ECE 459/559
Secure & Trustworthy Computer Hardware Design

Counterfeit Taxonomy and Detection

Garrett S. Rose
Spring 2017

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Recap

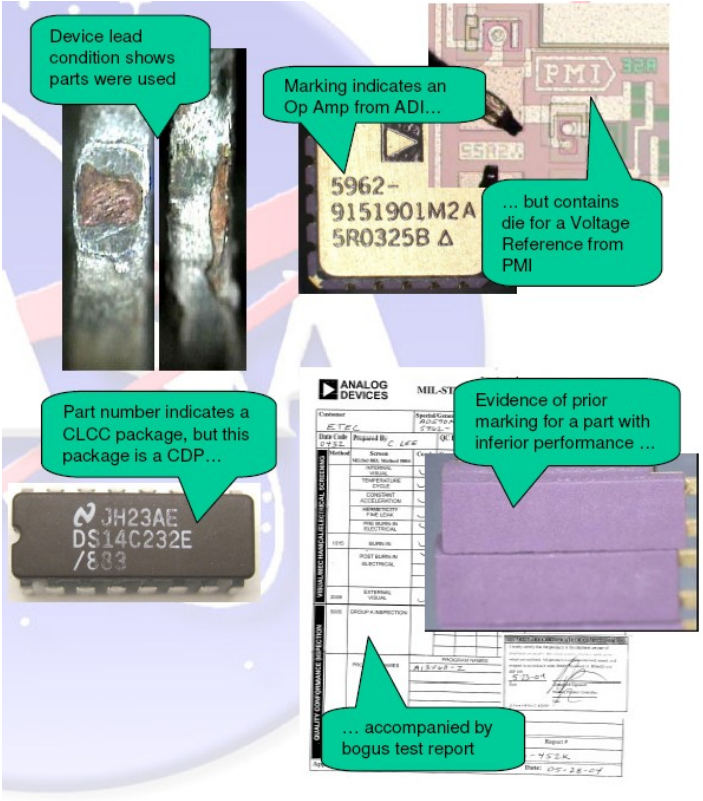
- “Bird's eye view” of integrated circuit design
  - Transistors as switches
  - Static CMOS circuits
- Top-down design flows
  - VHDL to silicon

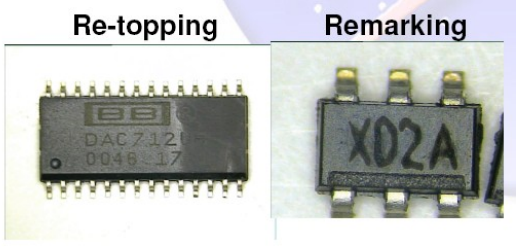
What Motivates Counterfeiting?

- 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 supply chain of nation's defense system
  - To contaminate a company's reputation
  - To kill market share for a company
  - More …

Counterfeit Electronic Parts

- Parts remarked or re-topped
- Defective parts scrapped by OCM (Original component manufacturer)
- Previously used parts salvaged from scrapped assemblies
- Devices refurbished, but represented as new product
- Overproduced parts by foundry
- Cloned IP or IC
- Forged documentation Misrepresentation of IC
- Manufacturer reject





THE UNIVERSITY OF TENNESSEE KNOXVILLE

A Counterfeit Component …

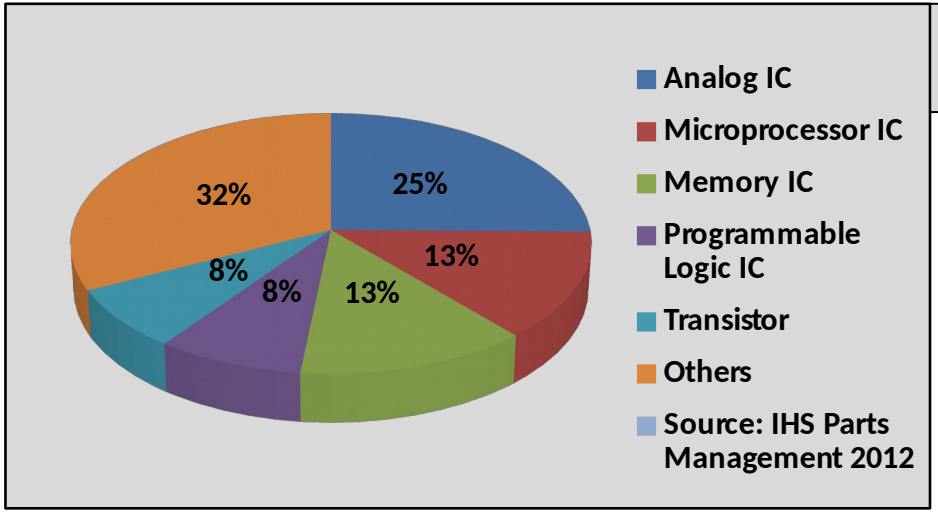
- Is an unauthorized copy,
- Does not conform to OCM design, model, or performance standards,
- Is not produced by the OCM,
- Is out-of-specification, defective, or used product sold as new
- Has incorrect or false markings or documentation, or
- Is produced or distributed in violation of intellectual property rights, copyrights, or trademark laws

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.

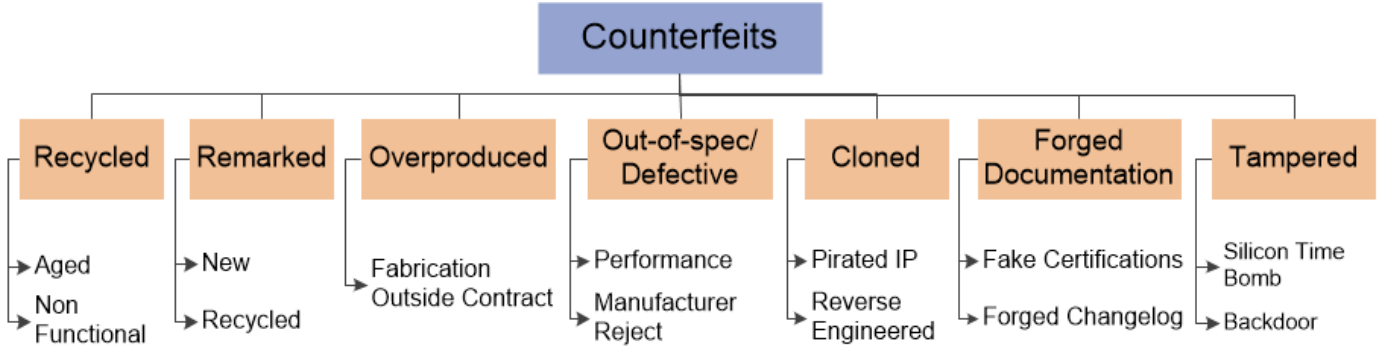


IHS reports a $169B annual risk

Top Part Type Reported in Counterfeit Incidents	Industrial Market	Automotive Market	Consumer Market	Wireless Market	Wired Market	Compute Market	Other
	Where Used →						
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 incidents
- Untrusted foundry/assembly can introduce overproduced and out-of-spec/defective parts
- Cloning can be done by wide variety of adversaries (from small entity to large corporation)
- Tampered parts act as a backdoor to secret information from chip or for sabotage of system functionality

Recycled Parts

- More than 80% of counterfeit components are recycled*
- In 2005, the U.S. only properly recycled 10-18% of all electronic waste – number rose to 25% by 2009
- Most recycled parts are at the end of life
  – Damaged considerably due to usage and aging
- Recycled parts
  - Genuine OCM part manufactured and used in some equipment, device or gadget for period of time
  - User discards device for any number of reasons
  - Scrap devices broken down into bare circuit boards and components
  - Crudely extracted from boards, prepared for resale

*L.W. Kessler and T. Sharpe, “Faked Parts Detection,” Circuits Assembly, 2010.

IC Recycling Process

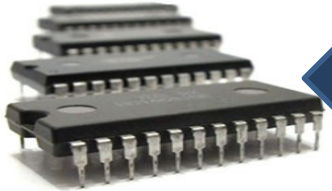
A recycling center

PCBs taken off of electronic systems

ICs taken off PCBs

Refine recycled ICs

Resold as new



Critical Application

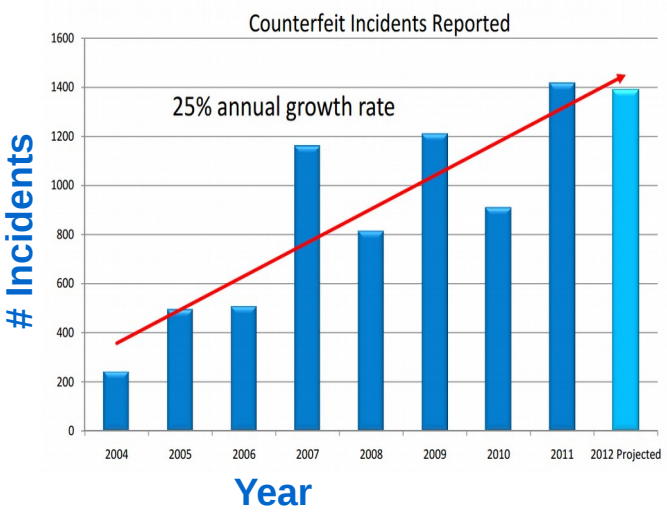
Identical:
Appearance, Function, Specification

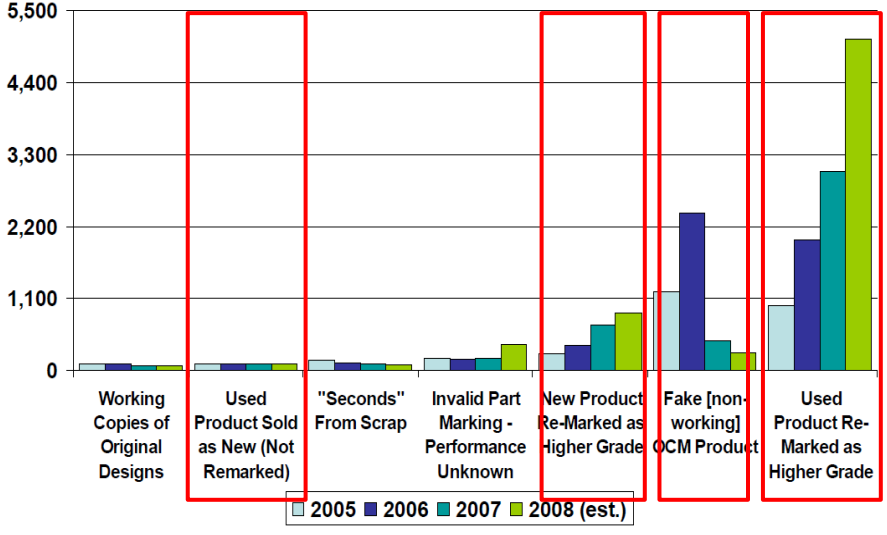
Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Recycled and Remarked ICs

- Recycling and remarking of ICs have become major security and reliability problems
- IC recycling: $9B – $15B per 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

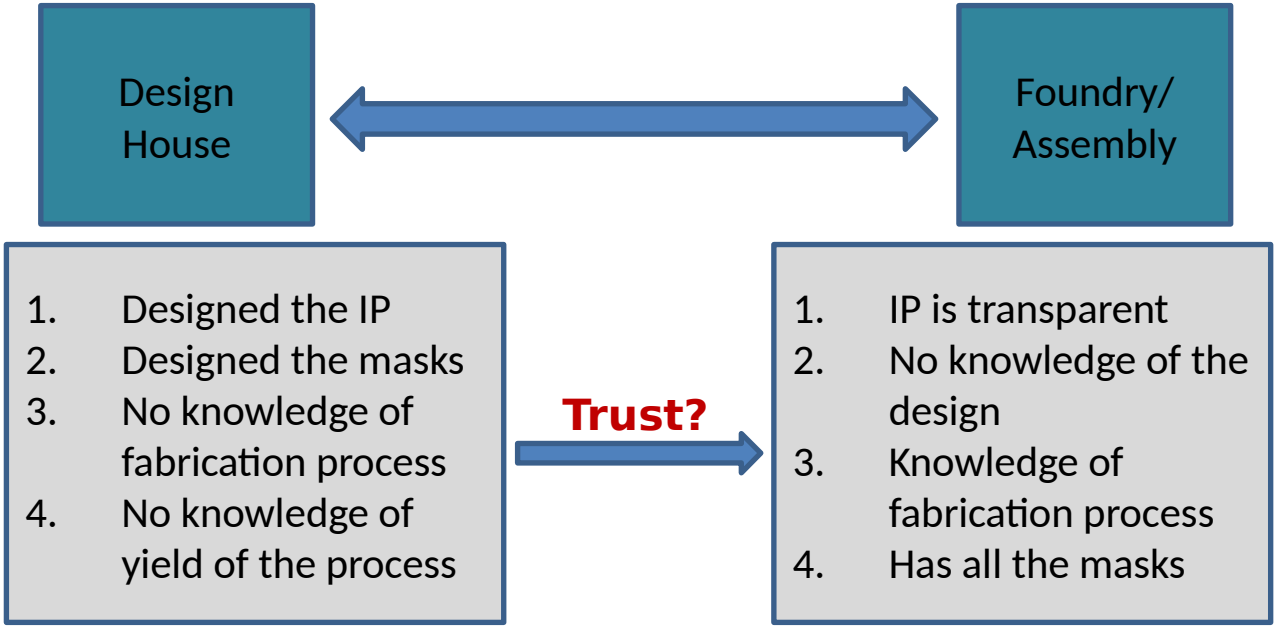
- Two types of remarking parts:
  - Recycled components
  - New components
    - Change specification of component (commercial grade → military grade)
- Remarking process
  - Packages sanded or ground down to remove old markings
  - New coating is created and applied to the parts
    - Thermal or UV-cured epoxy

Remarking Example

Overproduction

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

Overproduction



- Foundry can produce more parts than ordered
  - Fabricate the yield data and sell extra chips to market
  - Can produce extra chips without sending information to design house

Out-of-Spec/Defective

- Foundry can sell:
  - Defective Parts
    - Chip may fail one particular structural test pattern
    - Highly unlikely that defect will appear in normal operation of chip in first few hours or days or months
    - Eventually, it will fail at some point in time
  - Out-of-Spec Parts
    - Fail to perform at design specification (leakage current, dynamic current, performance, etc.)
    - Chip might fail at extreme physical/environmental conditions

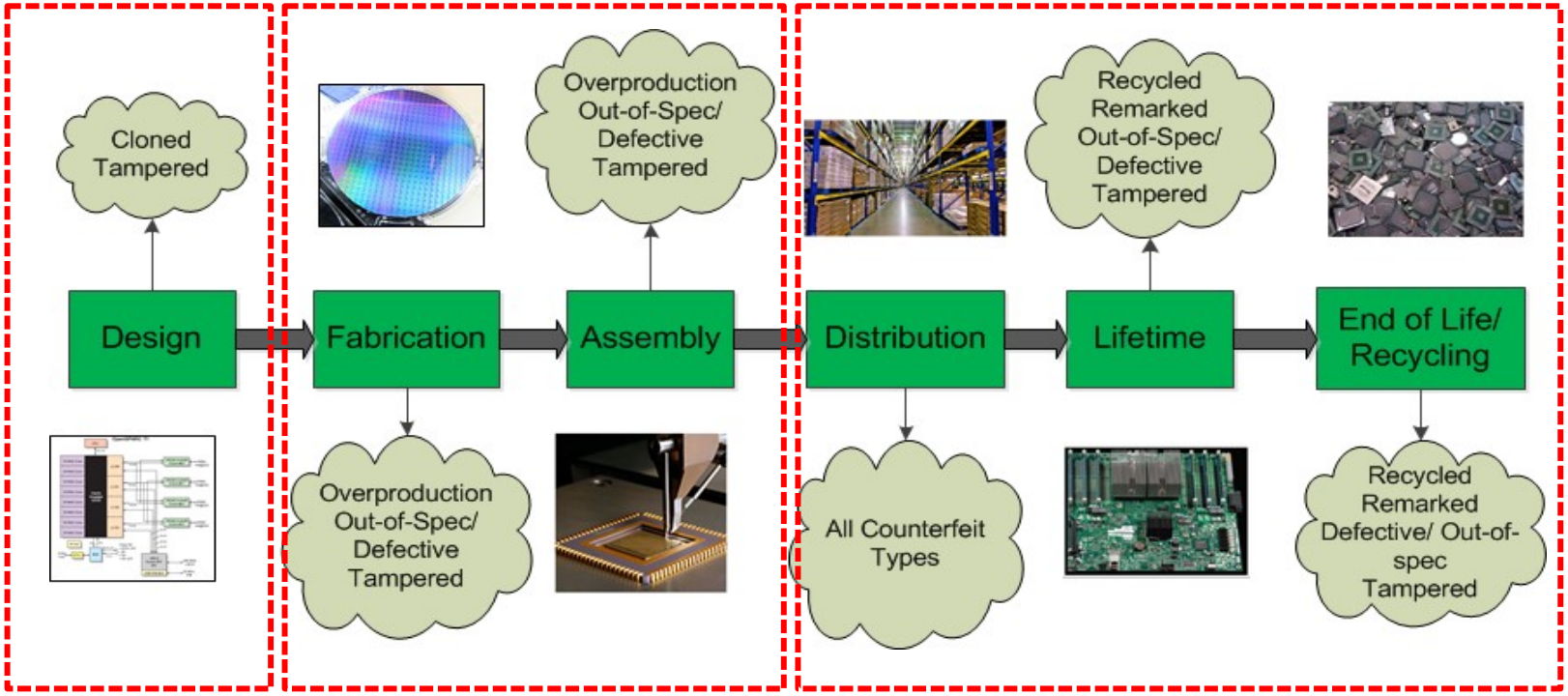
Cloning

- Unauthorized production of a part
  - Cloned parts do not have authorized IP, could be fabricated in different foundry
- Cloned parts:
  - Pirated IP – counterfeiters acquire IP in illegal manner (Saved design cost of the IP)
  - Reverse engineered – counterfeiters reverse engineer design and make new one just like original

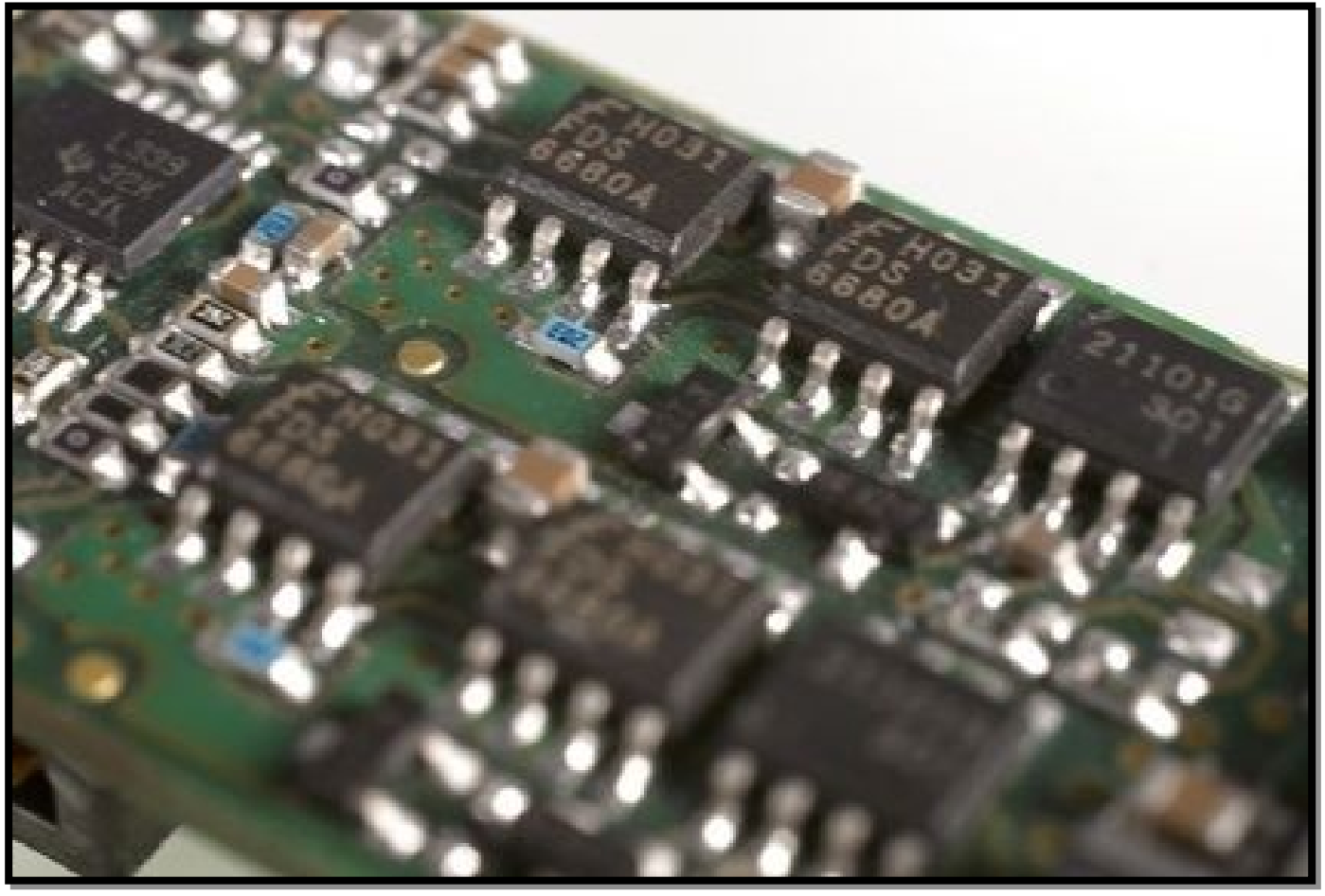
Forged Documentation

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

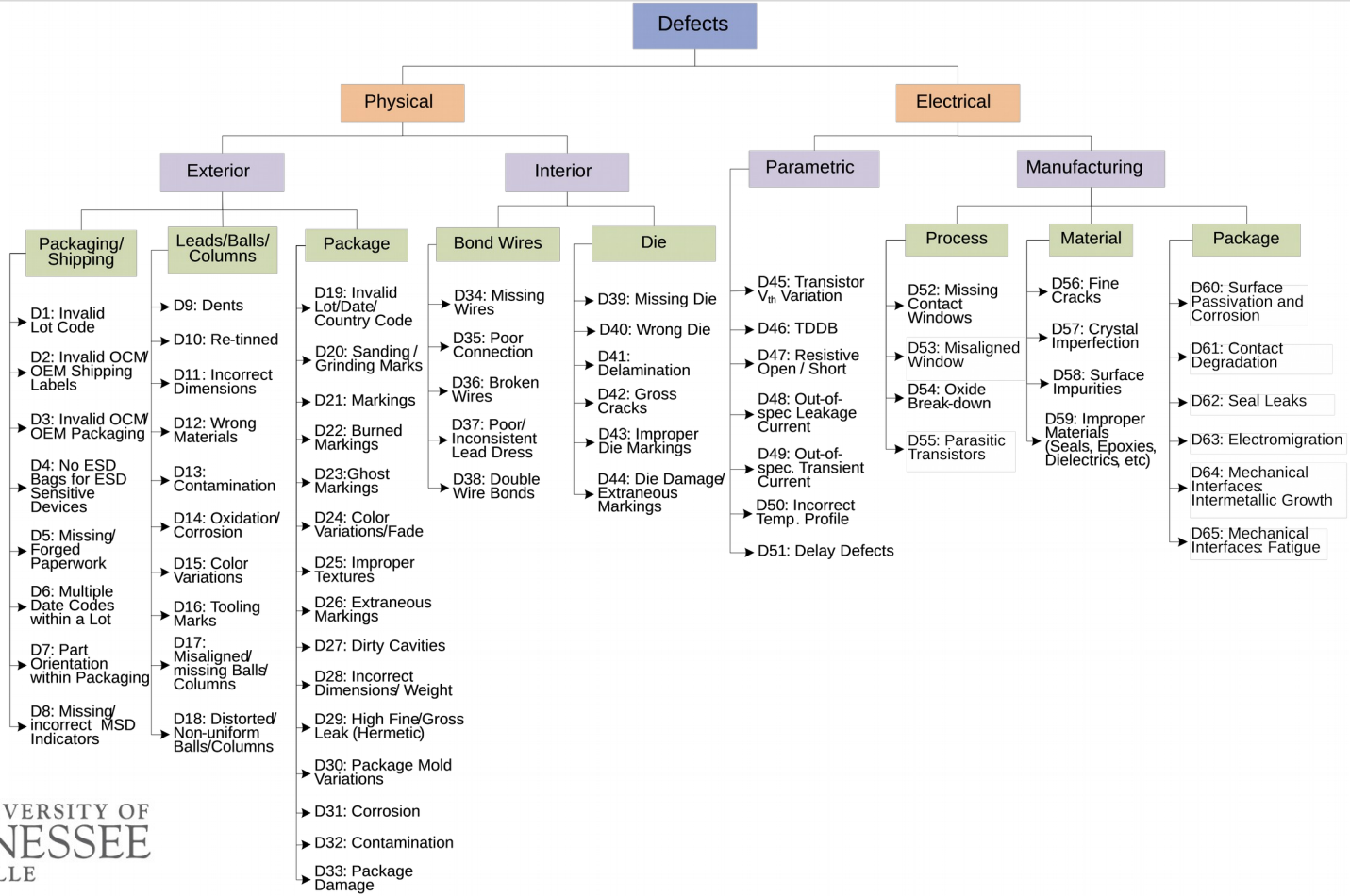
Supply Chain Vulnerability



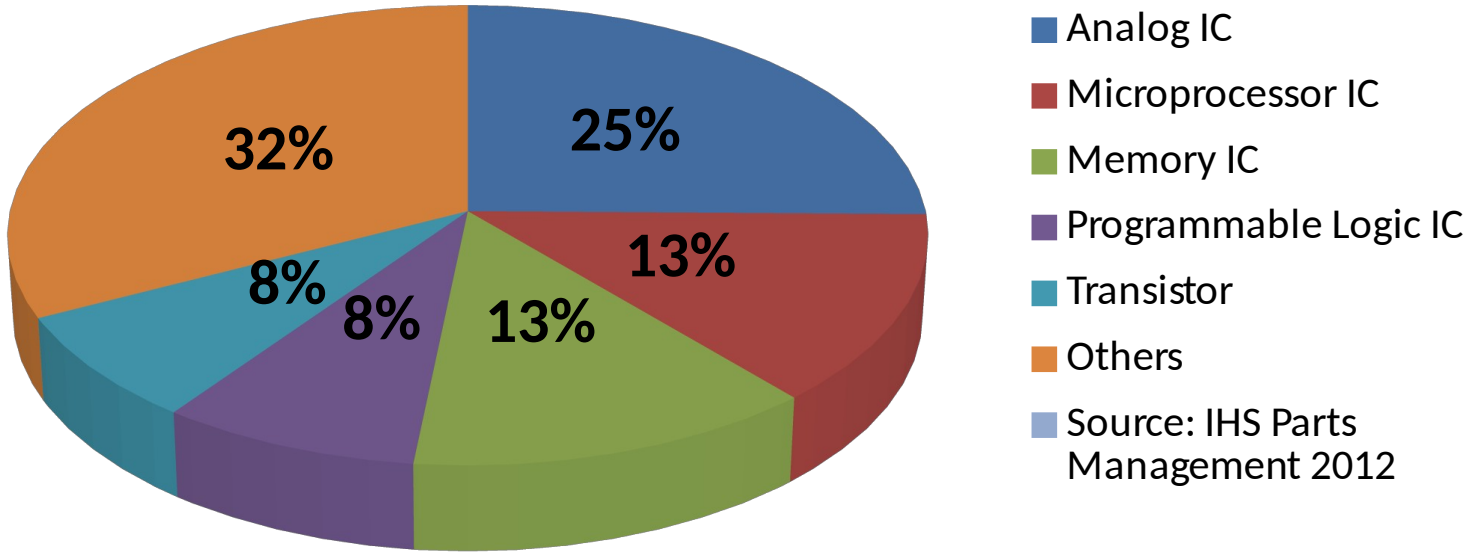
Counterfeits are Defective!



Counterfeit Defect Taxonomy



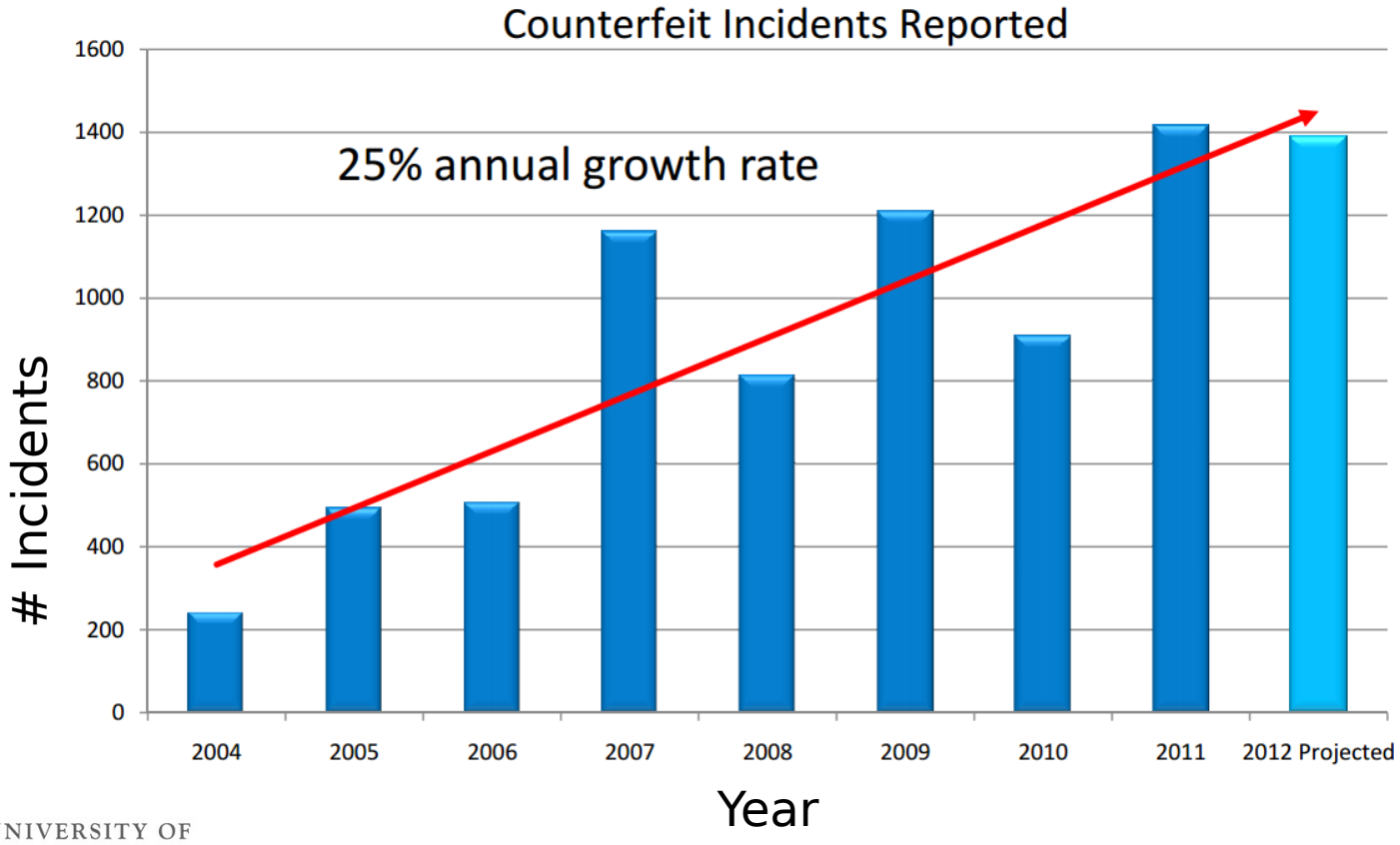
Most Counterfeit Parts in 2011 (% Reported Incidents)



IHS reports a $169B annual risk

"Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge," IHS Newsroom, 2011.

Counterfeits 2004 – 2012



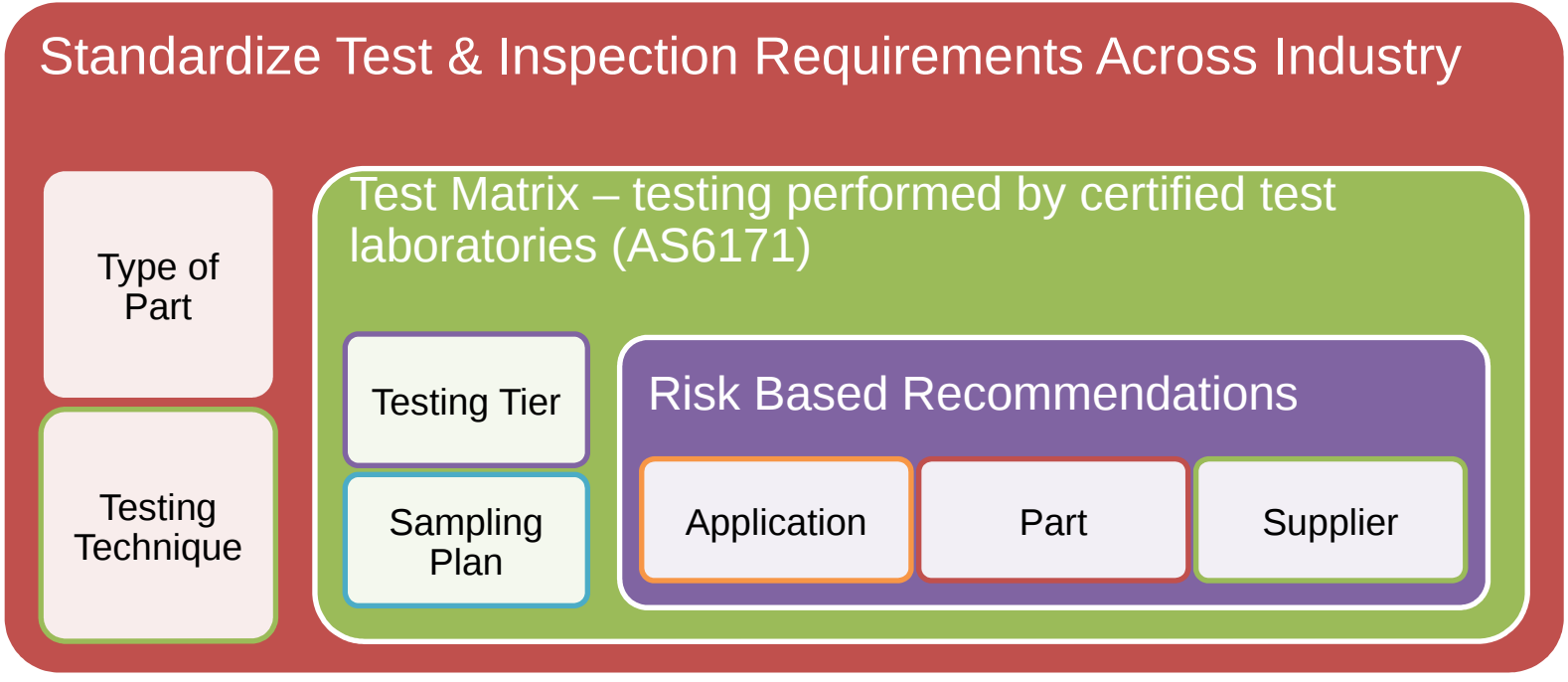
IHS Newsroom, 2012.

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 needs for inspection of electronic components traded in the open market

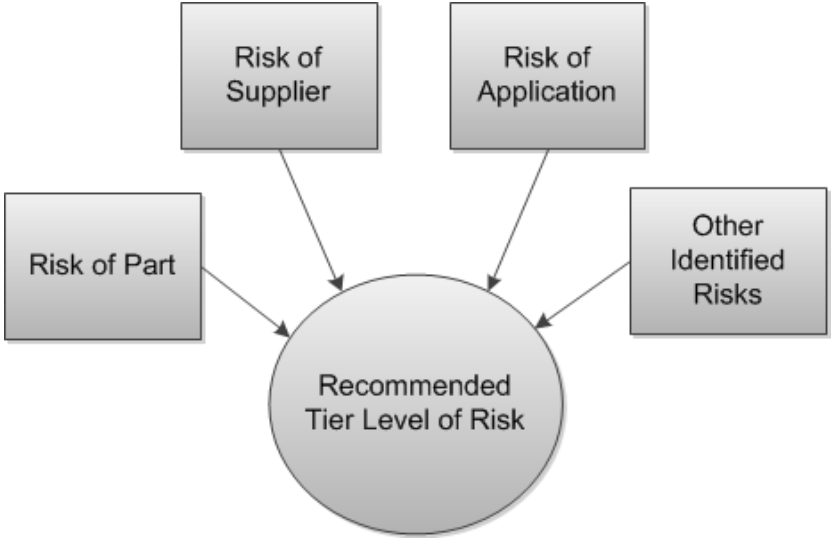
SAE G-19A Test Laboratory Subcommittee

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

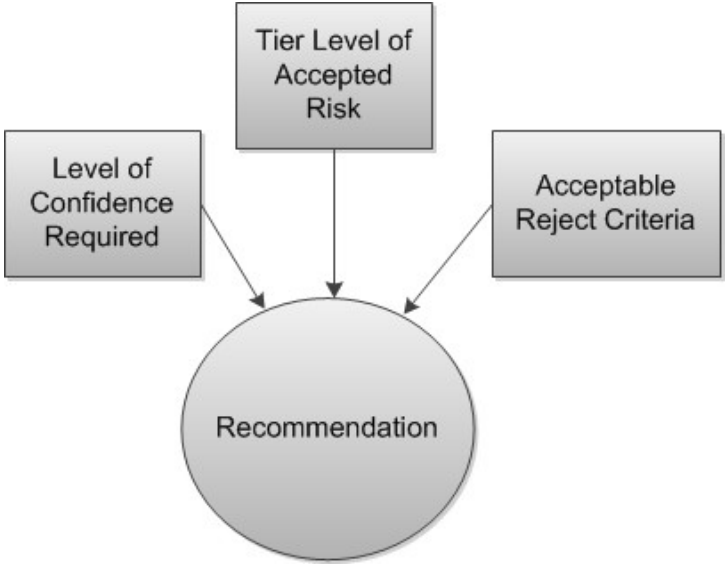


AS 6171 – Aerospace Standard

Recommended Risk Decision Tree



Recommended Sampling Plan



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	-	-	-	

CCAP-101: Integrated Circuits

- Digital Logic:
  - DC parameters, 25C and min/max temperature
  - Other tests useful to verify authenticity
- Linear, Op Amps & Mixed Logic:
  - Full power & voltage conditions
  - DC parameters, 25C and min/max temperature
  - AC parameters, 25C
- Microprocessors, DSPs, Microcomputers & Similar:
  - Key DC parameters at 25C and min/max temperatures
- Memories, RAM, SRAM, FPGA, etc.:
  - Input and output pins, open and short
  - DC parameters at min/max temperature
  - FPGAs are unprogrammed
  - Write and read to memory and speed, for RAM and FPGA
  - Other applicable tests
- Other Types of Devices:
  - Similar parameter verification based upon datasheet

Drawbacks of Testing Standards

- All of these standards
  - Deal with only two types of counterfeit parts (recycling and remarking)
  - Work from sampling basis
- Test time is extremely high (several hours per part)
- Test methods can only detect physical defects
- Electrical test methods too simple to address detection of counterfeit ICs

Example: Leads (Visual Inspection)

Non-gold leads

Gold leads on real device

Example: Dual Marking (Visual Inspection)

Example: Wrong Markings (Visual Inspection)

- Good part only has two lines of markings

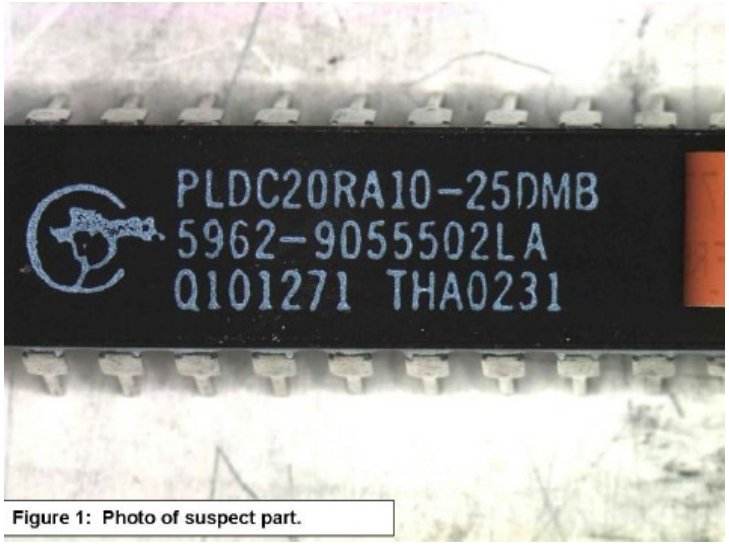
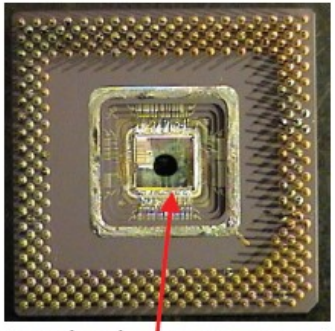


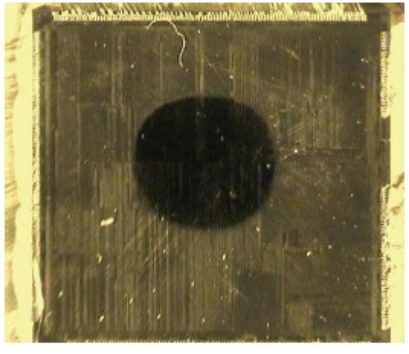
Figure 1: Photo of suspect part.

Figure 2: Photo of Known Good Part

Example: Rejected Device (Delid & Internal Visual Inspection)



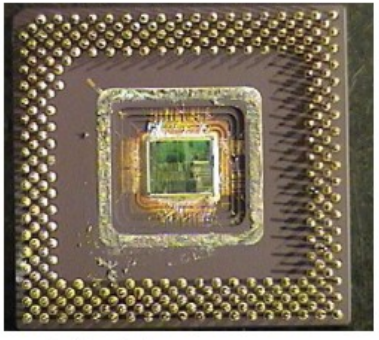
Looks simple enough Intel device, marking not too bad, OH OH!!



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

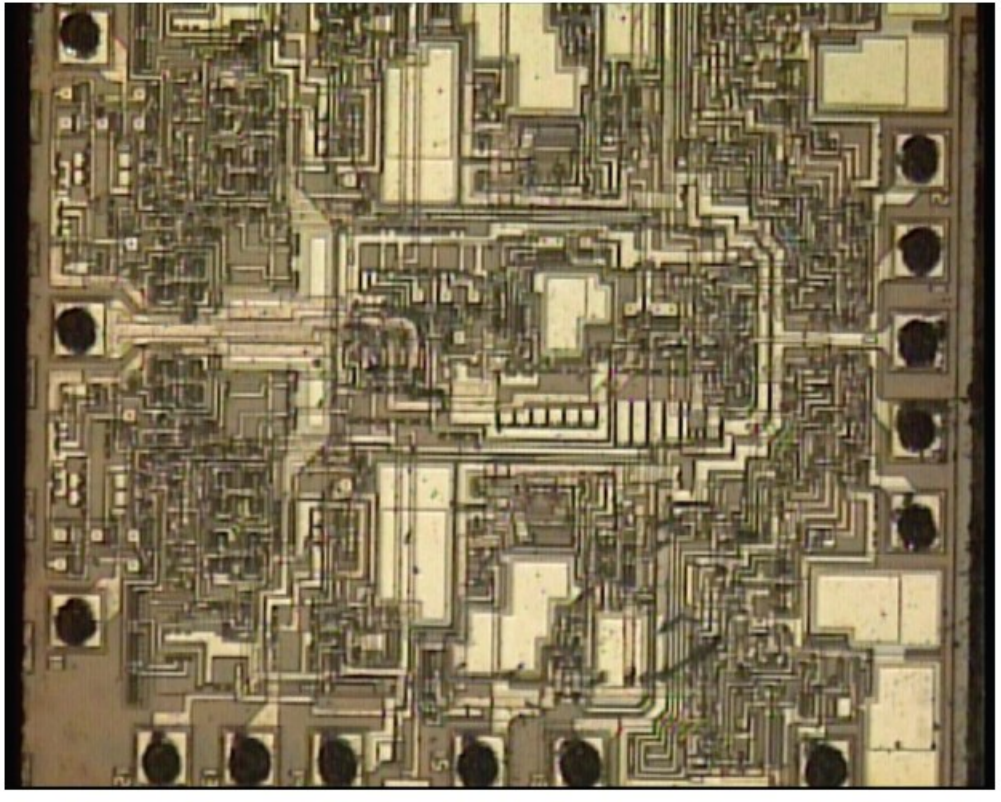
Example: Rejected Device (Delid & Internal Visual Inspection)



Same lot, same numbers but there is no ink dot

A close look at the characters shows they are backwards

Example: Cloning (Delid/Visual OR X-Ray Inspection)



This is a cloned semiconductor chip