Chapter 6

Electronic Supply Chain

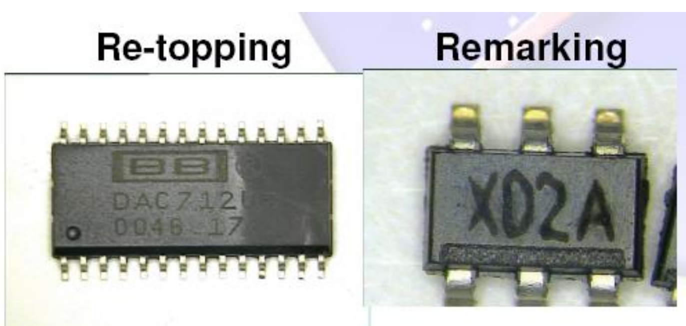
Counterfeit Detection and Avoidance

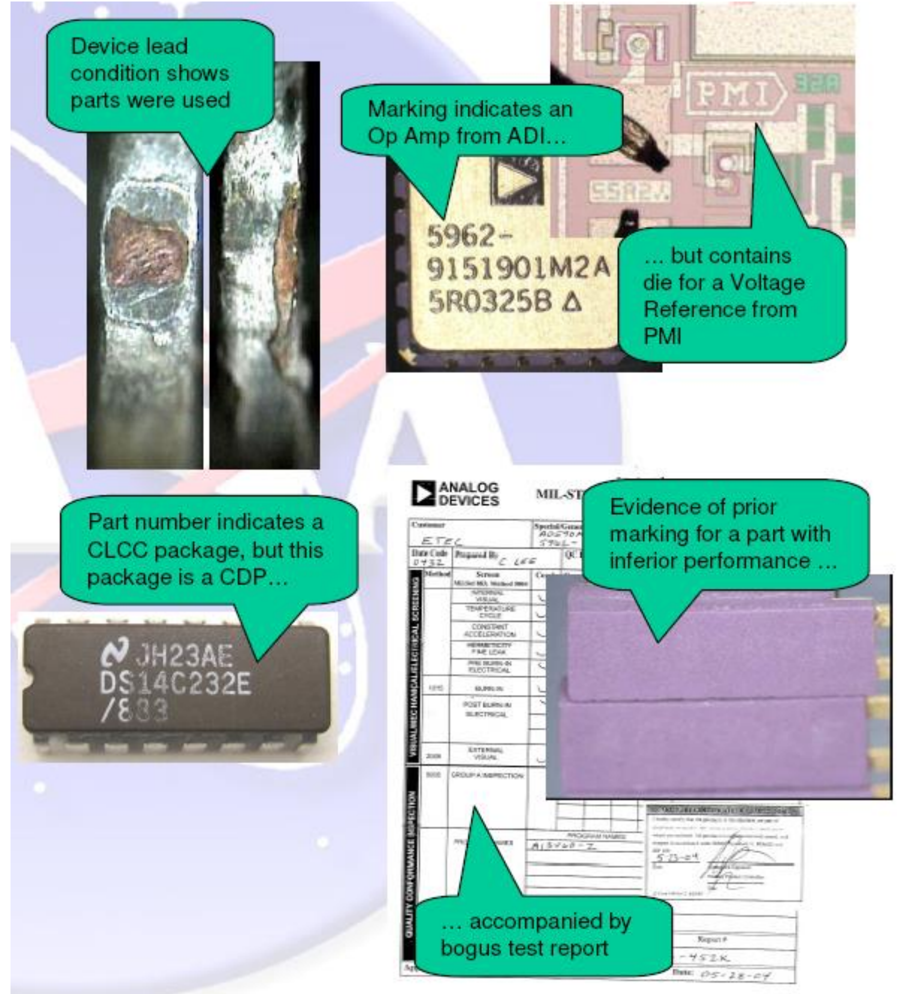
Why Counterfeiting?

- **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





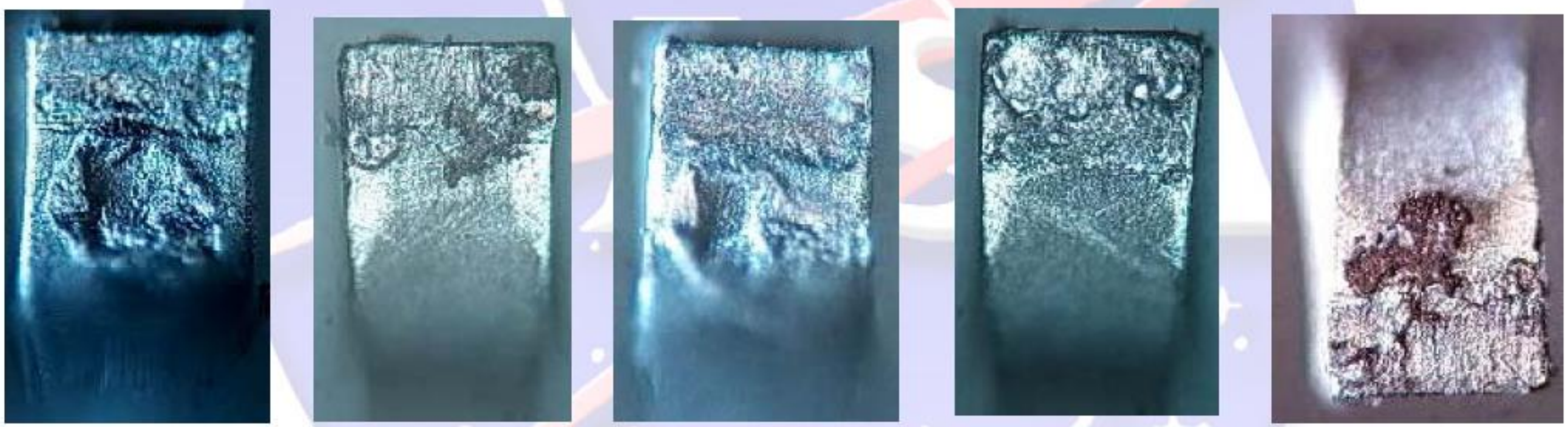
Counterfeit Electronic Parts

- 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

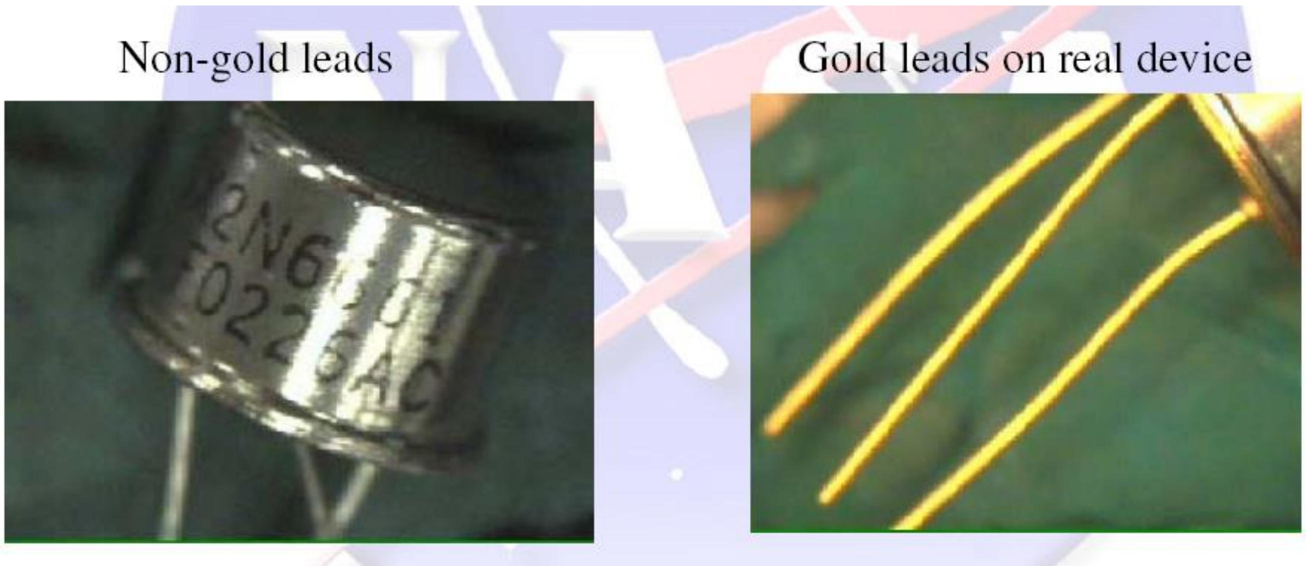
Examples

- Leads:



Examples- Cont.

- Incorrect device leads:



Examples- Cont.

- Dual Marking:

Examples- Cont.

- Good part has only two lines of marking

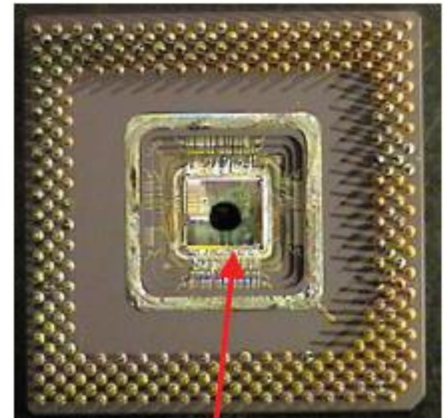
Figure 1: Photo of suspect part.

Figure 2: Photo of Known Good Part

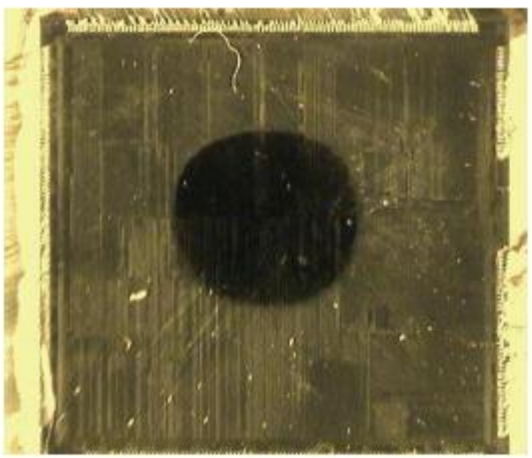
Examples- Cont.

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.

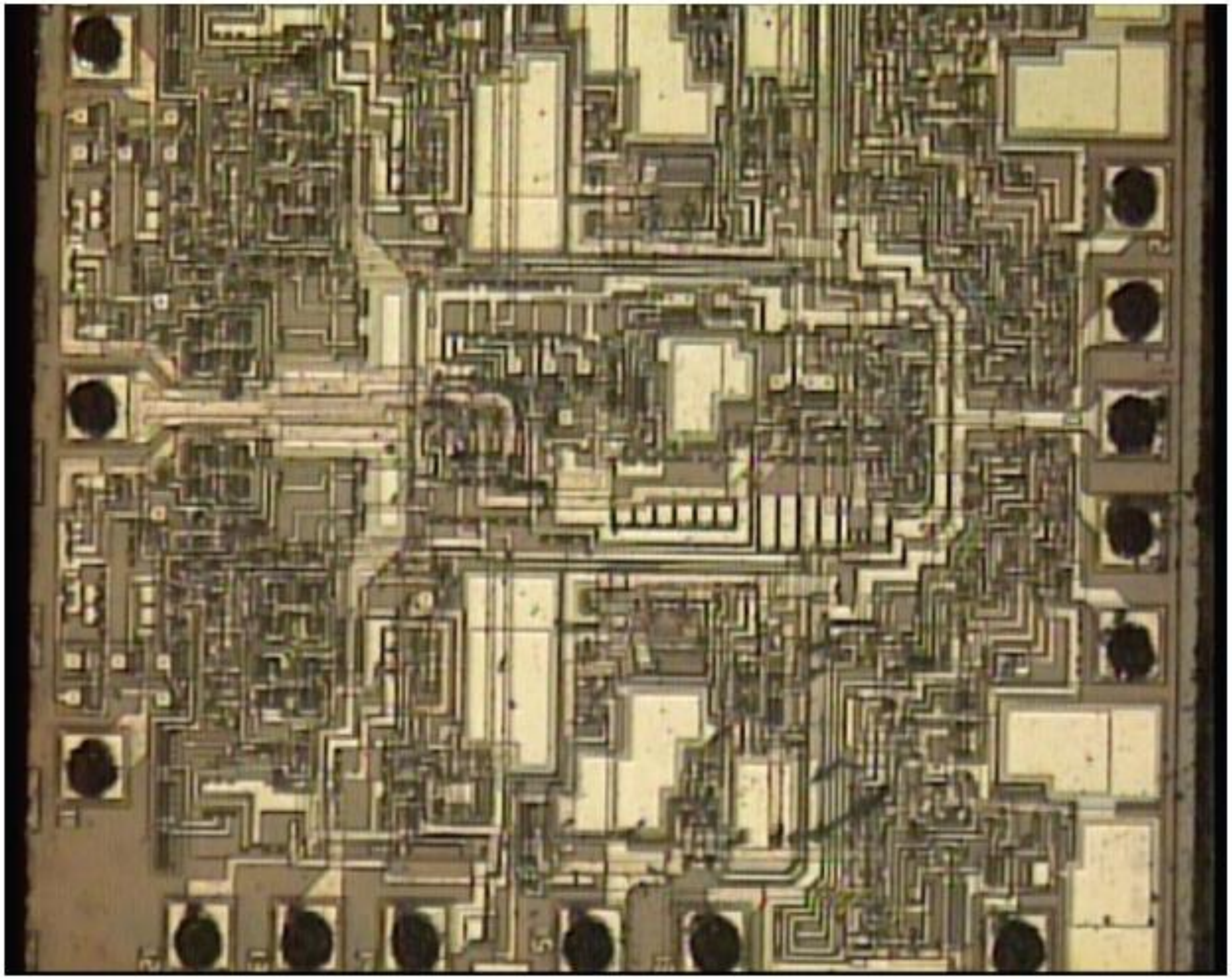
Here is the chip ID found after decap, looks good and matches the package marking

Examples- Cont.

Same lot, same numbers but there is no ink dot

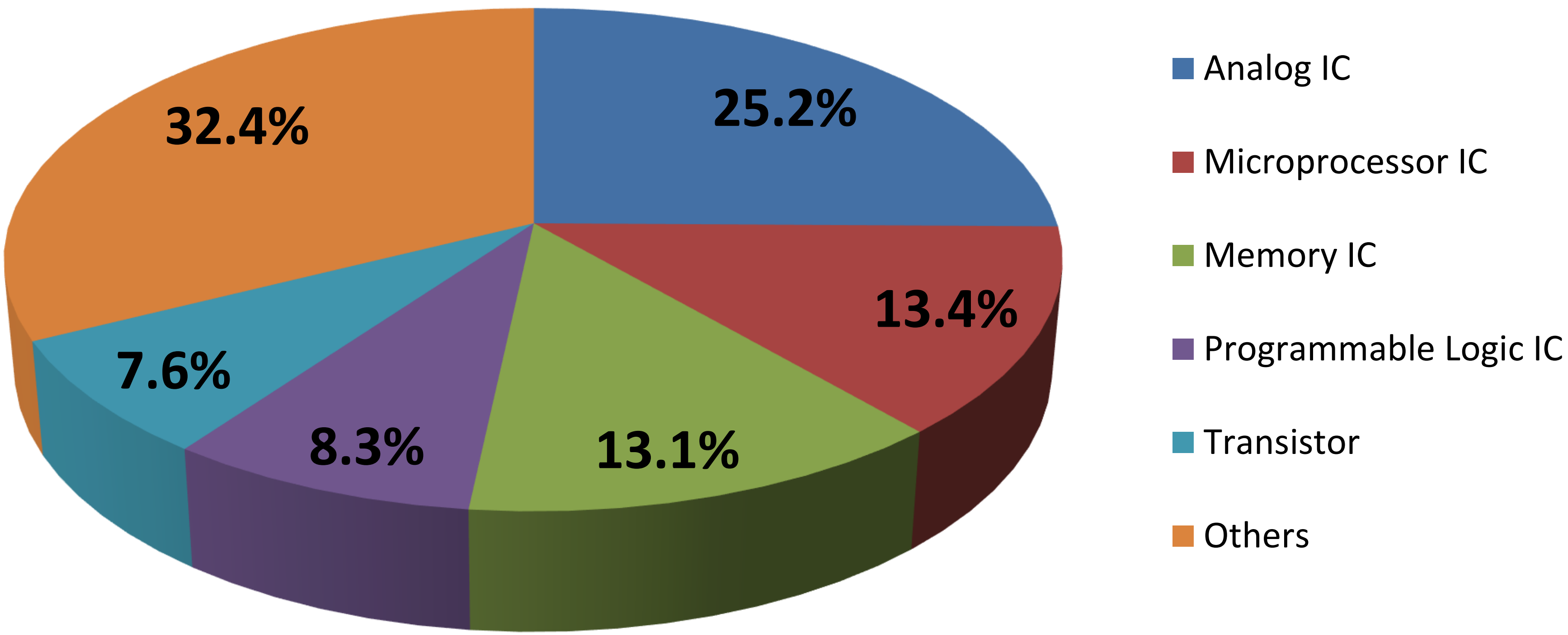
A close look at the characters shows they are backwards

Examples- Cont.



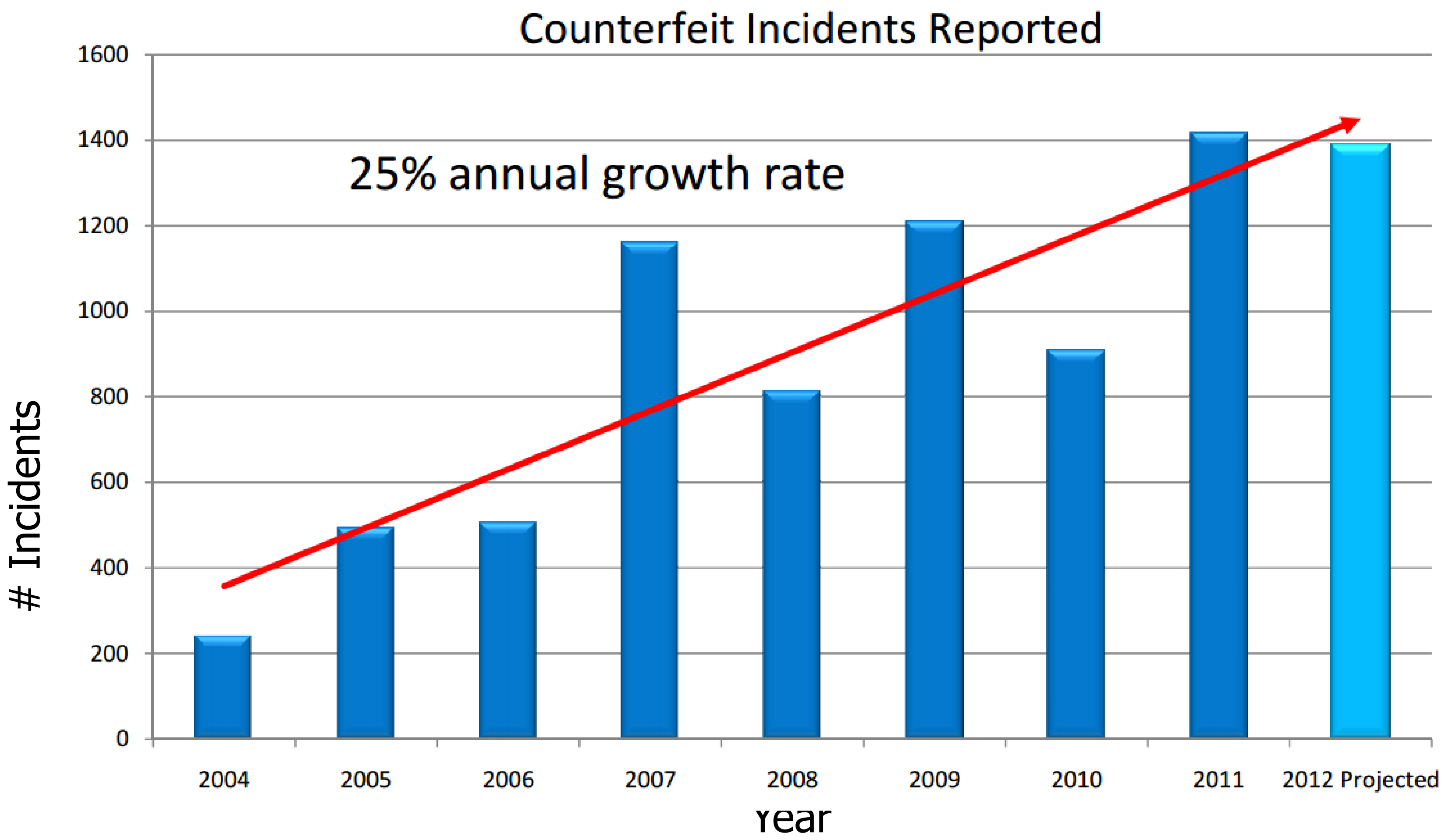
This is a cloned semiconductor chip

Most Counterfeited Parts in 2011 (% Reported Incidents)



IHS reports a $169B annual risk [3]

Reports of Counterfeits

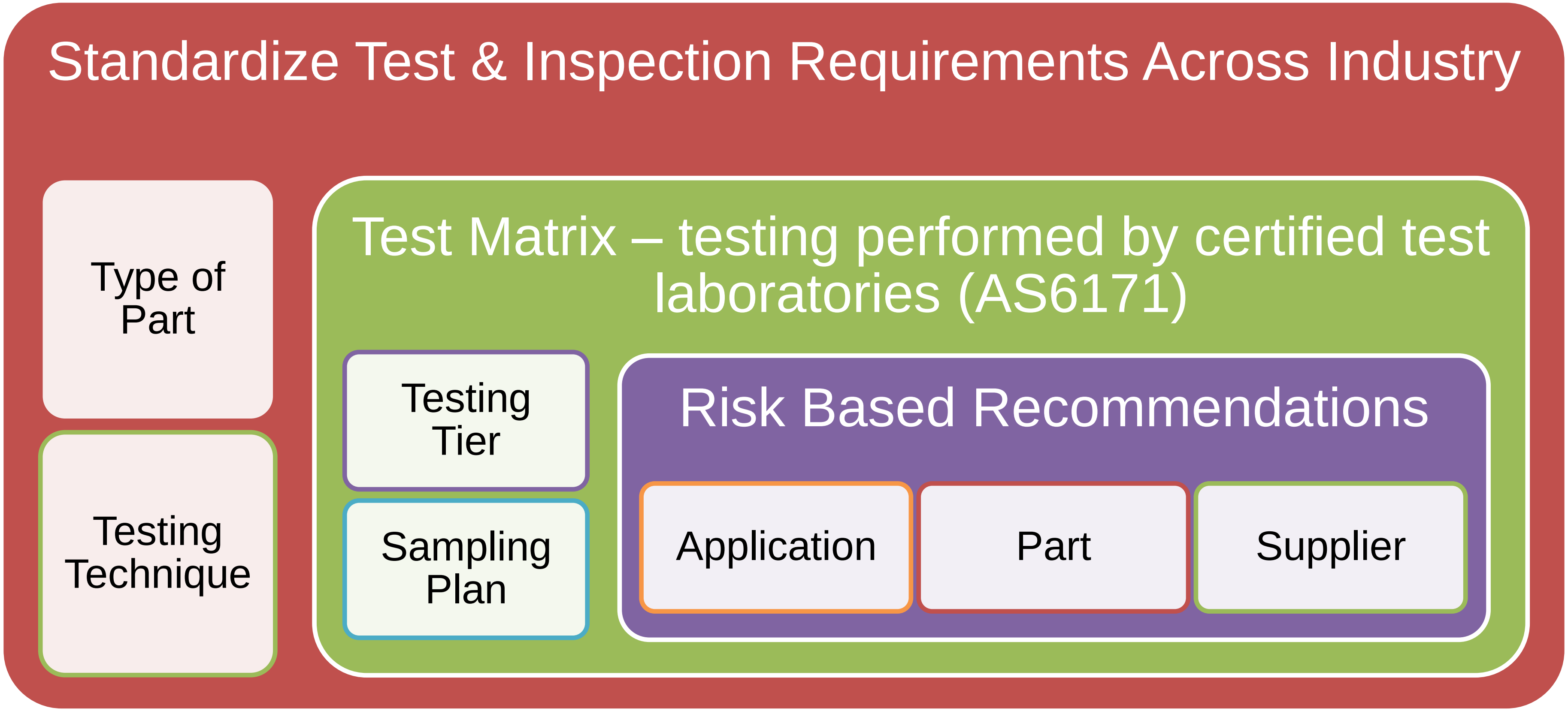


Counterfeit incidents reported by IHS [4]

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

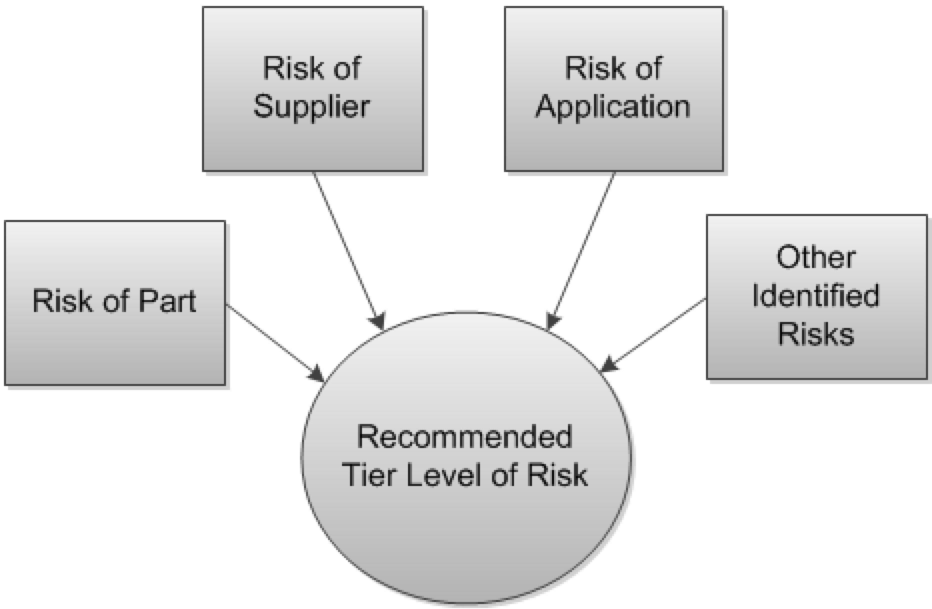
SAE G-19A Test Laboratory Subcommittee



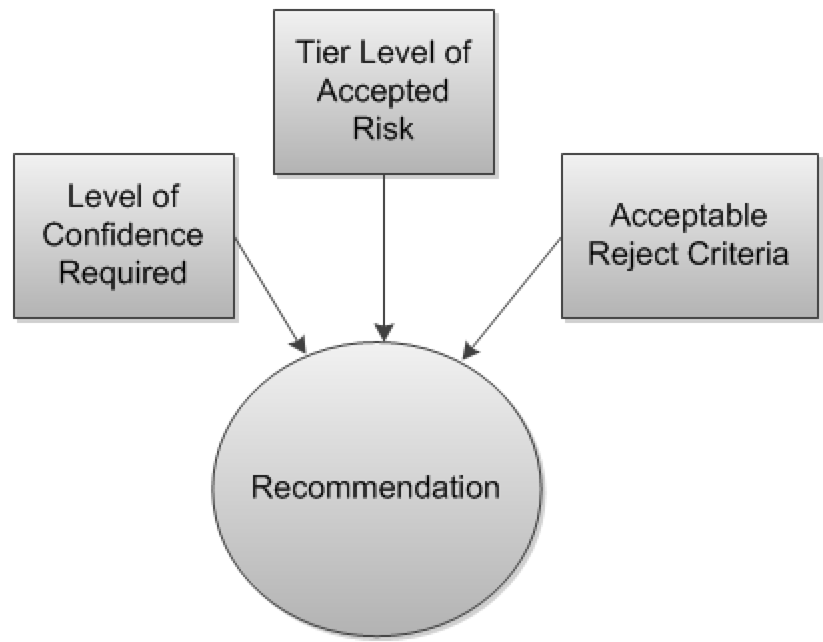
- ***System intended to create standardized testing methodology and consistency throughout industry***

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	-	-	-	

CCAP 101 define mandatory practices for use by independent distributors to detect and avoid delivery of counterfeit electronic components to their customers.

- Integrated Circuits
  - Digital logic:
    - DC parameters, 25^0C and min/max temperature
    - Other tests useful to verify authenticity
  - Linear, Op Amps & Mixed logic
    - Full power & voltage conditions
    - DC parameters, 25^0C and min/max temp
    - AC parameters 25^0C
  - Microprocessors, DSPs, Microcomputers & similar
    - Key DC parameters at 25^0C 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).

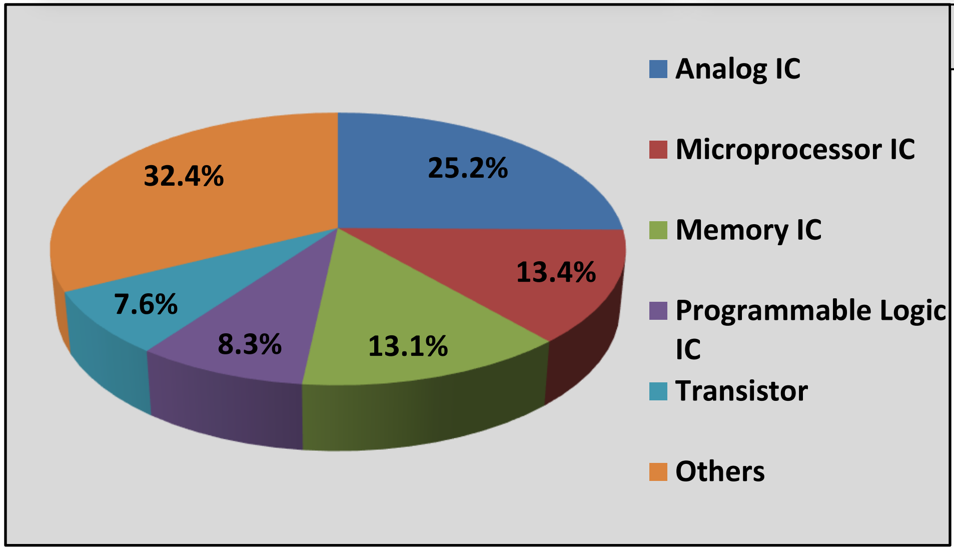
Components

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.



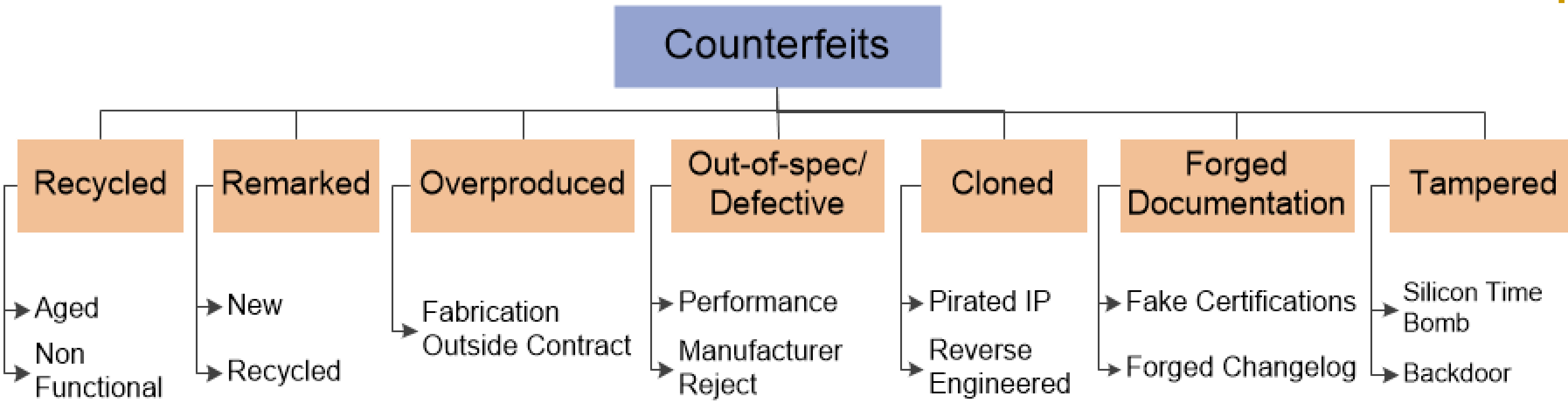
IHS reports a $169B annual risk

Where Used →

Top Part Type Reported in Counterfeit Incidents	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

Refine recycled ICs

Resold as new

Identical:
Appearance, Function, Specification

Critical Application

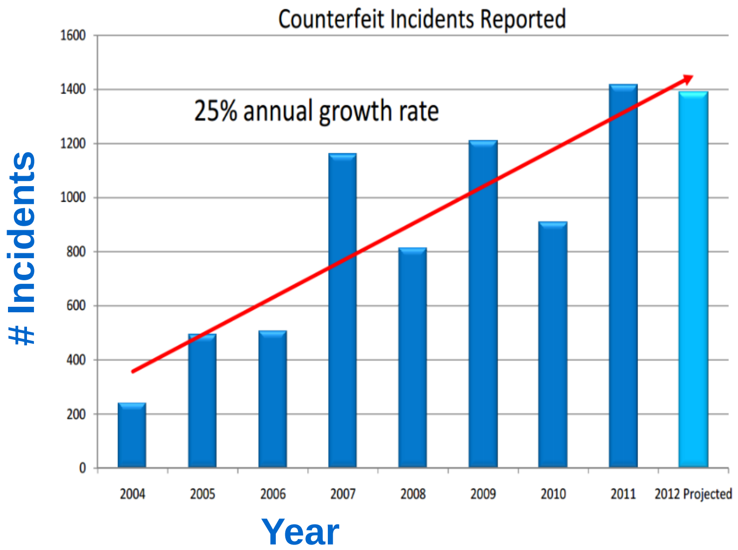
Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

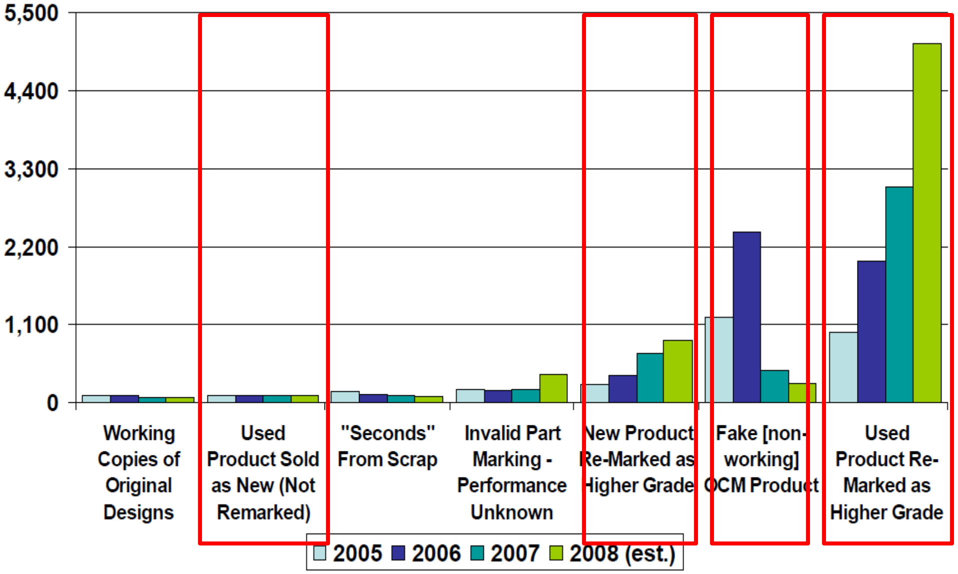
Source: Images are taken from google

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

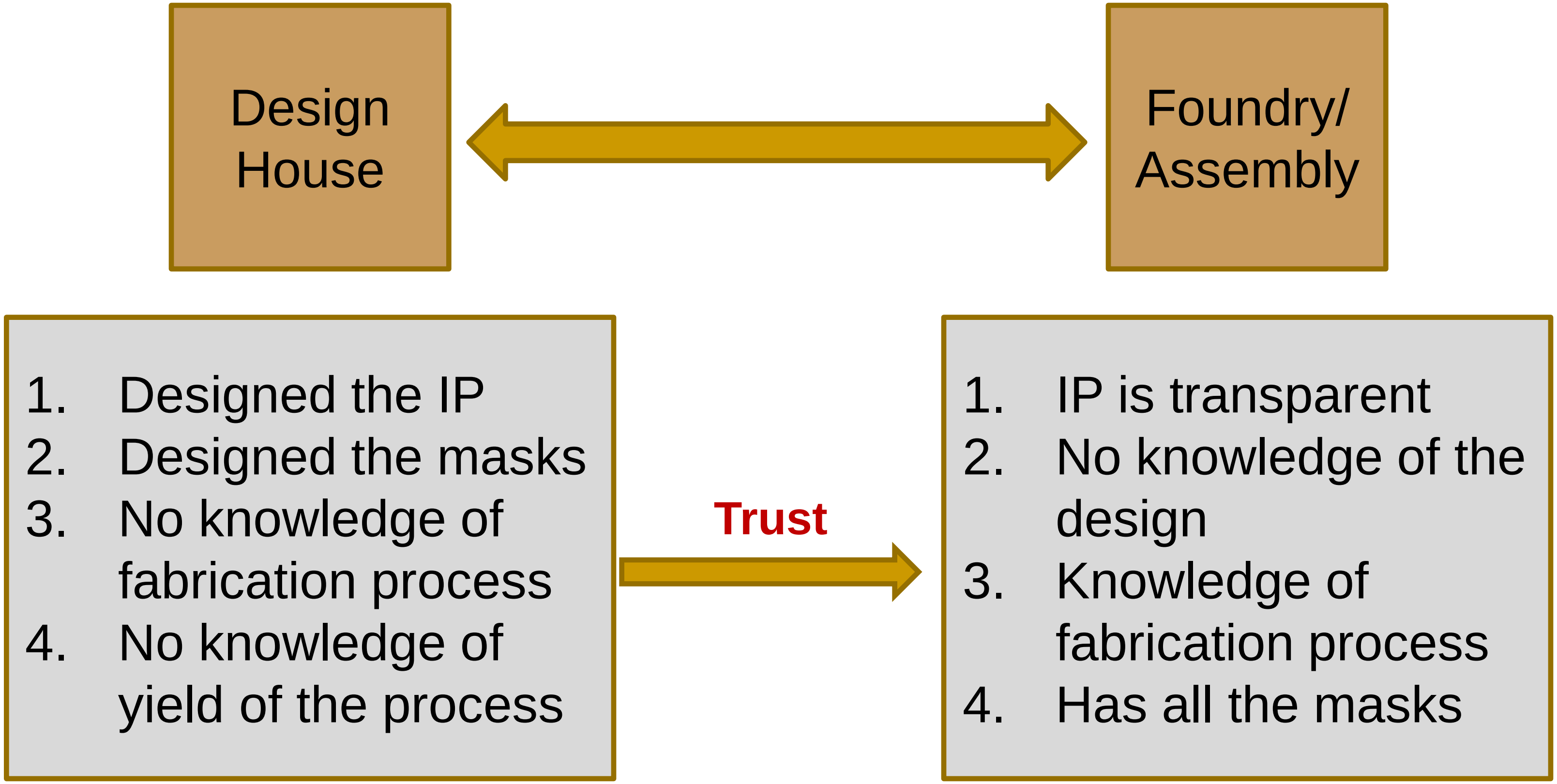
- Recycling and Remarking are the most discussed counterfeit parts
- **Remarking parts are of two types**
  - Recycled components
  - New Components
    - To change the specification of the component (commercial grade → military grade)
- **Remarking Process**
  - packages are sanded or grounded down 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 contact 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.

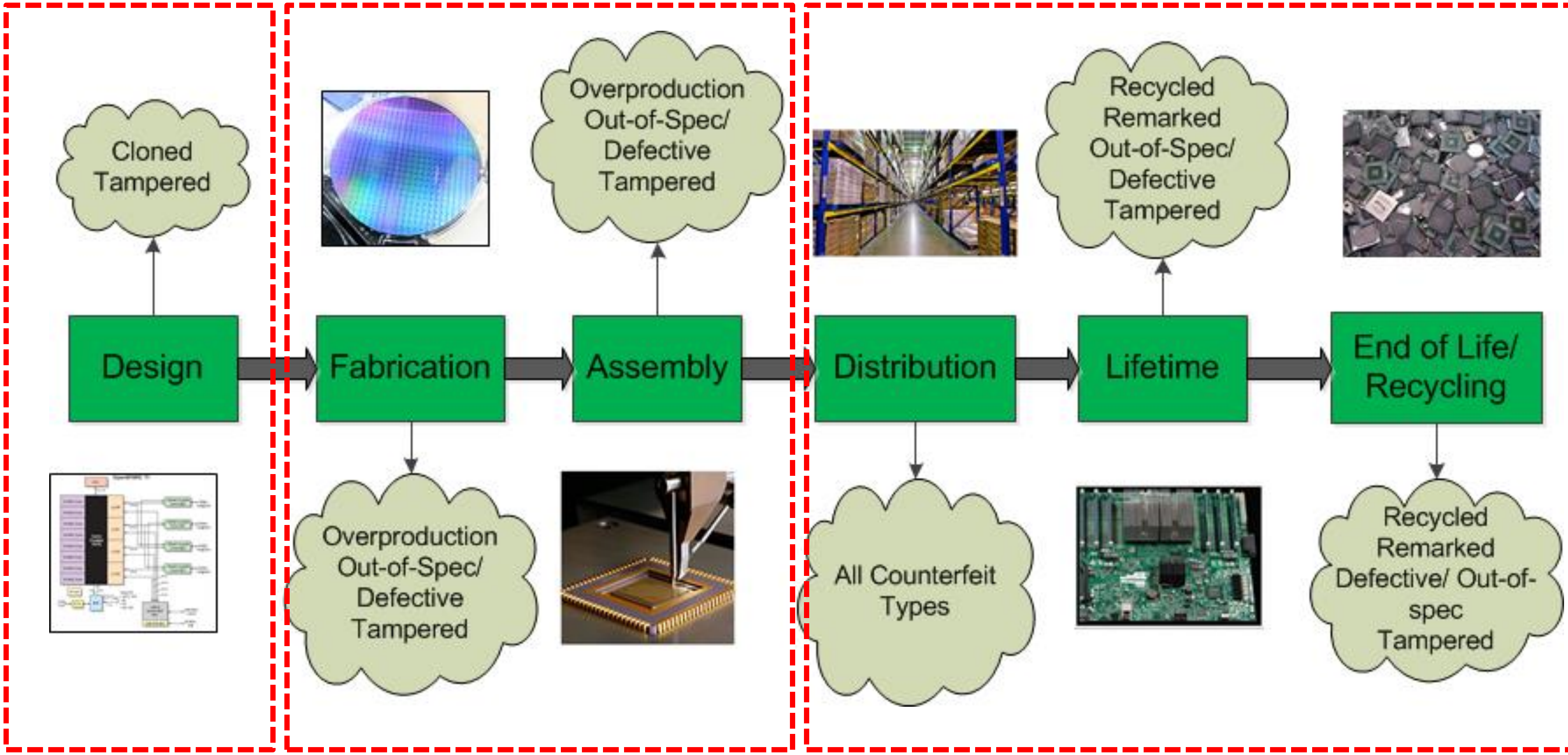
Cloned

- **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!