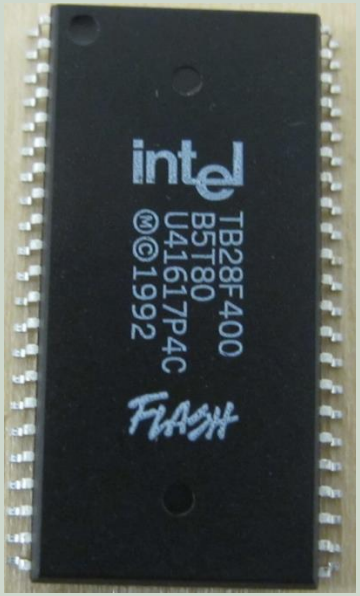
Determines:

- 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
				

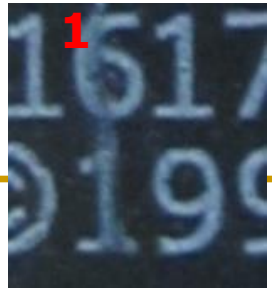
Observations:

All Samples look the same at Camera level

Except for :

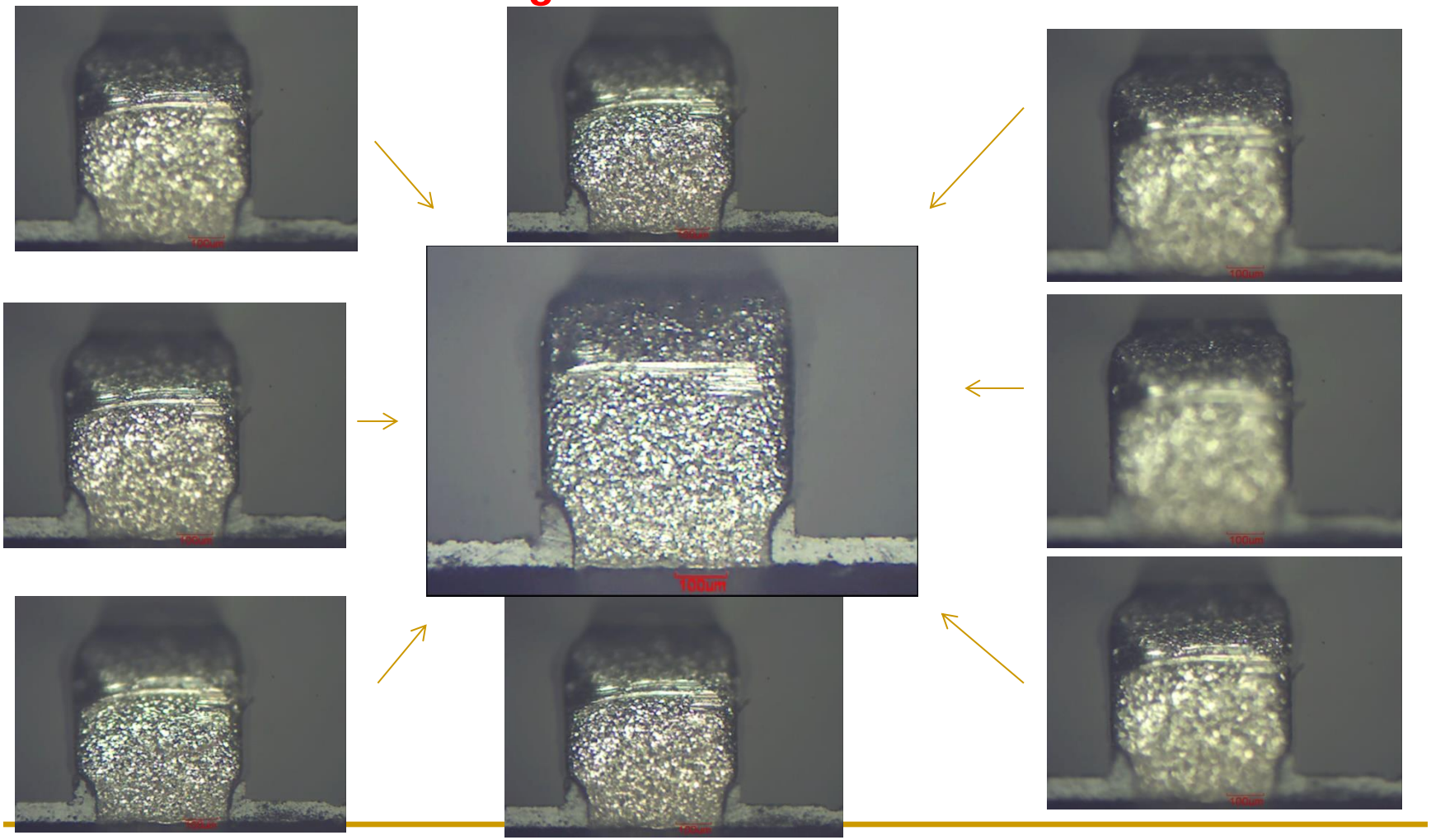
Sample 3 has a scratch on markings starting with U

Sample 2 scratch on marking over numbers 6 and 1



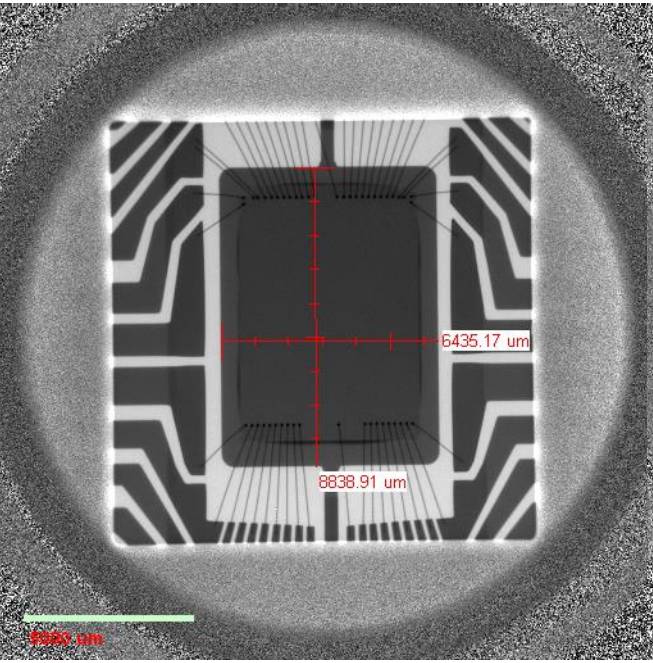
Optical Microscope + Z stack Improved Depth of field

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

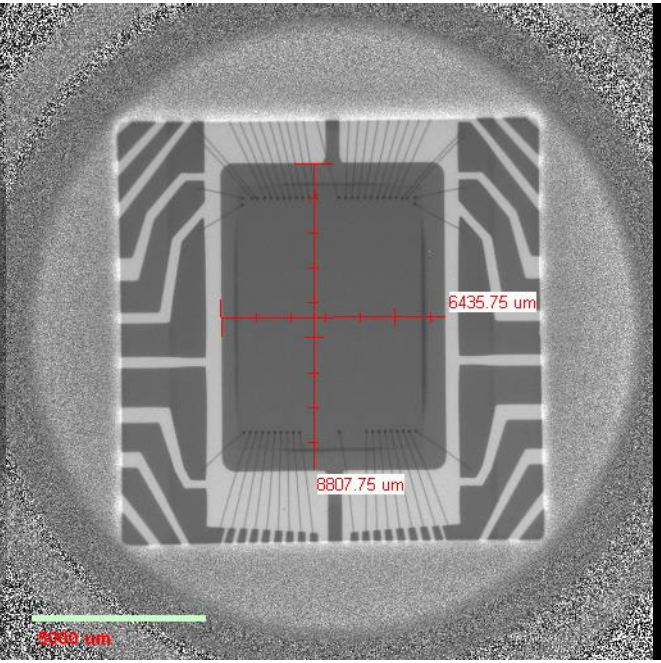


2D X-ray Radiography

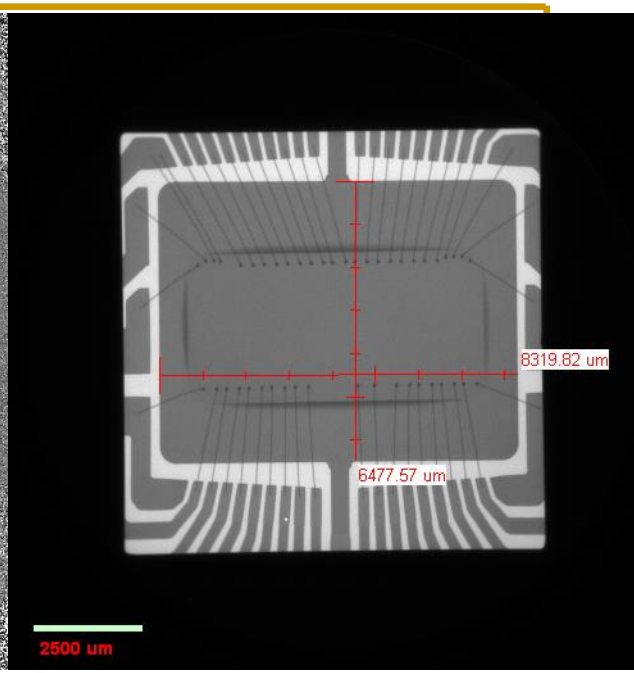
Sample 1



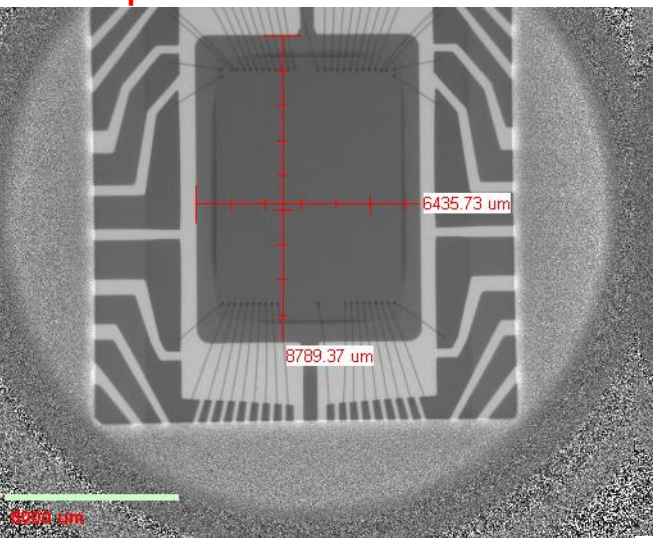
Sample 2



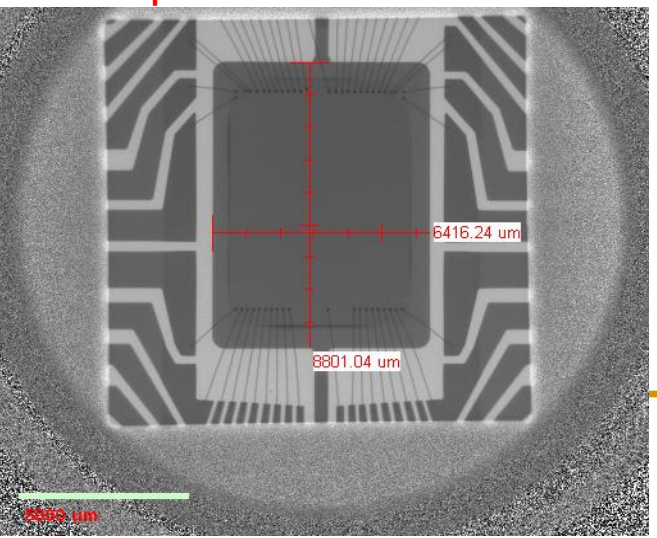
Sample 3



Sample 4



Sample 5



Observation:

Sample 3 has a different Die and bond wires

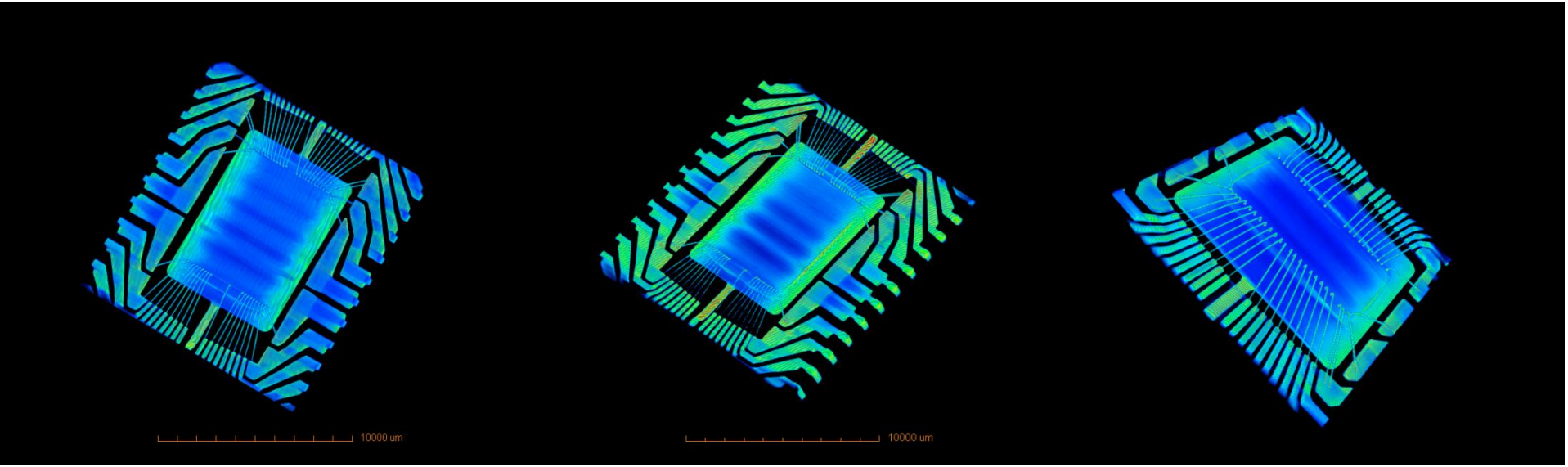
Samples 1,2,4,5 look very similar

3D X-ray Tomography

Sample 1

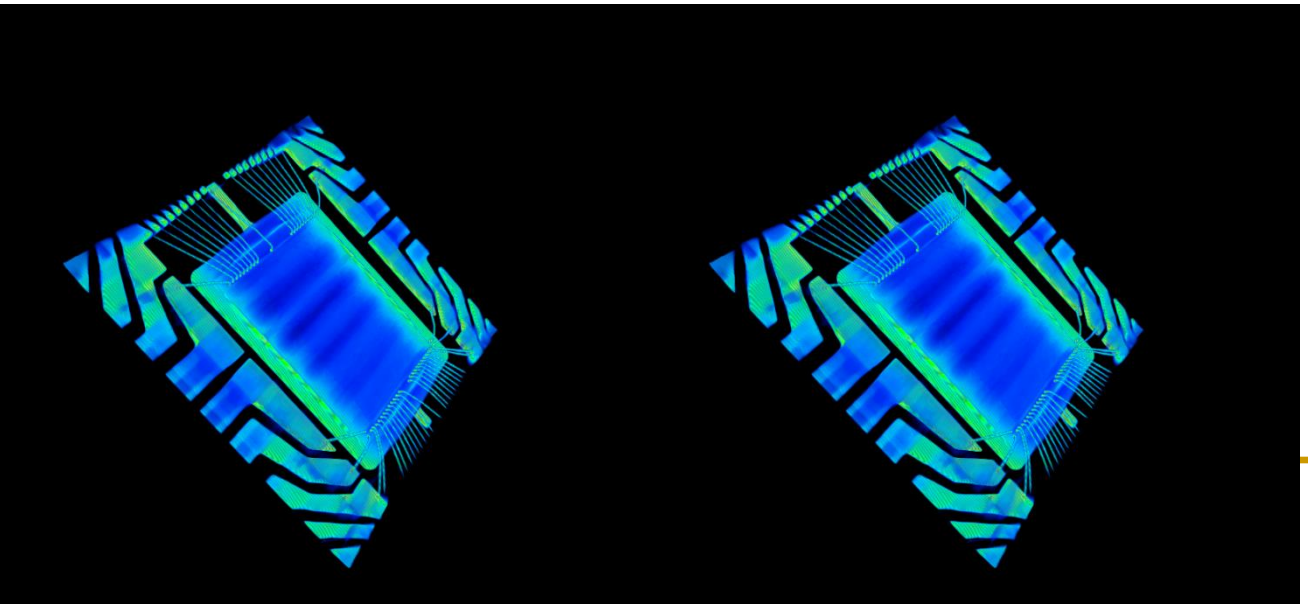
Sample 2

Sample 3



Sample 4

Sample 5



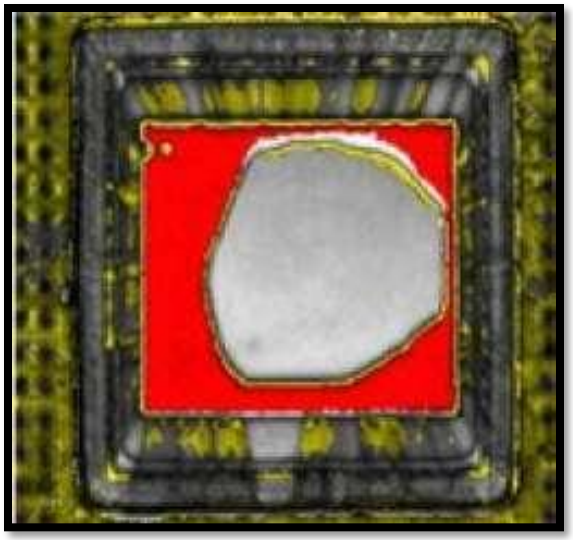
Observation:

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



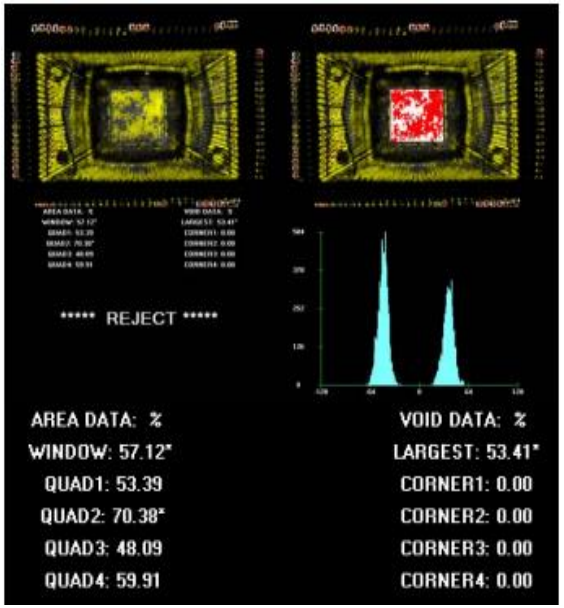
MuAnalysis look deeper

Red areas indicate delamination

Sonoscan

C-SAM® Series – Model Gen6™

(Advanced C-SAM® System for Laboratory Environments)

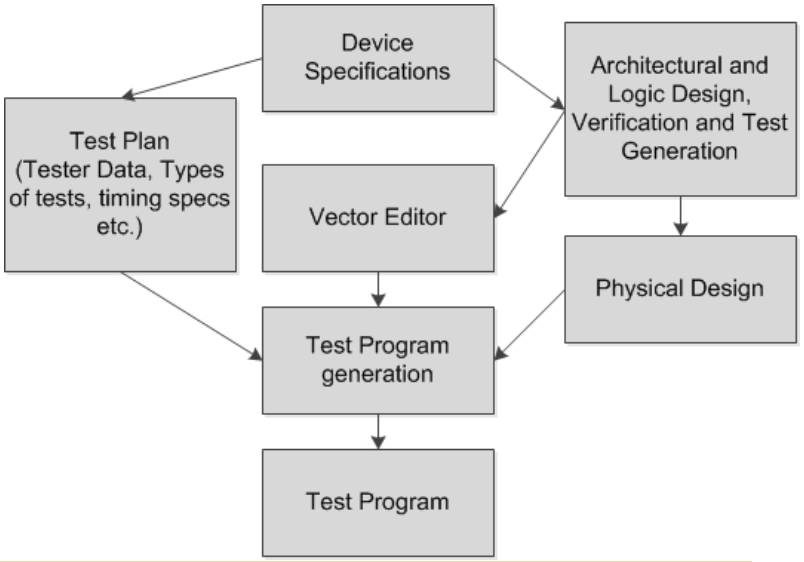


Electrical Tests

- 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-SiO_2 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

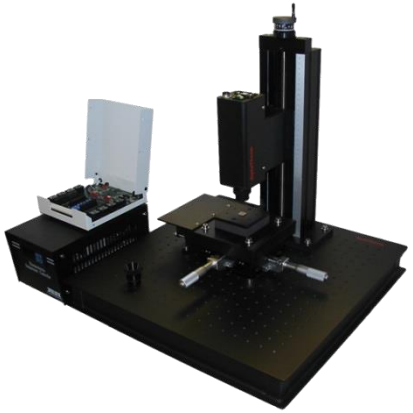
- **DC Parametric Test**
  - Contact Test
  - Power Consumption Test
  - Leakage Test
  - Output Short Current Test
  - Output Drive Current Test
  - Threshold Test
- **AC Parametric Test**
  - Propagation delay test
  - Setup/hold time test
  - Access time test
  - Rise and fall time test

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.

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

Hardware Metering

- Passive Metering
  - Provides a way for unique identification of a chip, or for specifically tagging an IC’s functionality so that it can be passively monitored.
- Active metering
  - In addition to unique identification or remote passive monitoring of a device, provides an active way for the designers to enable, control, and disable the device.

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

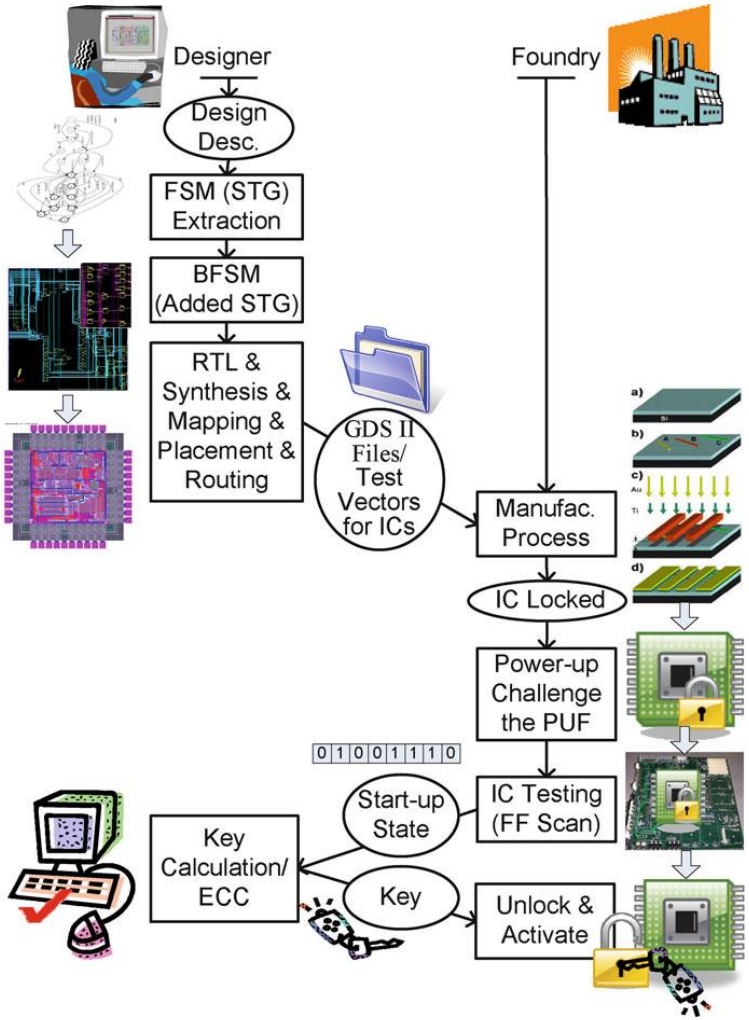
IC Enabling by Active Metering

- The designer (design house) holds the IP rights and the Foundry manufactures the ICs.
- The designer inserts a lock in their high level design description and the design goes through subsequent design phases (RTL, synthesis, mapping, layout, and placement).
- The foundry receives
  - Blue-print in the form of OASIS files (or GDS-II)
  - Other information
  - Test vectors

IC Enabling by Active Metering

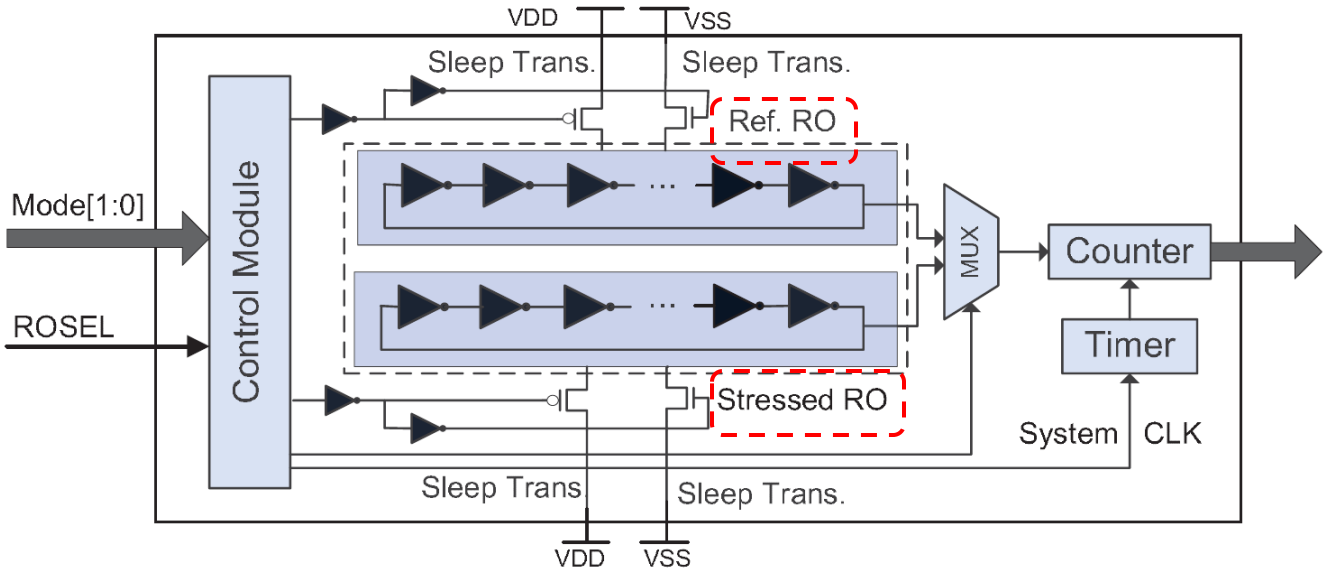
- During the start-up test phase
  - Fab scans the unique identifier information out of each IC and sends the content to design house.
  - Design house compute the unlocking sequence depending on the cryptographic protocol.
  - The designer compute the error correcting code (ECC) to correct for any further changes to the unclonable digital identifiers.
  - The un-locking sequence is send to the fab for unlocking the ICs.

IC Enabling by Active Metering



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