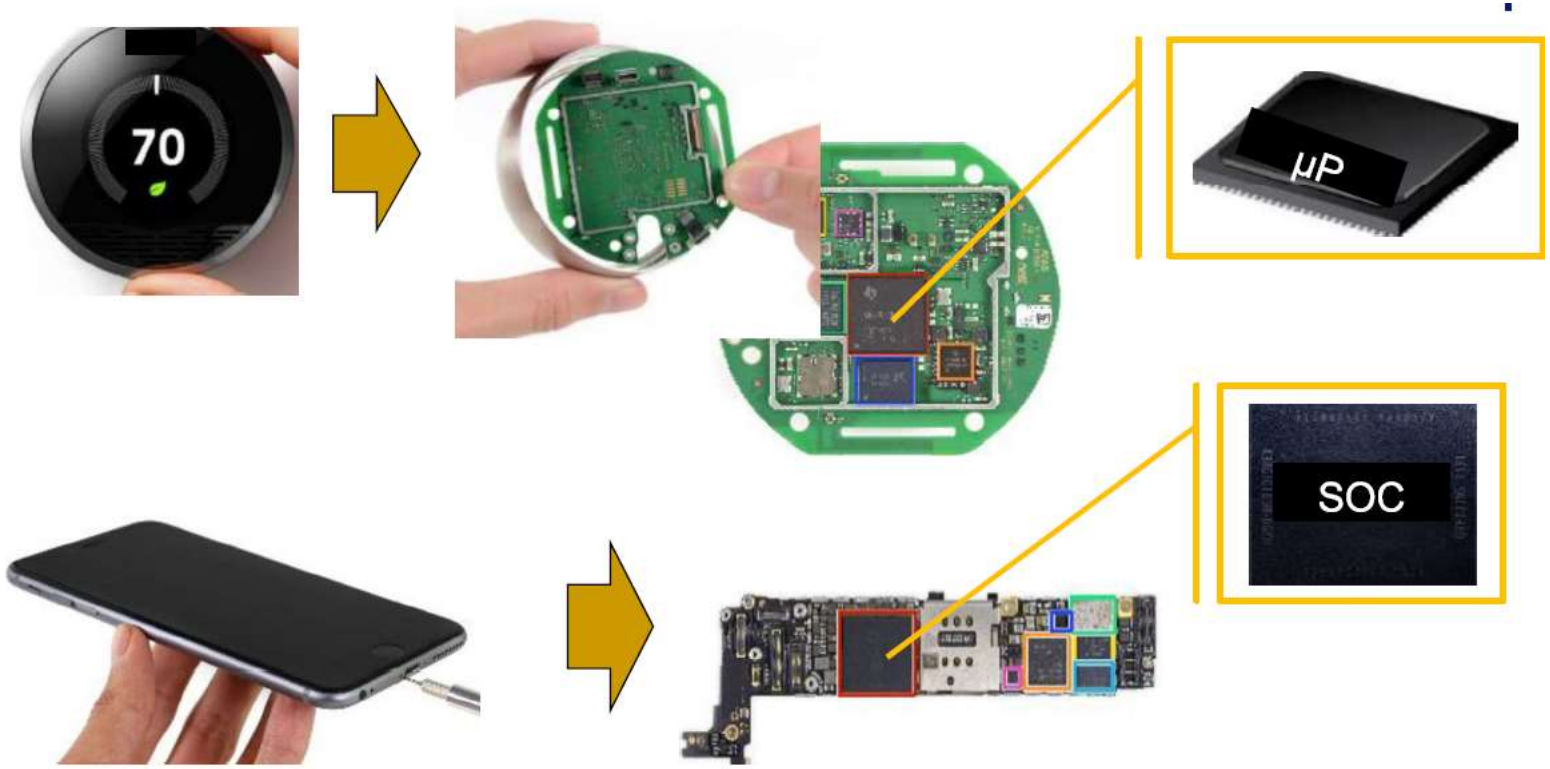
Security Issues in the Hardware Design, Manufacturing, Distribution Purchasing and Decommisioning

PROF. SERGIO SAPONARA

Hardware Supply Chain Security - Motivation

- The remarkable growth of outsourcing in the hardware supply chain has brought about serious challenges in the form of new security attacks, particularly, **IC counterfeit** and **Hardware Trojan** insertion.
- Such attacks can have severe consequences:
  - Financially, counterfeiting is costing the semiconductor companies billion of dollars and is putting thousands of jobs at risk.
  - The consequences of an insecure IC supply chain are not only limited to major financial losses, they also pose national security threats.

What is Hardware?
Integrate circuits like microprocessors, memories, System-on-Chip assembled on PCB (Printed Circuit Boards)



Example of Security Issues due to Unsecure Hardware (defense)

Roy Zoppoth stands over a Xerox 914 copy machine, the world's first, which was used in soviet embassies all over the world. The machine was so complex that the CIA used a tiny camera designed by Zoppoth to capture documents copied on the machine by the soviets and retrieved them using a "Xerox repairman" right under the eyes of soviet security.

Example of Security Issues due to Unsecure Hardware (defense)

The Pentagon is worried that "backdoors" in computer processors might leave the American military vulnerable to an instant electronic shut-down. Those fears only grew, after an Israeli strike on an alleged nuclear facility in Syria. Many speculated that Syrian air defenses had been sabotaged by chips with a built-in 'kill switch" — commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips' function and temporarily blocked the radar."

This all had a very familiar ring to it. Those with long memories may also recall exactly the same scenario before: air defenses knocked out by the secret activation of code smuggled though in commercial hardware.

This was back in 1991 and the first Iraq War, when the knockout blow was administered by a virus carried by a printer : One printer, one virus, one disabled Iraqi air defence.

Example of Security Issues due to Unsecure Hardware

The Hunt for Kill Switch, IEEE Spectrum 2008

- Increasing threat to hardware due to globalization
- Extremely difficult to detect kill switches (utilized by enemies to damage/destroy opponent artillery during critical missions) as well as intentional backdoors (to enable remote control of chips without user knowledge), which may have huge consequences
- Example: Syrian's Radar during Israeli attack, French Government using kill switches intentionally as a form of active defense to damage the chips if they fall in hostile hands, and more...

Example of Security Issues due to Unsecure Hardware ICT or energy business sectors

Fake Cisco routers risk "IT subversion"

- An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors.
- $76 million **fake Cisco routers**

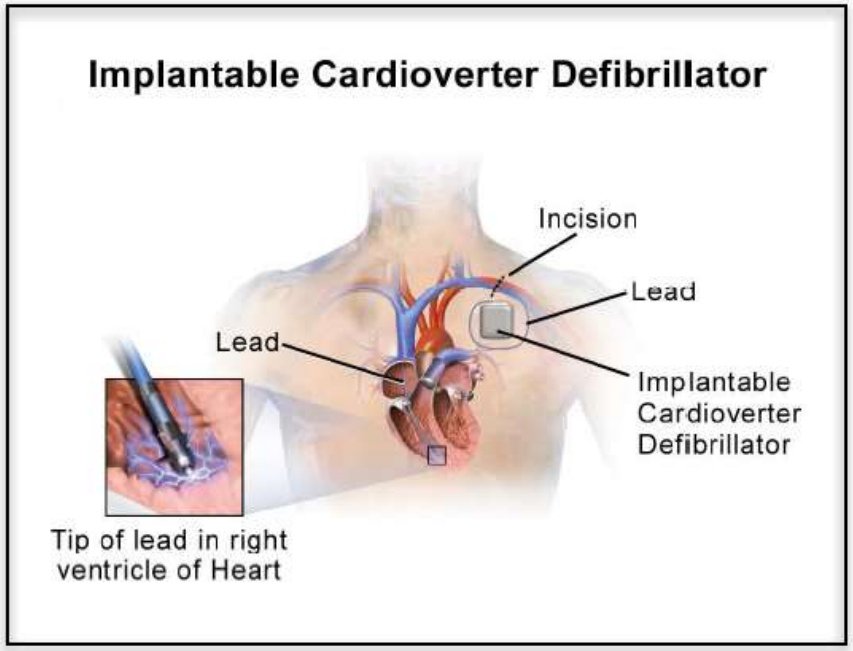
Energy Theft Going From Bad to Worse

- Tampering with "smart" meters
  - Oil, electricity, gas, …
- $1B loss in CT because of electricity theft

Example of Security Issues due to Unsecure Hardware medical field

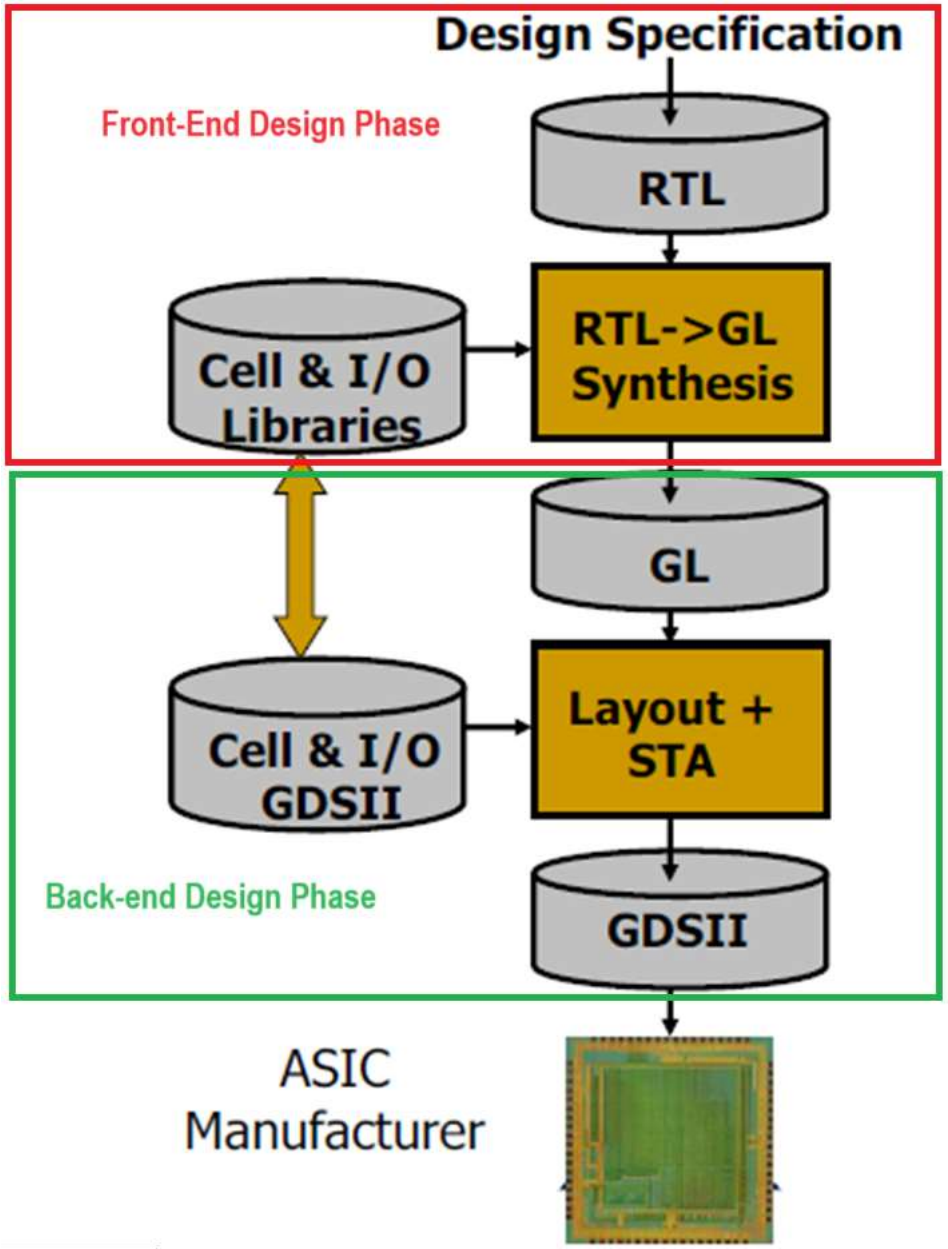
Medical Device Security

- Incorporating security is sometimes considered expensive
- Implantable devices: e.g., Heart rate monitor
  - Incorporating Security could potentially reduce the life-time of the device by 30%
  - Attacking these device could result in loss of lives



Example of Security Issues due to Unsecure Hardware in automotive field (due to CAN chip vulnerabilities)

Chip Design & Fabrication Flow



- Traditional approach:

All steps involved in the design process used to be, in many cases, the same as the IC manufacturer

→ "full control" of the IC designer of whole design process (secure approach)

RTL: Register Transfer Level, GL: Gate Level

STA: Static Timing Analysis,

ASIC: Application Specific Integrated Circuit,

GDSII: Graphic Database System Information Interchange

RTL to GL (Front-end)

GL to GDSII and chip manufacturing (Back-end)

ASIC: technology where there is a technology provider and you program onto it.

1. Design specs. Then using HDL you describe at logical level your chip and so you design the version at RTL. Then given a certain technology library (so you have a tech provider), the RTL is mapped to that specific logic and get a gate level representation.
2. With gate level description, given the technology, you make the layout of your chip and make static timing analysis. Then you get your GDS2, which is a file format for the design we can pass to a manufacturer.

Then you have the manufacturing phase.

FRONT END DESIGN PHASE

Note: in the most cases, it's rare that a company do both the design and the manufacturing.

NOTE: GDS2 at the end is a database that you send.

Yes, ASIC manufacturers provide technology platforms that designers can use to build their chips. These platforms typically include:

- **Process Technology**: Fabrication processes at different nanometer (nm) nodes, such as **TSMC's 3nm, 5nm, 7nm, etc.**, which define how small and efficient the transistors on the ASIC can be.
- **EDA (Electronic Design Automation) Tools**: Design and verification software from companies like **Cadence, Synopsys, and Mentor Graphics**, which help engineers create ASIC layouts and simulate their behavior.
- **IP Cores & Libraries**: Pre-designed building blocks like **memory modules, standard logic gates, and specialized functions (e.g., encryption, AI accelerators)** that designers can integrate into their ASICs instead of designing everything from scratch.
- **Foundry Services**: Pure-play foundries like **TSMC, GlobalFoundries, and UMC** manufacture ASICs for designers who don't have their own fabrication facilities (fabs). Some companies, like **Samsung and Intel**, both design and manufacture chips.

Cell and I/O libraries are essential building blocks in ASIC and FPGA design. They provide pre-designed, optimized components that allow engineers to translate high-level hardware descriptions into actual gate-level implementations.

Cell Libraries (Standard Cell Libraries)

- Contain **pre-designed logic gates** (AND, OR, XOR, etc.), flip-flops, multiplexers, and other digital components.
- These cells are characterized for different process technologies (e.g., **5nm, 7nm, 28nm**) and optimized for factors like **power, performance, and area (PPA)**.
- Used to synthesize RTL (Register Transfer Level) code into a **gate-level netlist**, ensuring correct logic behavior and physical constraints.

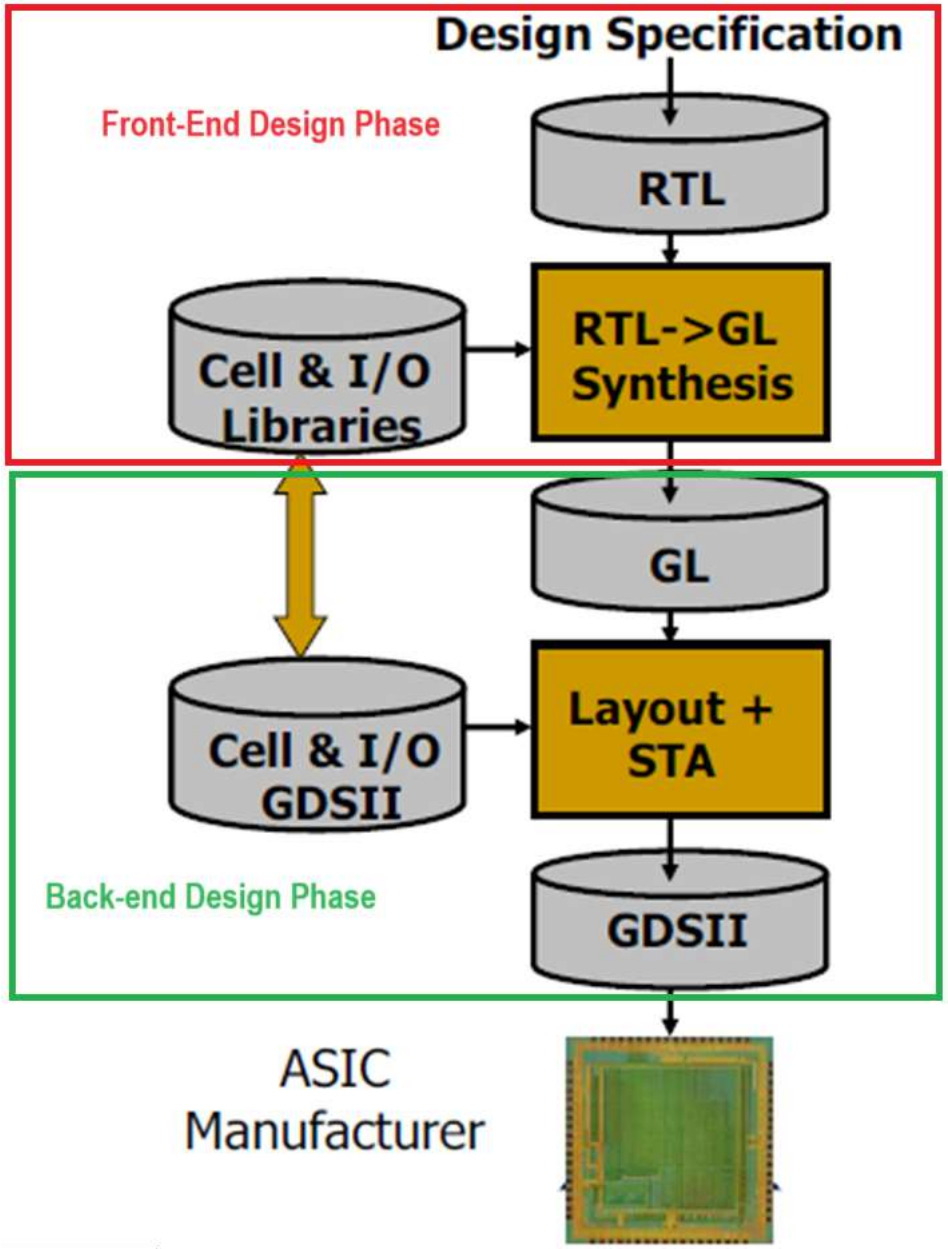
I/O Libraries

- Provide **specialized circuits** for handling signals at the boundary of the chip, such as **input/output buffers, level shifters, electrostatic discharge (ESD) protection, and pad drivers**.
- Ensure signals are correctly interfaced between different voltage domains and external systems.
- Often customized for the target application, like **high-speed SerDes, DDR memory interfaces, or GPIOs**.

Who Provides Cell & I/O Libraries?

- **Foundries** like **TSMC, Samsung, and GlobalFoundries** provide **process-specific standard cell libraries**.
- **EDA Tool Vendors** like **Synopsys, Cadence, and Mentor Graphics** offer **optimized cell libraries** for different applications.
- **IP Vendors** like **Arm and Synopsys** supply **custom standard cell libraries** tailored for performance, low power, or specific functionality.
- **ASIC Design Houses** often create their own cell libraries for **custom optimizations**.

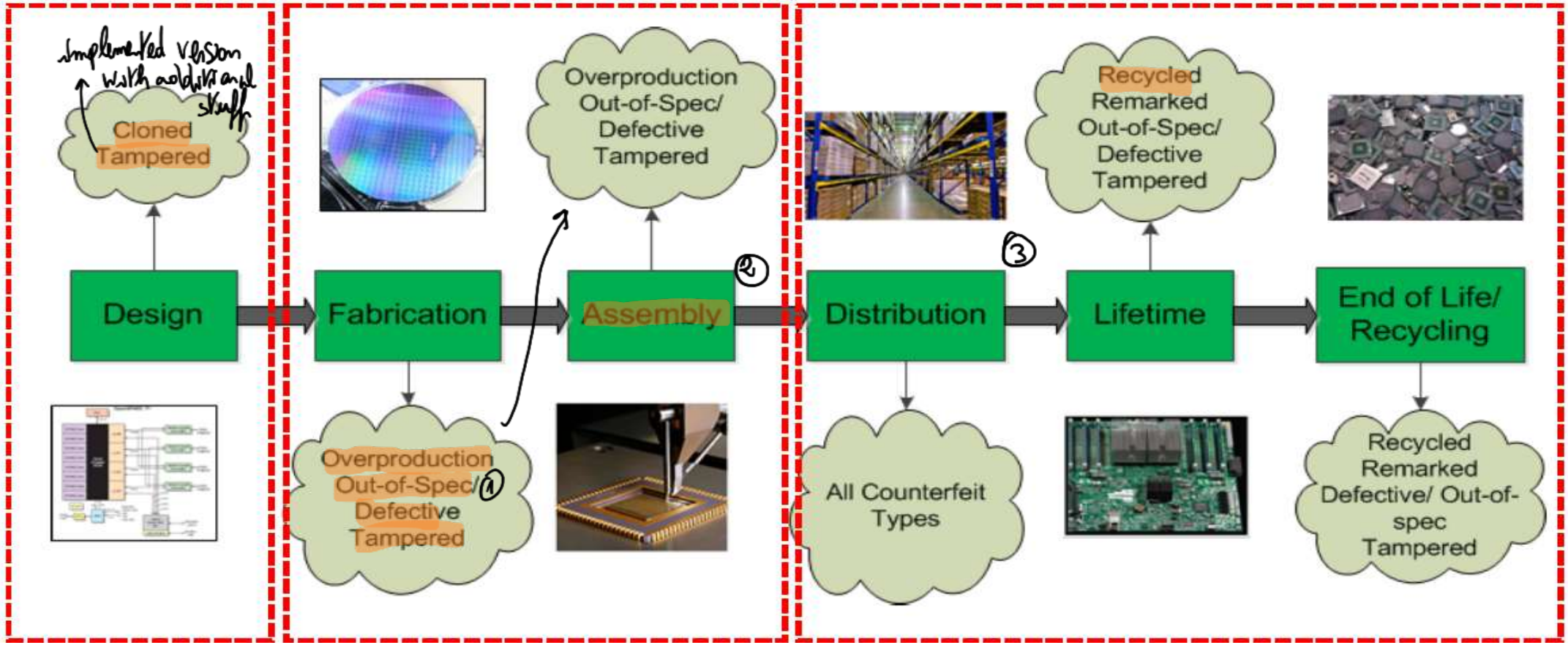
Chip Design & Fabrication Flow



- The implementation of this design flow considering as target technologies IntelAletra FPGA using SystemVerilog HDL (Hardware Description Language) plus QuartusII tool will be part of the hands-on laboratory part of the course with Prof. Luca Crocetti and will be part of the exam project and technical report.

FPGA: Field Programmable Gate Array

After Chip Design & Fabrication there are Assembly (packaging, PCB board soldering,..), distribution, end of life management



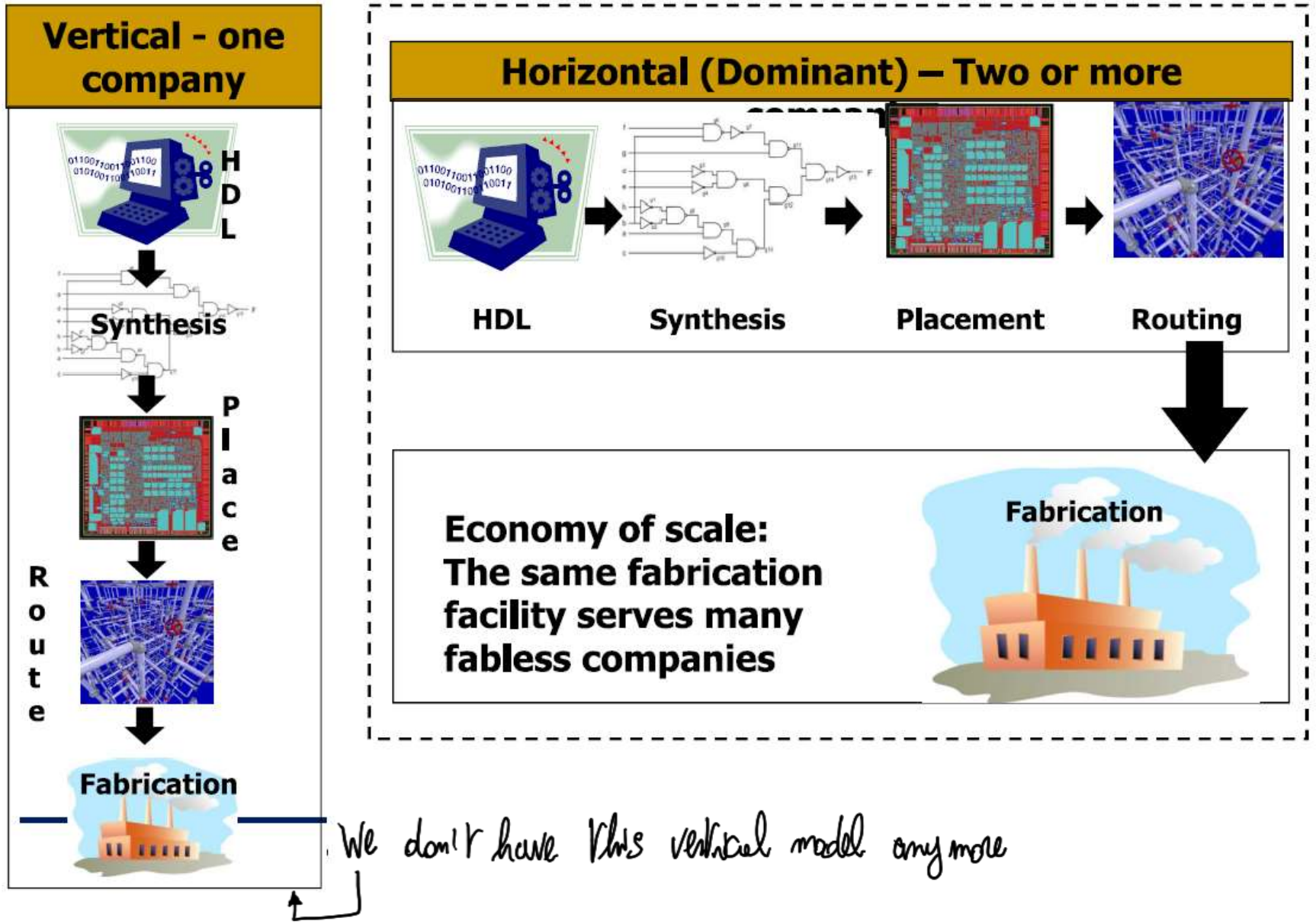
① Out of spec: when you produce electronics, on average you have pieces having the right values, but a percentage of the chips will have specs that can change up to 10-20%. You usually specify some boundaries to adhere to, so of 1M components, 1.5M have to be produced and the 0,5M that are not in spec should be marked as defective and be destroyed.

② Who is making the assembly?

③ Sell to other company or to people. Especially for international distribution you won't just have 1 company managing everything.

④-⑤ If HW is not destroyed, can be disassembled, remarked and recycled (even modified) and sold as new.

Change of Chip Business Model



Fabless Business Model

Most companies are now Fabless: i.e. they design the chip up to RTL or GL or GDSII but the fabrication is done by external foundries

For example, NVIDIA is a Fabless company (up to GDSII)

→ most important designer of processors

ARM is a Fabless company (up to RTL or GL) selling to companies like NXP, STMicroelectronics, Infineon, that produce chip or up to GDSII

STMicroelectronics makes design and manufacturing for some product lines, but for extreme scale nodes (e.g. 5 nm) is fabless

INTEL, Samsung make design and manufacturing

TSMC, GlobalFoundry, are only foundries (manufacturing based on GDSII received by other companies)

1. Physical Design (From Gate-Level to GDSII)

At the **gate level**, the design consists of interconnected logic gates, but it's not yet mapped to the physical silicon layout. The next steps are:

- **Synthesis**: Converts the gate-level netlist into specific standard cells (predefined logic gate layouts) provided by a fabrication process (e.g., 5nm, 28nm, etc.).
- **Placement**: Determines where each logic gate will be placed on the silicon die.
- **Routing**: Connects the gates with metal interconnects to form a working circuit.
- **Timing and Power Optimization**: Ensures signals travel within clock constraints and power usage is optimized.
- **DRC & LVS Checks**: Validates that the layout follows manufacturing rules and matches the original logic design.

The final result of this process is the **GDSII file**, which is what foundries use to create the masks for manufacturing.

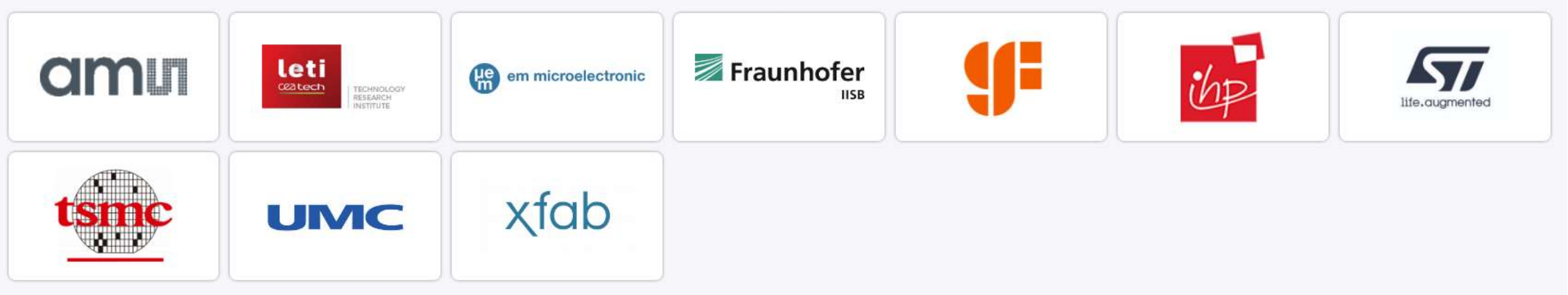
NOTE: from a pure digital POV, if you have a pure digital design, the smaller the transistors are, the faster. But for other techs you might need big chips.

Europractice Foundries for Small Production

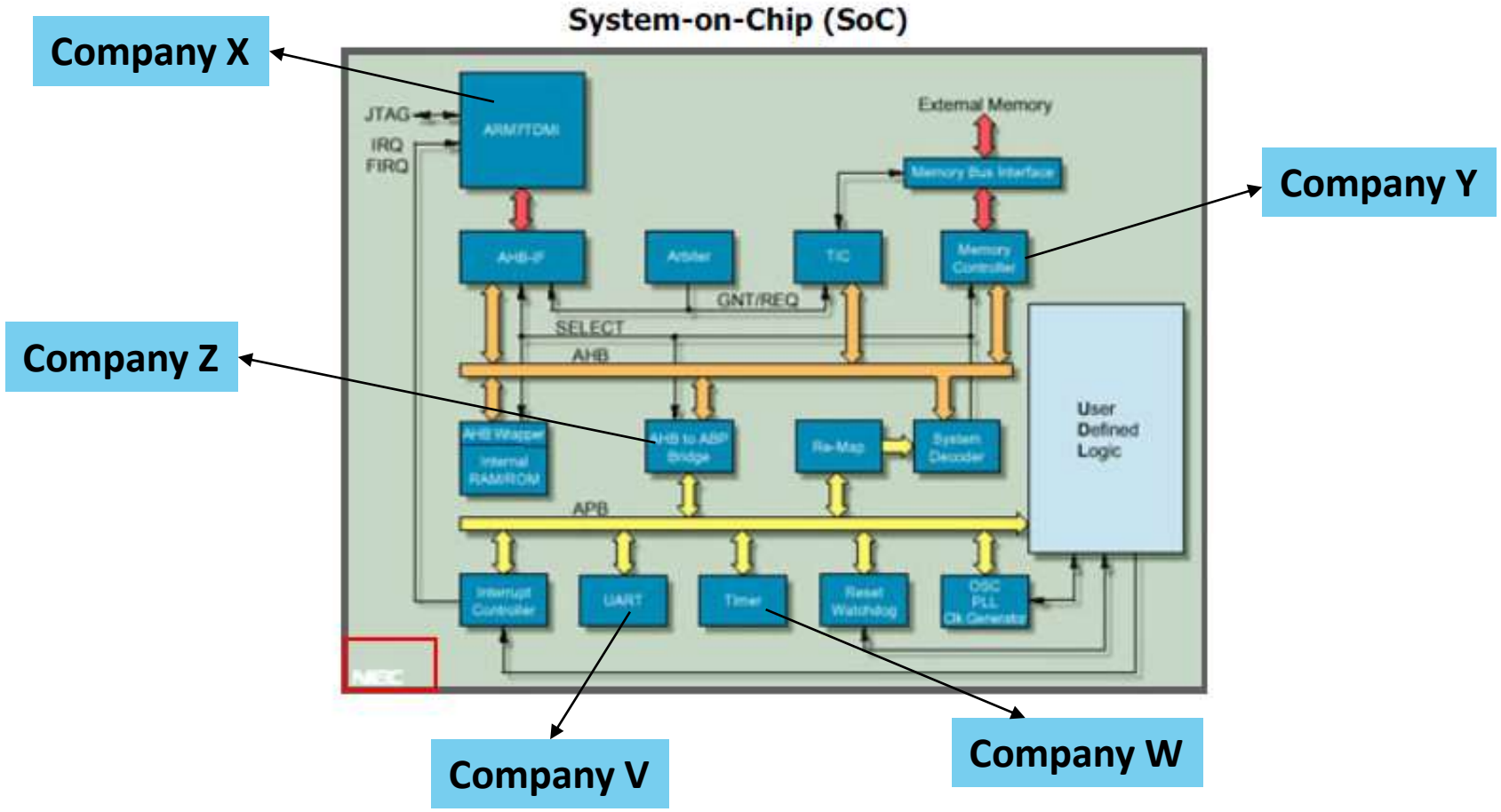
Foundry service for Universities, research centers and Small Medium Enterprises in Europe with Multi Wafer Approach for low-volume production
AMS, STMicroelectronics, UMC, TSMC, IHP, ….. from 2 um (Power ICs) to 7 nm (DSP, HPC,..)
The cost of building a new foundry in a scaled node is in the order of Billions of USD

Today most advanced production is 4nm TSMC and INTEL (in Europe is GF12nm in Dresda)

https://europractice-ic.com/



Today SoC are a combination of multi-party Intellectual Property (IP) Macrocells (soft macro, i.e. RTL IPs or GL IPs; hard macro, i.e. layouted IP) → Issues with Third-Party IP Cells Design



An IP at back end level (technology dependent) is hard macro.
An IP at RTL or GL before layout, you call that soft IP (macro).
Hard IP is locked in a technology and config. A soft IP can be implemented on different tech.

Soft Macro

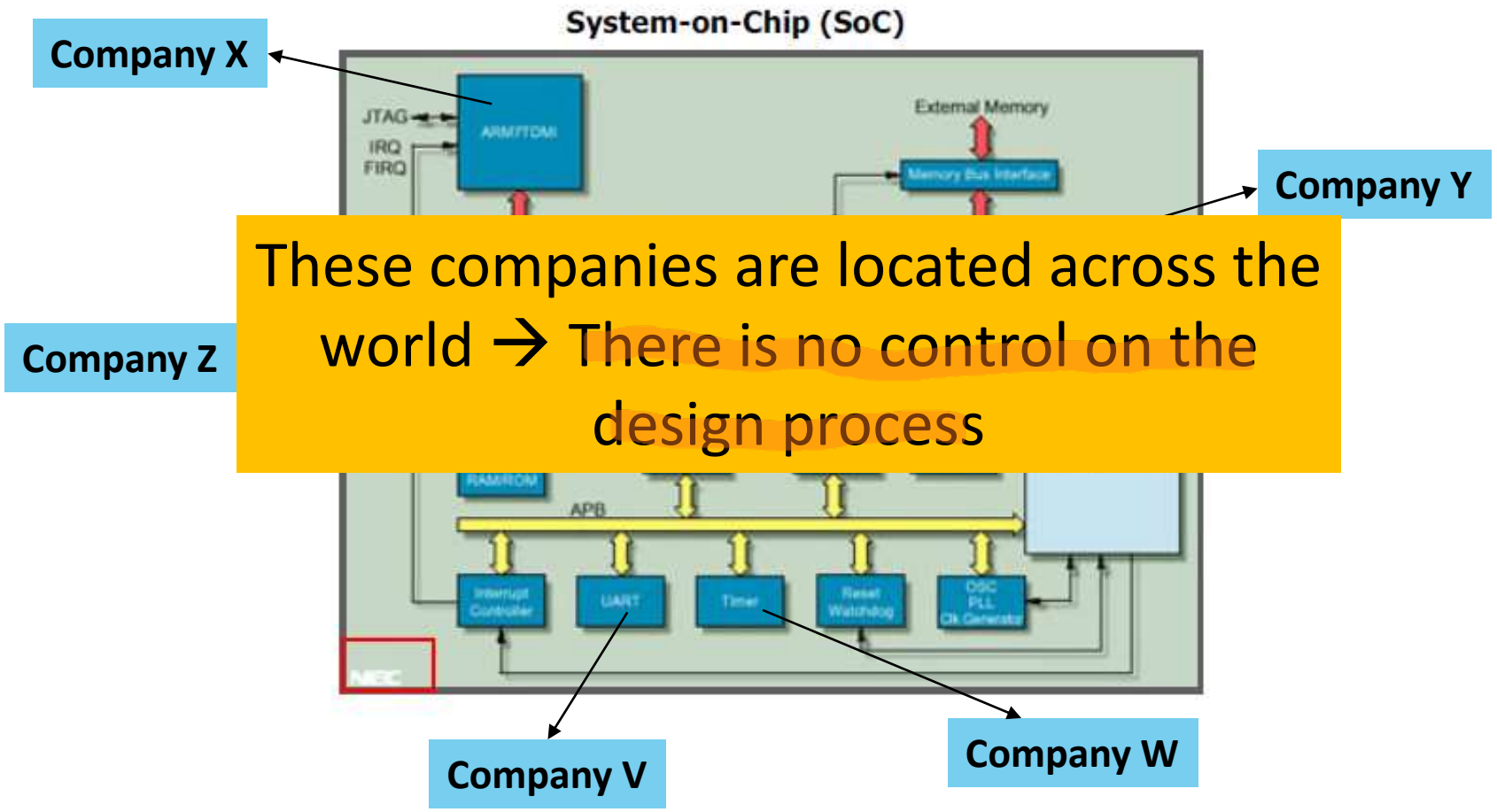
- **Description**: A **soft macro** is a high-level, technology-independent design, usually provided as **RTL code (Verilog/VHDL)** or synthesized **gate-level netlists**.
- **Flexibility**: Since it's not tied to a specific **process node** (e.g., 5nm, 7nm), designers can **modify, optimize, and synthesize** it for different manufacturing technologies.
- **Usage**: Used for **standard logic**, ALUs, multiplexers, and other parts of a design that need customization or tuning.

Hard Macro

- **Description**: A **hard macro** is a fully **placed, routed, and technology-dependent** design, often delivered as a **GDSII or OASIS** file, which contains detailed layout information.
- **Tied to Technology**: It is designed for **a specific process node (e.g., TSMC 5nm, Samsung 7nm)**, meaning its **transistor sizes, routing, and layout constraints** are locked to that node.
- **Why It's Rooted in Technology and Configuration**:
  - The **physical layout** is **optimized** for the **electrical, thermal, and power** characteristics of a specific manufacturing process.
  - **Fixed transistor placements and routing** ensure predictable performance, power consumption, and area (PPA).
  - They **cannot be modified easily** without a full redesign because their geometry follows strict **foundry design rules**.
- **Usage**: Used for **memory blocks (SRAM, ROM), analog circuits (PLLs, ADCs), high-speed interfaces (SerDes, PCIe), and custom processors** where performance and power efficiency matter.

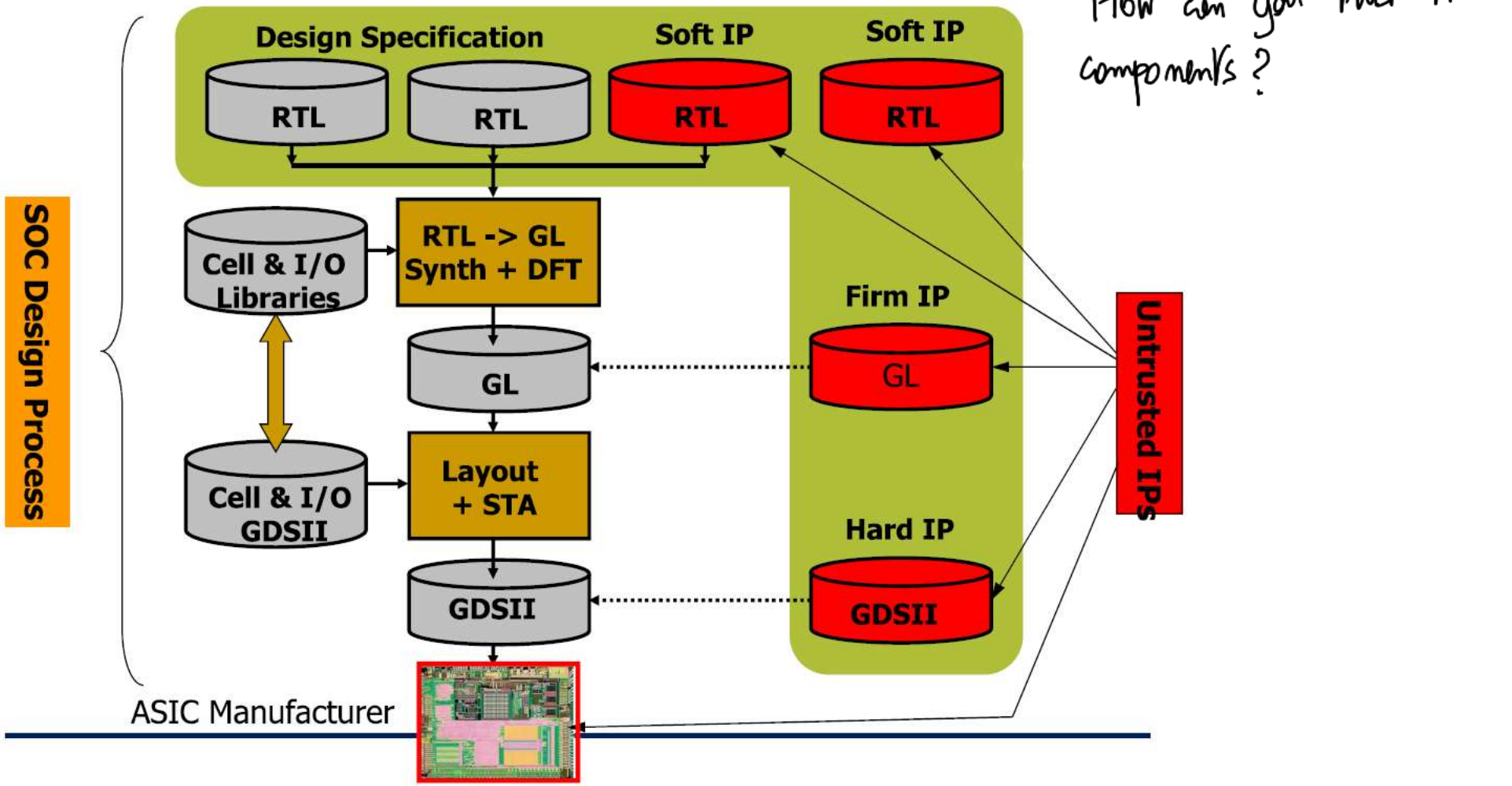
Who Develop the IPs? Who Design the ICs? Who Fabricate them?

Issues with Third-Party IP Design

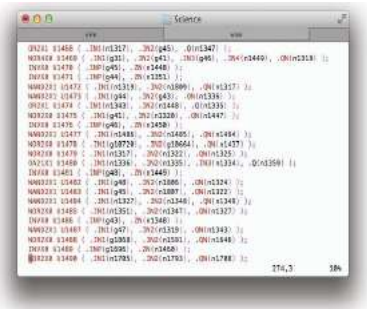


Issues with Third-Party IP Design

How can you trust these components?

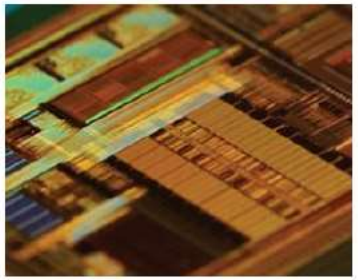


HW Threats



IP Vendor

System Integrator



Manufacturer

Any of these steps can be untrusted

IP Vendor

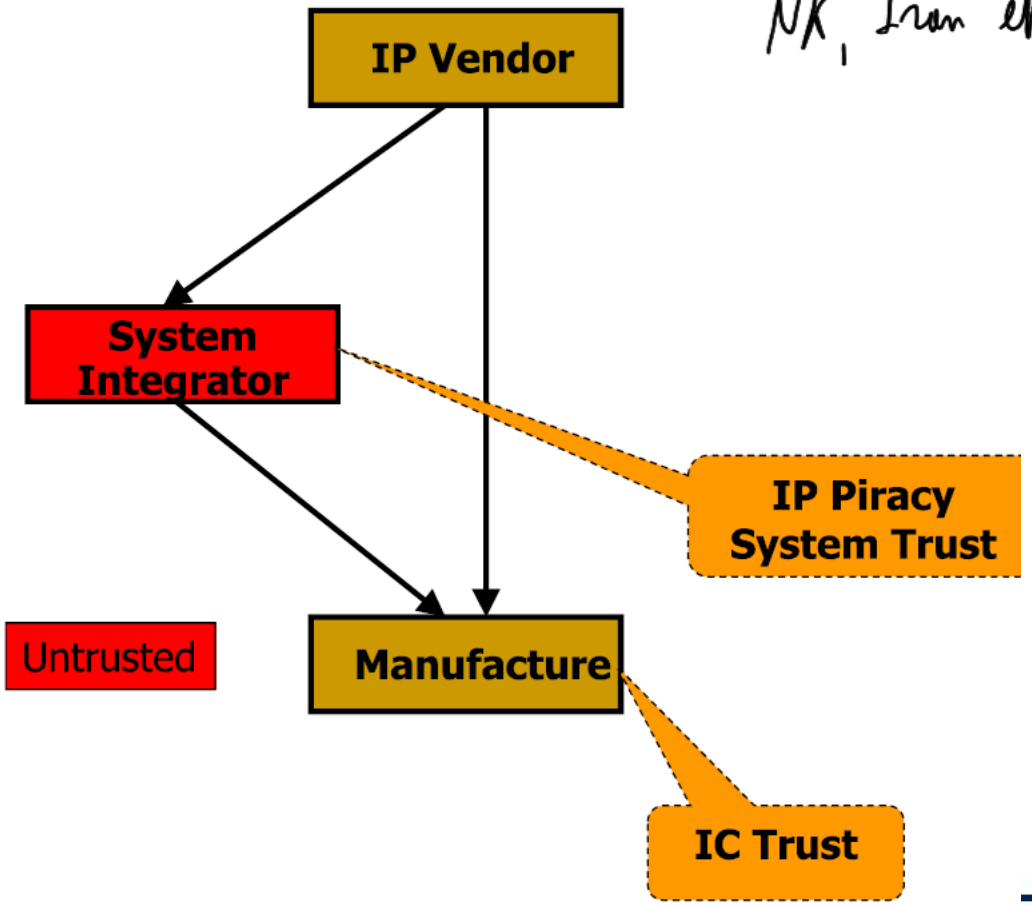
System Integrator

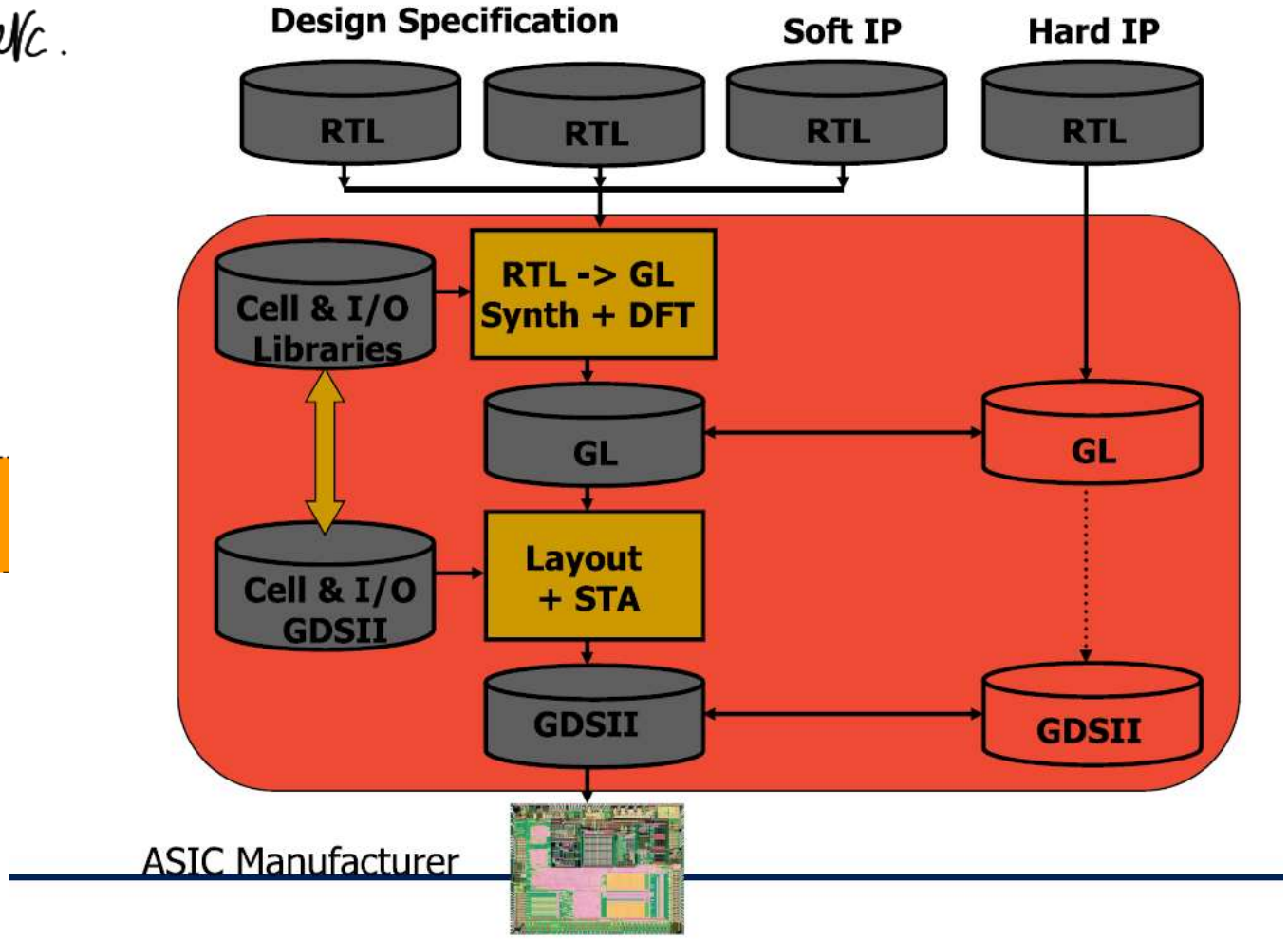
Manufacture

Untrusted

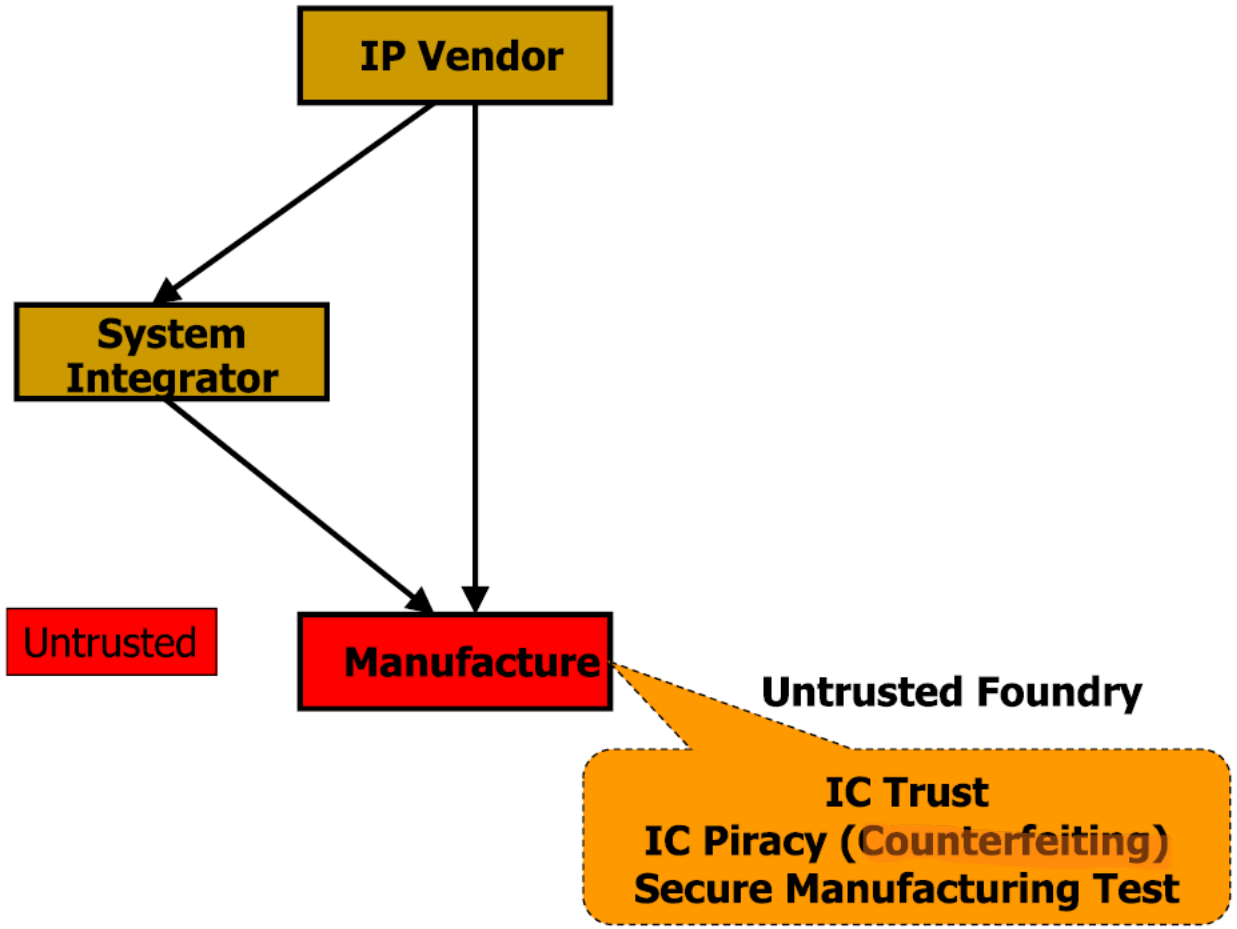
Maybe as an IP vendor you will have to respect some rules (no selling to Iran if you are in a western countries), but maybe a system integrator, with low control, will make chips for that country too: ex. a company from Turkey takes your solution and uses it for NK, Iran etc.

HW Threats





HW Threats


IP Vendor
System Integrator
Untrusted
Manufacture
Untrusted Foundry
IC Trust
IC Piracy (Counterfeiting)
Secure Manufacturing Test

1. *IP Vendors (Intellectual Property Vendors)*

- Provide **pre-designed, reusable building blocks** (IP cores) that SoC designers integrate into their chips.
- These can be **processors (e.g., Arm Cortex, RISC-V cores), memory controllers, interfaces (PCIe, USB, Ethernet), AI accelerators, and DSPs**.
- Examples: **Arm, Synopsys, Imagination Technologies, Cadence, CEVA**.

2. *System Integrators (SoC Designers / ASIC Design Houses)*

- Take IP cores from vendors and **combine them into a complete SoC** by integrating CPU, memory, peripherals, and communication interfaces.
- Optimize the design for **power, performance, and area (PPA)**.
- Handle RTL coding, logic synthesis, verification, and physical implementation.
- Examples: **Apple, Qualcomm, NVIDIA, Broadcom, AMD**.

3. *Manufacturers (Foundries / Fabrication Companies)*

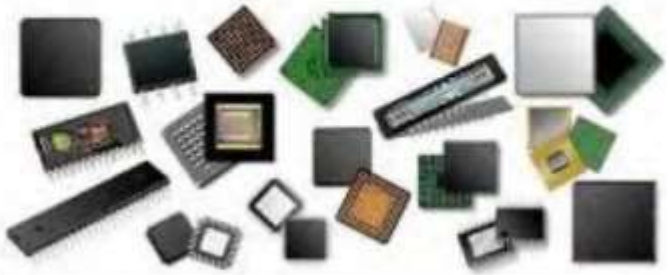
- Physically manufacture the SoC using **semiconductor fabrication processes** (e.g., 3nm, 5nm, 7nm).
- Require a **cleanroom environment and advanced photolithography tools**.
- Examples: **TSMC, Samsung Foundry, Intel Foundry, GlobalFoundries, UMC**.

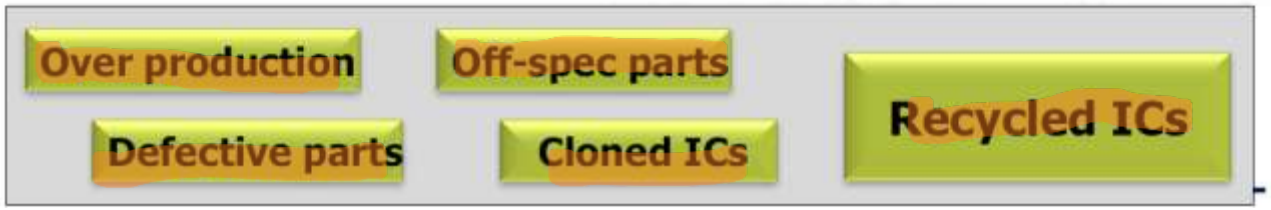
Main Hardware Security Threats due to Unsecure (Untrusted) Supply Chain

Counterfeiting

Main threats: people that want extra money

- Most prevalent attack today
- Unauthorized production of wafers
- It is estimated that counterfeiting is costing semiconductor industry more than several billion dollars per year





Hardware Trojan Horses

- A Hardware Trojan Horse is a malicious modification of an integrated circuit
  - Performed at any design and/or manufacturing step
- A real threat?
  - Few real cases… discovered!
  - A big fear!!

- Can be timely activated, by event or by external code activated

Main Hardware Security Threats due to Unsecure (Untrusted) Supply Chain

- If you are sceptical about the actual impact of hardware Trojans (many people are), spend some time to read through the story at the following links

  https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

  https://www.google.co.uk/amp/s/gigazine.net/amp/en/20181010-supermicro-motherboard-attack

- HW Trojans (examples and mitigation strategy) will be further discussed by Prof. Daniele Rossi in his lessons

Make or Buy Integrated Circuits

Make or Buy Integrated Circuits

A company producing system-level products using PrintedCircuitBoards and Integrated Circuits (Processors, memories, crypto accelerators, graphic accelerators, networking devices,…) always has this dilemma:

Buying integrated circuits purchasing them from Commercial components available in the market, these components are called COTS (Components Off The Shelf)- in Italian Componenti dallo Scaffale?

MAKE: you have more control over it, it is tailored for you
Select a semiconductor company partner and making (i.e. designing and manufacturing) an ASIC, i.e. Application Specific Integrated Circuit has a high fixed costs called NRE (Non Recurrent Engineering) costs for chip design, set-up the foundry while the cost to be paied for each new device, called RE (Recurrent Engineering) costs, is small (since in terms of materials are few mm2 or cm2 of materials like silicon, plastic, ….).

The unit cost U for the production of N devices is
U=RE+NRE/N
If for example RE is 0.1 € for a new device and NRE is 2 M€
U= 0.1 € + 2 M€ /N

Electronic is characterized by a fixed NRE in the order of million of euros (setup of masks, set up the foundry etc.). After setup, the cost of the chip is very low.

U = Recurrent engineering cost + NRE/N.

So cost is low for unit if you produce a lot of them but you have an entry cost of Millions.

Make or Buy Integrated Circuits

Applying the equation U= 0.1 € + 2 M€ /N
We have that for N=1 device the cost for the device is 2 M€
For N=1K devices the cost for each device is 2000 €
For N=1 Million devices the cost for each device is 2.1 €
For N=10 Millions devices the cost for each device is 0.3 €
For N=100 Millions devices the cost for each device is 0.12 €

BUY

If instead you buy the device designed by a compnat for the whole market the initial unit cost low, but it is affected slightly by the increase in devices acquired.
E.g. a device with initial cost of 6 € may is linearly reduced at 4 € (33% savings) if you buy N=1 Million devices
This means that at N=500K devices the cost with the approach MAKE is 0.1 € + 2 M€ /500K=4.1 € while with BUY we have 5 €.

Initial cost is very low (and if you buy a lot they will make you a discount), but you will never arrive at what you get with MAKING it.

Counterfeit ICs

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

① ↑ Research and development costs.

① There is enough electronics to counterfeit!

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 defence system
  - To contaminate one **company's reputation**
  - To kill the **market share** of one company
  - …

An Interesting Story (I)

- **November 8, 2011**, the United States Committee on Armed Services held a hearing on an investigation of counterfeit electronic parts in the **defense supply chain**

- The investigation had revealed alarming facts:
  - Materials used to make counterfeit electronic (a.k.a. e-waste) parts are shipped from the United States and other countries…

http://www.industryweek.com/procurement/ticking-time-bomb-counterfeit-electronic-parts

An Interesting Story (II): Recycling

- The e-waste is sent to cities like Shantou, China, where:
  - It is disassembled by hand, washed in dirty river water, and dried on the city sidewalk
  - It is sanded down to remove the existing part number or other markings that indicate its quality or performance
  - False markings are placed on the parts that lead the average person to believe they are new or high-quality parts

http://www.industryweek.com/procurement/ticking-time-bomb-counterfeit-electronic-parts

An interesting Story (III): Recycling Process

The Chip Crisis in 2021

- Chips shortage represents a great opportunity for counterfeiters!

WSJ, Jul 15, 2021: **What's Worse Than a Chip Shortage? Buying Fake Ones**

https://www.wsj.com/articles/chip-shortage-has-spawned-a-surplus-of-fraudsters-and-fake-parts-11626255002

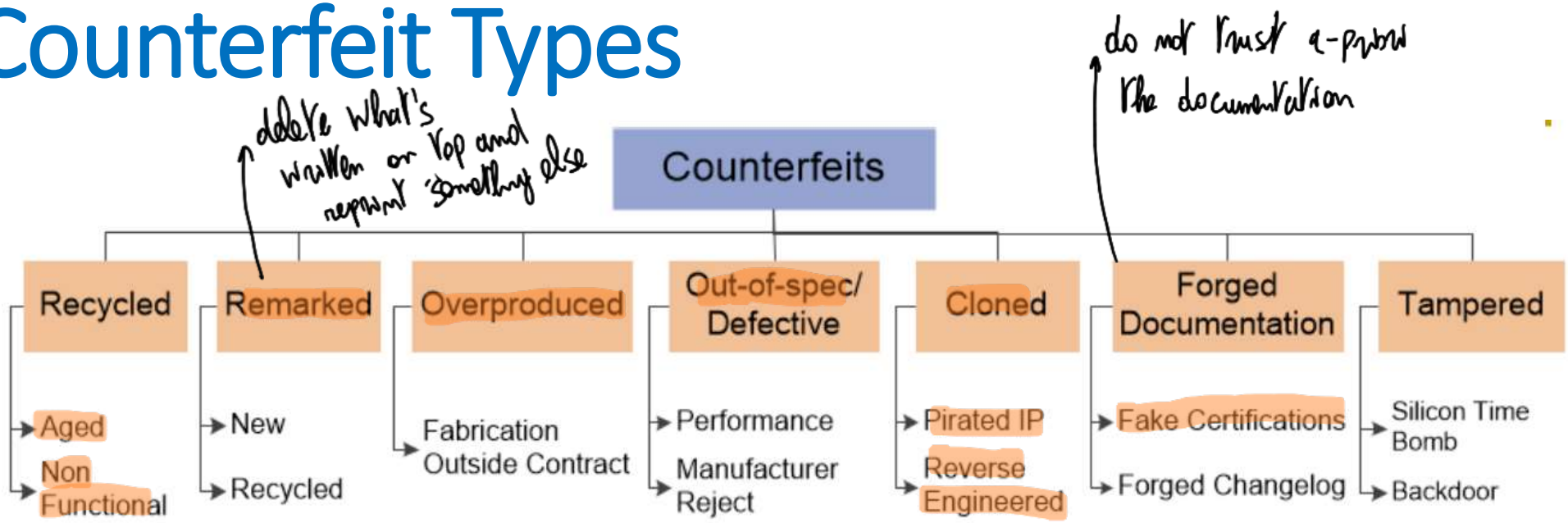
Forbes, Aug 12, 2021: **Protecting Your Production From The Risks Of Grey Market Devices**

https://www.forbes.com/sites/marcoannunziata/2021/08/12/protecting-your-production-from-the-risks-of-grey-market-devices/?sh=d21dacab350b

eeNews Europe, Sep 24, 2021: **Counterfeit chips flood in to exploit chip shortage**

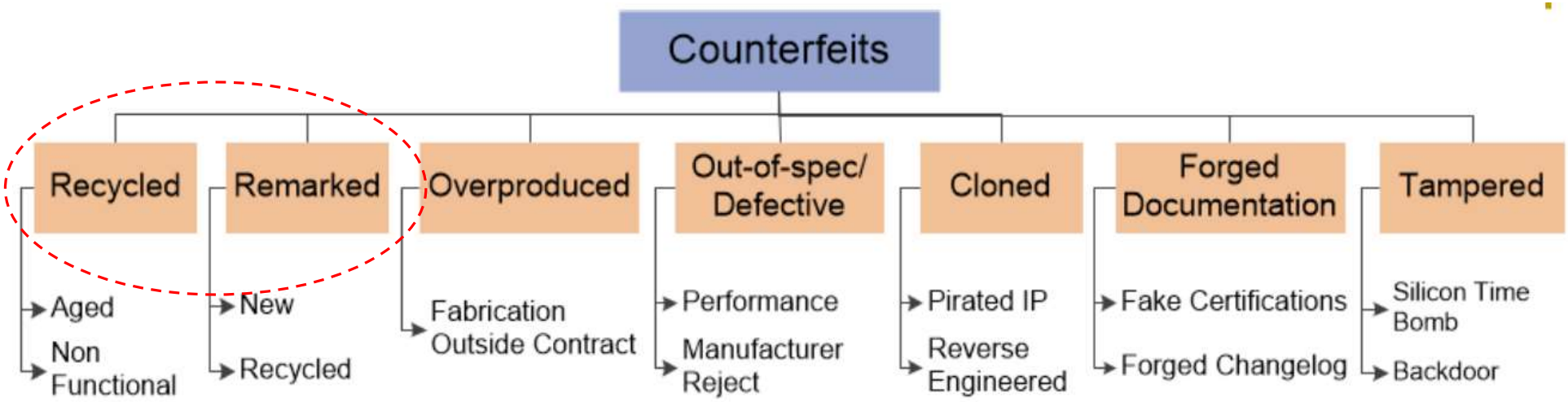
https://www.eenewseurope.com/news/counterfeit-chips-flood-exploit-chip-shortage

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

Counterfeit Types



For these, there isn't a real control of waste management

- More than 80% of the counterfeit components are recycled
- Most of the recycled parts are at the end of life → damaged considerably due to usage and aging

Counterfeit Electronic Parts

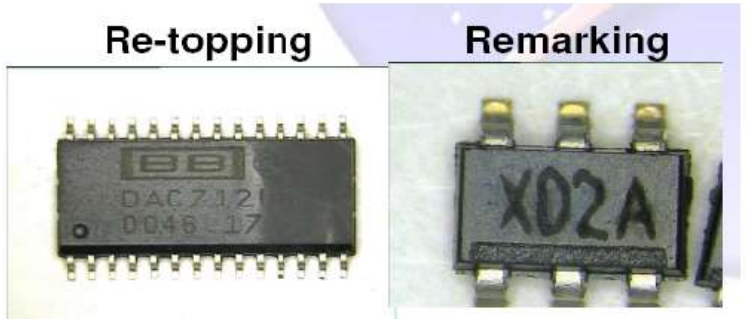
- A counterfeit component
  - is an unauthorized copy,
  - does not conform to OCM (Original Component Manufacturer) design, model, or performance standards,
  - is not produced by the OCM,
  - is out-of-specification, defective, or a used OCM product sold as new,
  - has incorrect or false markings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

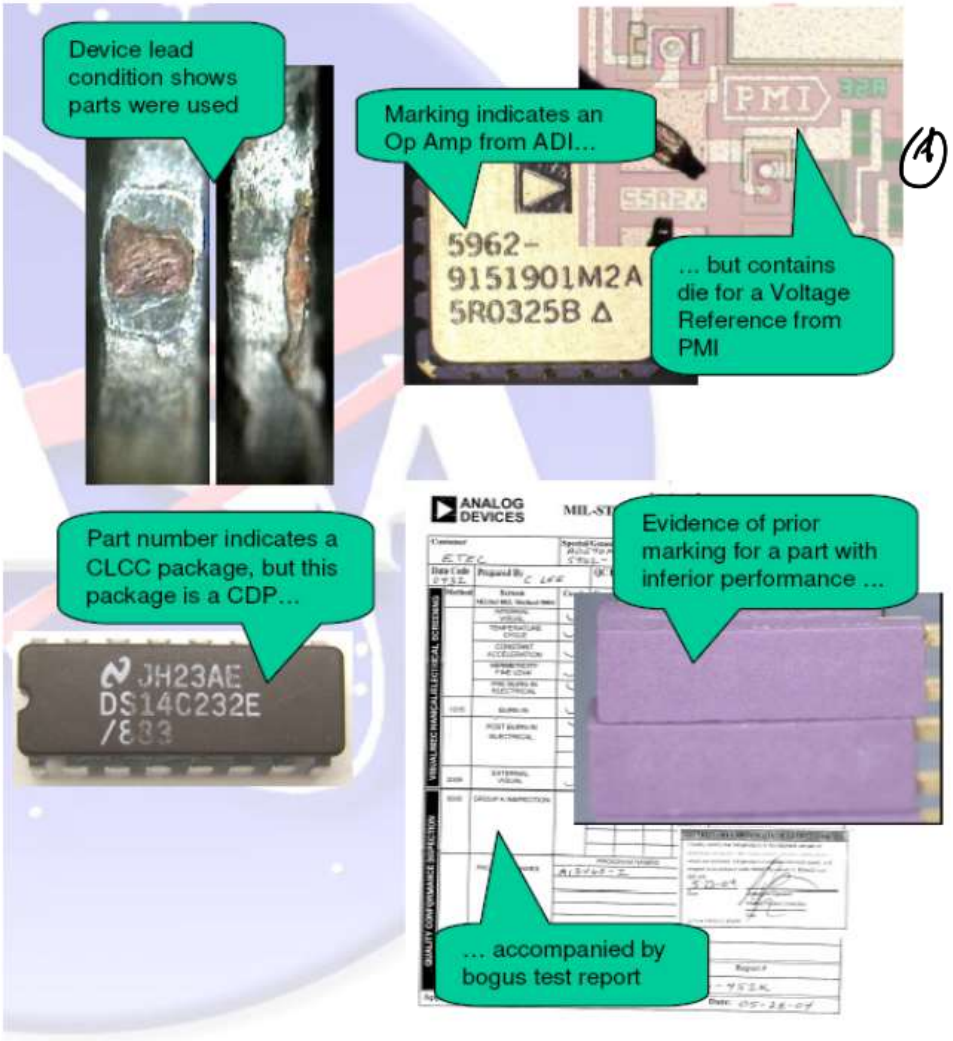
OCM: Original Component Manufacturer

Is there a way to understand if you are dealing with counterfeits?

Counterfeit Electronic Parts - Examples

- 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



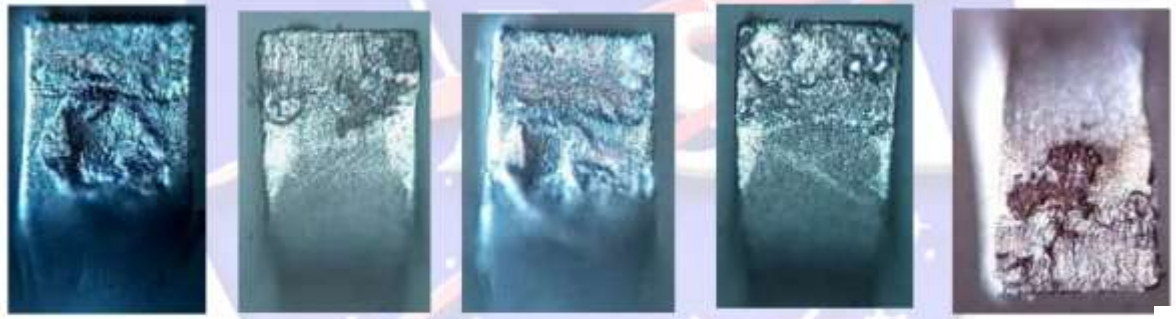


- Visual test: check the marking, if they are damaged, remarked. If the lead is damaged this can show that probes were used. So you might have a very convenient vendor, but spending money to check what you're getting can be worth it.
- Understand if codes for marking are correct!

① On with XRAY analysis you discover that inside a chip you have something you shouldn't have.

- Can I get in touch with the person that signed the testing document?

Examples



Poorly manufactured or damaged leads

Incorrect decive leads

Non-gold leads

Gold leads on real device

Examples

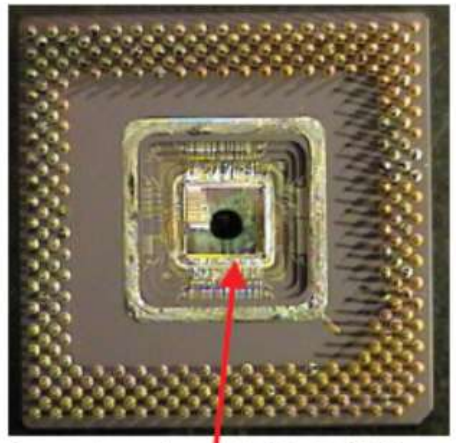
Dual marking

Good part has only two lines of marking

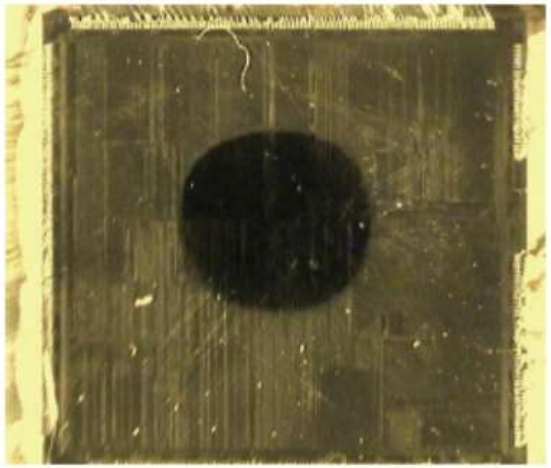
Photo of suspect part.

Photo of Known Good Part.

Examples



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

Main Counterfeiting Issue: Recycling

Between 2005-08, 55% of microcircuit producing companies found counterfeit copies in open market (US Dept. of Commerce)

Estimated loss to the US economy was $7.5 billion per year (EE Times 2017)

- **More than 80%** of the counterfeit components are **recycled**
- In 2019, only **17.4%** of 2019's e-waste was formally collected and recycled worldwide, with Europe leading this chart with 42.5% of its total e-waste generated (https://theconversation.com/global-electronic-waste-up-21-in-five-years-and-recycling-isnt-keeping-up-141997).
- Most of the recycled parts are at the end of life → damaged considerably due to usage and aging

IC Recycling Process

- 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

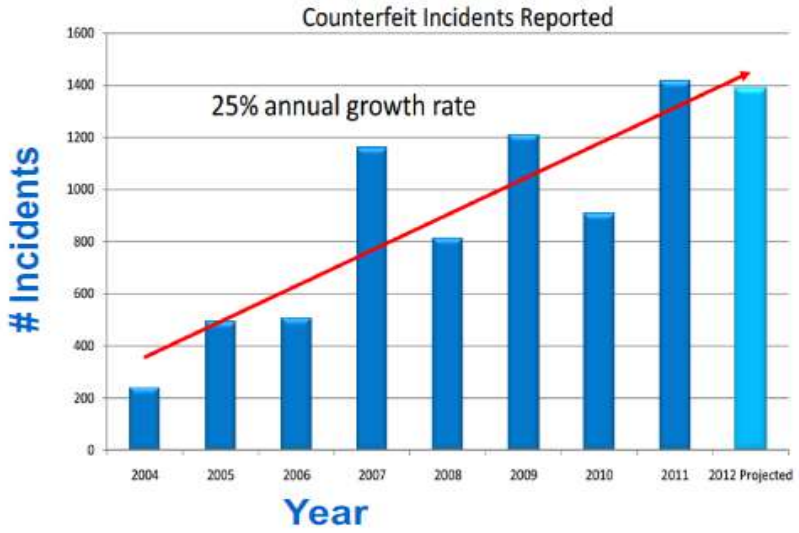
- Consumer trends suggest that more gadgets are used in much shorter time

more e-waste !

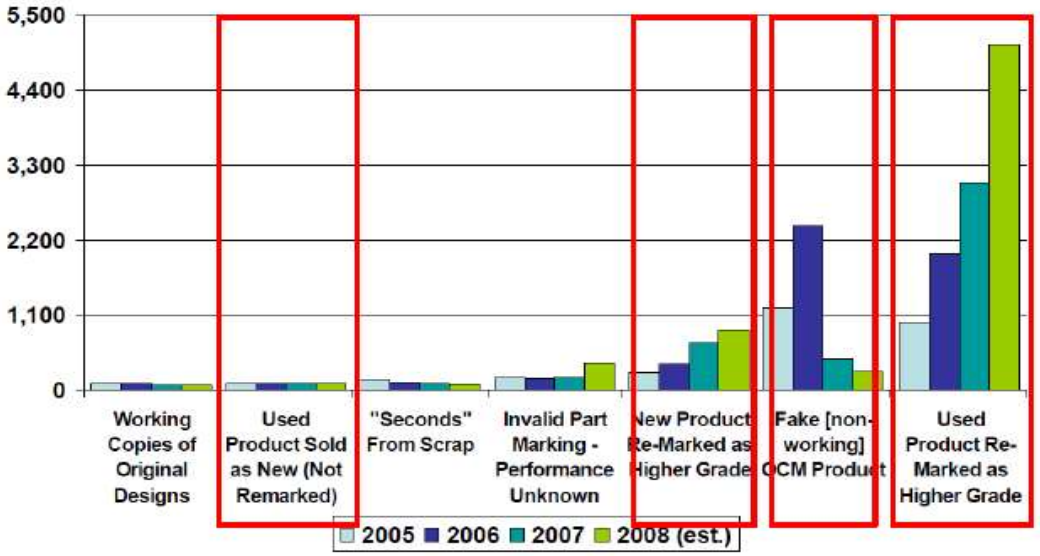
Recycled and Remarked ICs

- 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



Source: IHS 4/2012



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 (v3 sold as v7)
  - New Components, to change the specification of the component (commercial grade military grade) (1)
- **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

When you buy a chip

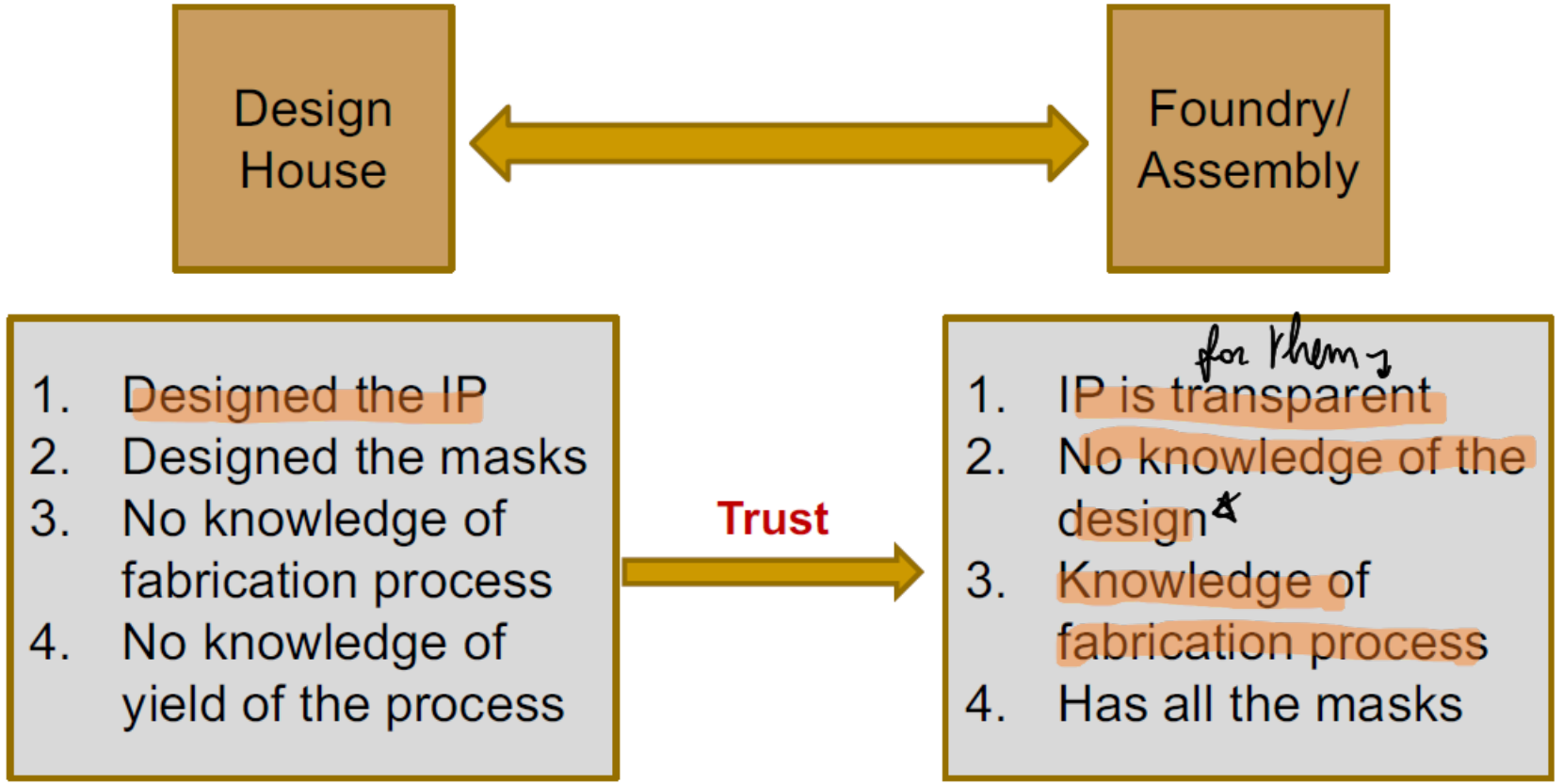
One risk is that chip is real and new, but maybe even distributor, changes the code to sell it for higher performances that it can sustain. ①
You pay for military grade a commercial grade. Difficult to test.

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).

* To protect your IP you should give the foundry no knowledge of the design.

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

What are other tests you can do for defective parts?
With aging, the leakage current increases.
↳ So if you don't pass tests, this can be a sign of out-of-spec or recycled. This is a cheap test you can do.

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 in 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.

↳ Check power consumption with your specifications.

① ②

① Dynamic current depends on how you stimulate your component.
② You can still check performances. If your chip crashes at 3.5 GHz it's okay, if it can't you can have a sign of aging.

Out-of-spec/Defective

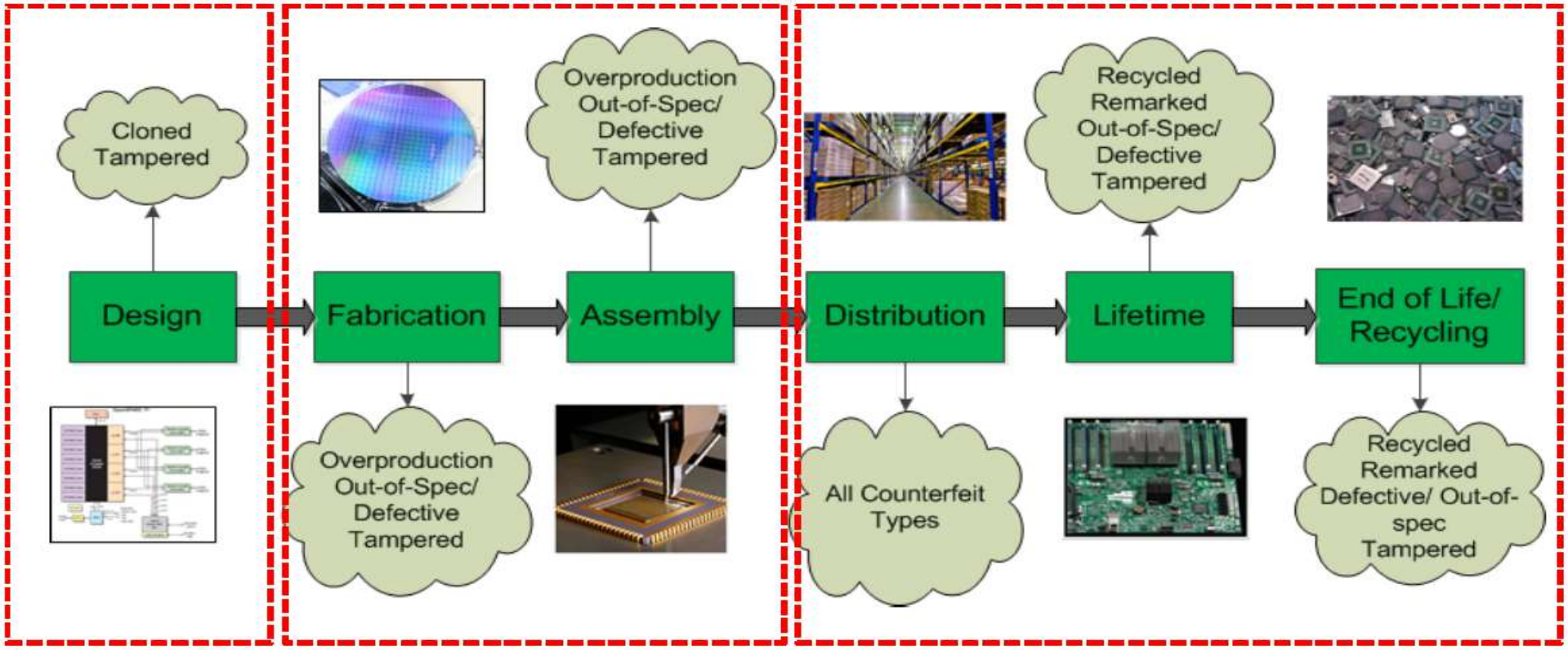
- **Unauthorized production of a part**
  - Difference between **overproduction** and **cloned** is that cloned parts do not have the authorized IP, could be fabricated in a different foundry
- **Cloned parts**
  - **Pirated IP** → Counterfeiters acquire the IP in an illegal manner (saved the design cost of the IP).
  - **Reversed Engineered** → Counterfeiters reverse engineer the design and make a new one just like the original design

1. **Overproduction:** This occurs when an authorized manufacturer produces more units than they are contractually allowed to, often without the knowledge or consent of the intellectual property (IP) owner. These excess units may be sold on the gray market. Even though they are made using the original process and materials, they can still be unauthorized and may lack official quality control.
2. **Cloned Parts**: These are fully unauthorized copies of a component, meaning they are manufactured without access to the original design files or proper licensing. Since they don't have the authorized IP, they are often reverse-engineered or based on stolen designs. Cloned parts can be made in a completely different foundry with unknown materials and processes, which can lead to significant differences in quality, reliability, and security.

Forged Documentation

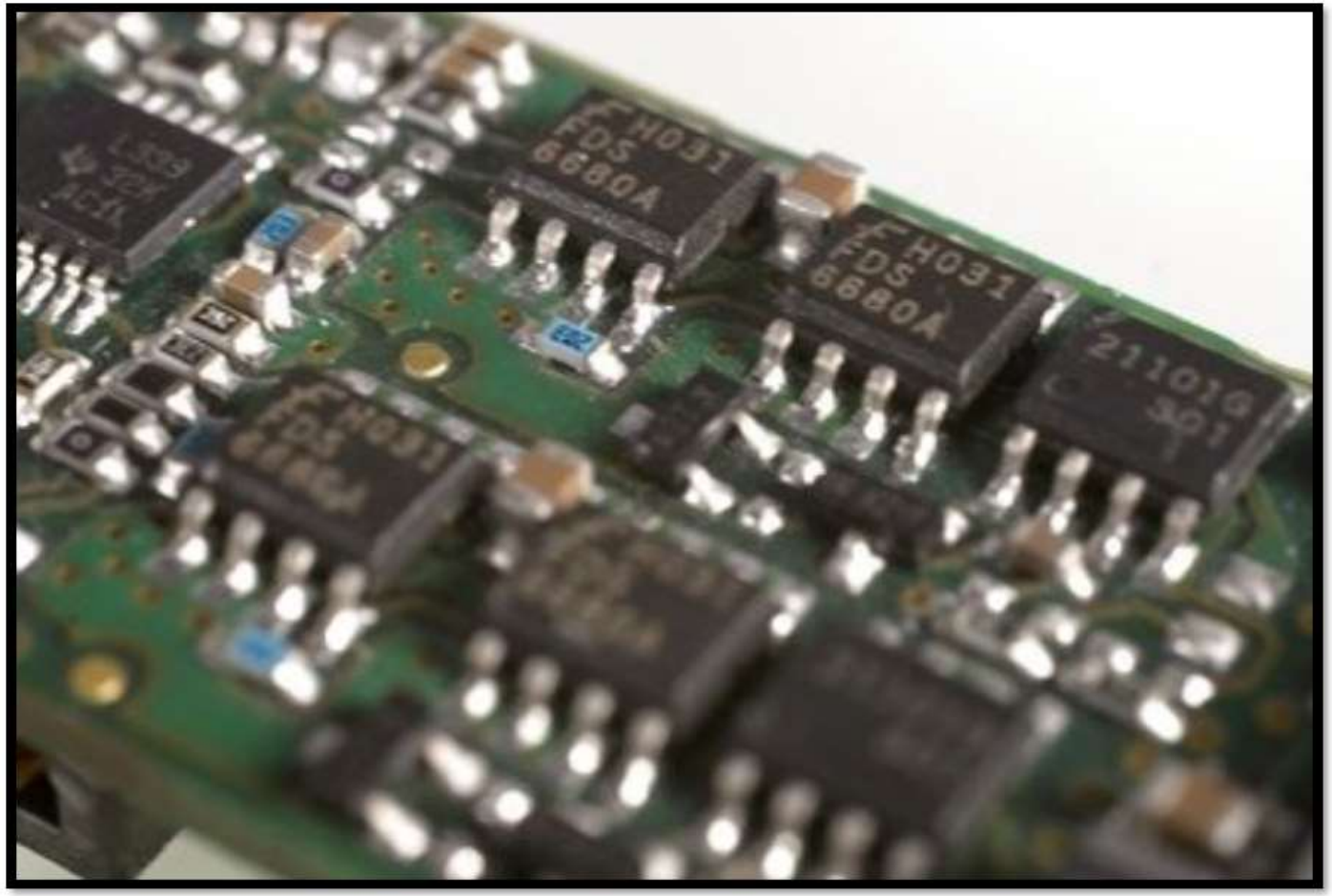
- The mismatch of specification documents between the purchased parts with the OCM (Original component manufacturer).
- Easy to detect as usually the original documents are present somewhere
- Old parts (parts in the supply chain for around several years) have the higher probability of getting counterfeited

Supply Chain Vulnerability: Let's Recap



Understand different points and risks.

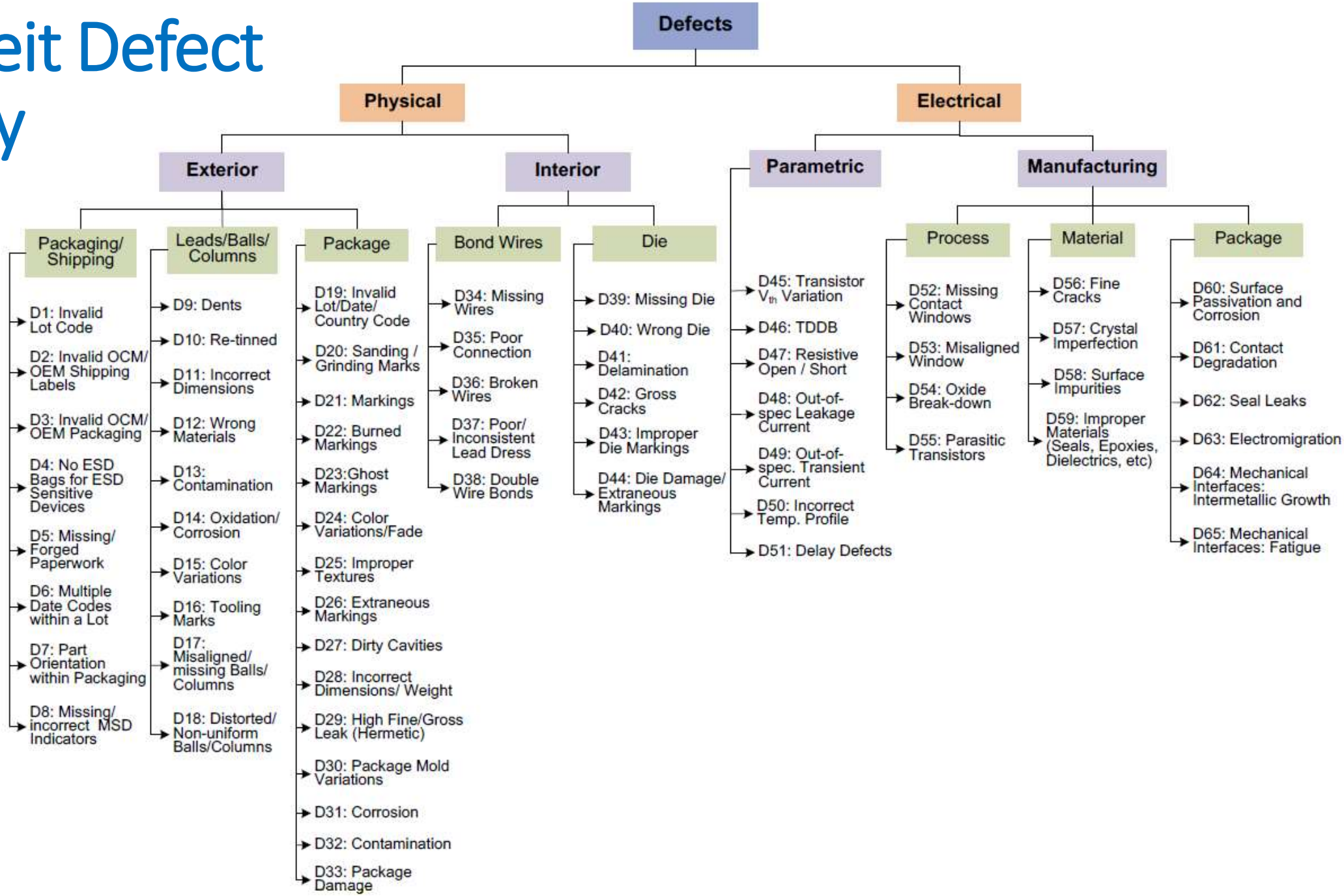
Counterfeits are Defective!



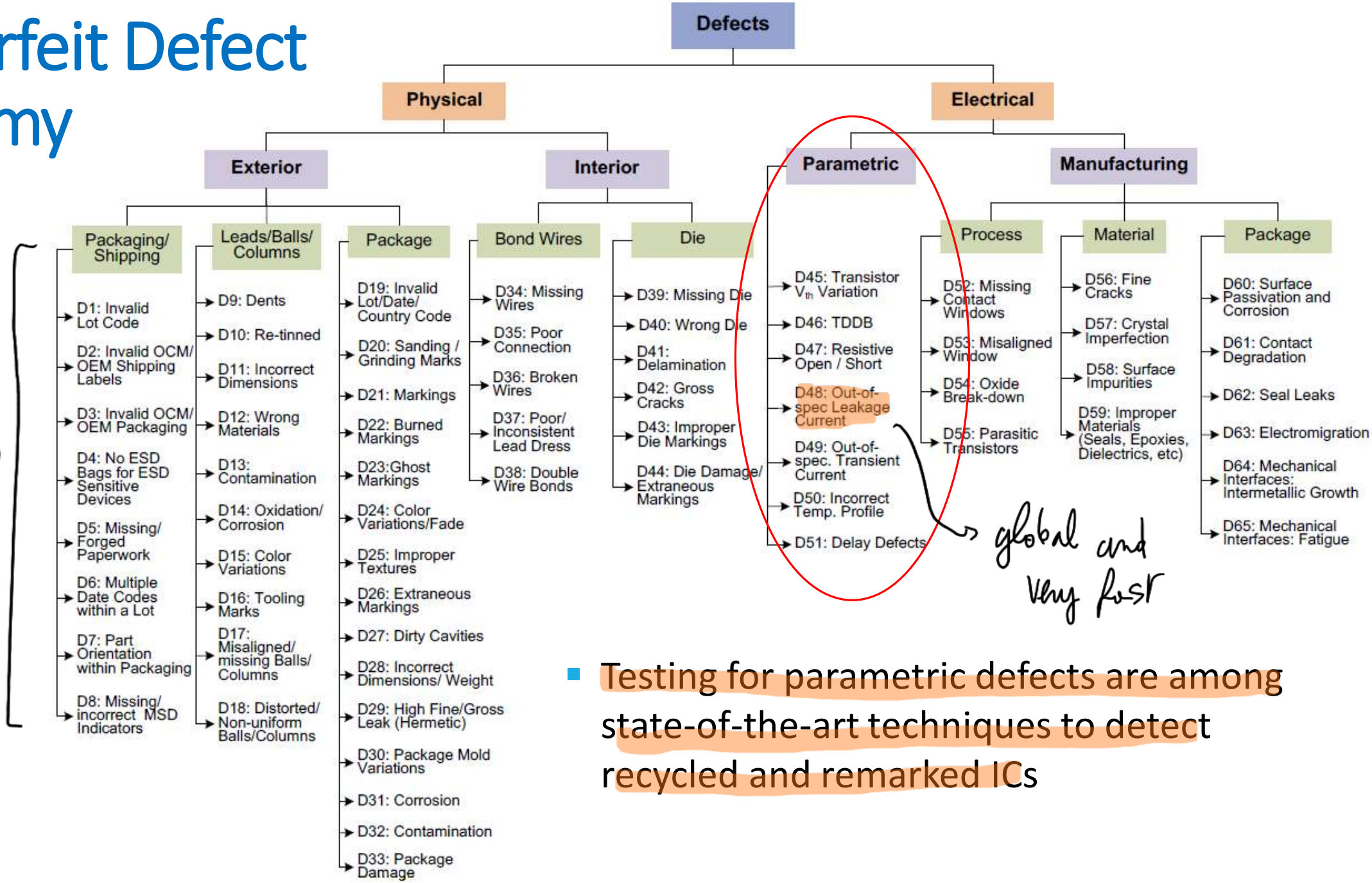
Countermeasures? Main ones: audit for trusted partners

Analysis and detection to check for trusted partners in HW purchasing and/or in IP design and/or chip manufacturing, packaging, assembling, testing, recycling, etc.

Counterfeit Defect Taxonomy



Counterfeit Defect Taxonomy



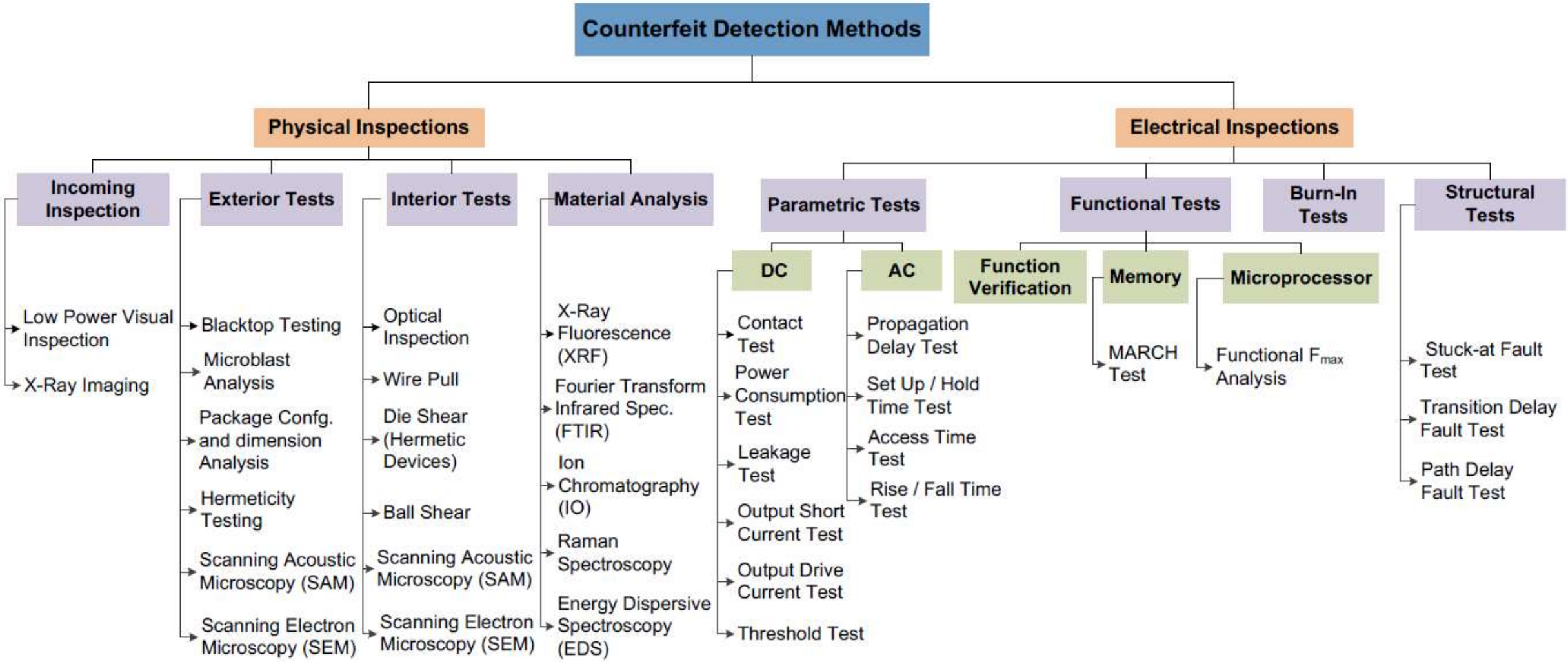
Checking these is too costly! You have the tradeoff of how much you want to spend to be secure

global and very fast

- Testing for parametric defects are among state-of-the-art techniques to detect recycled and remarked ICs

Testing for Defects

Detection Method Taxonomy



→ At least do this: basic approach: you can see broken leads, fake marks

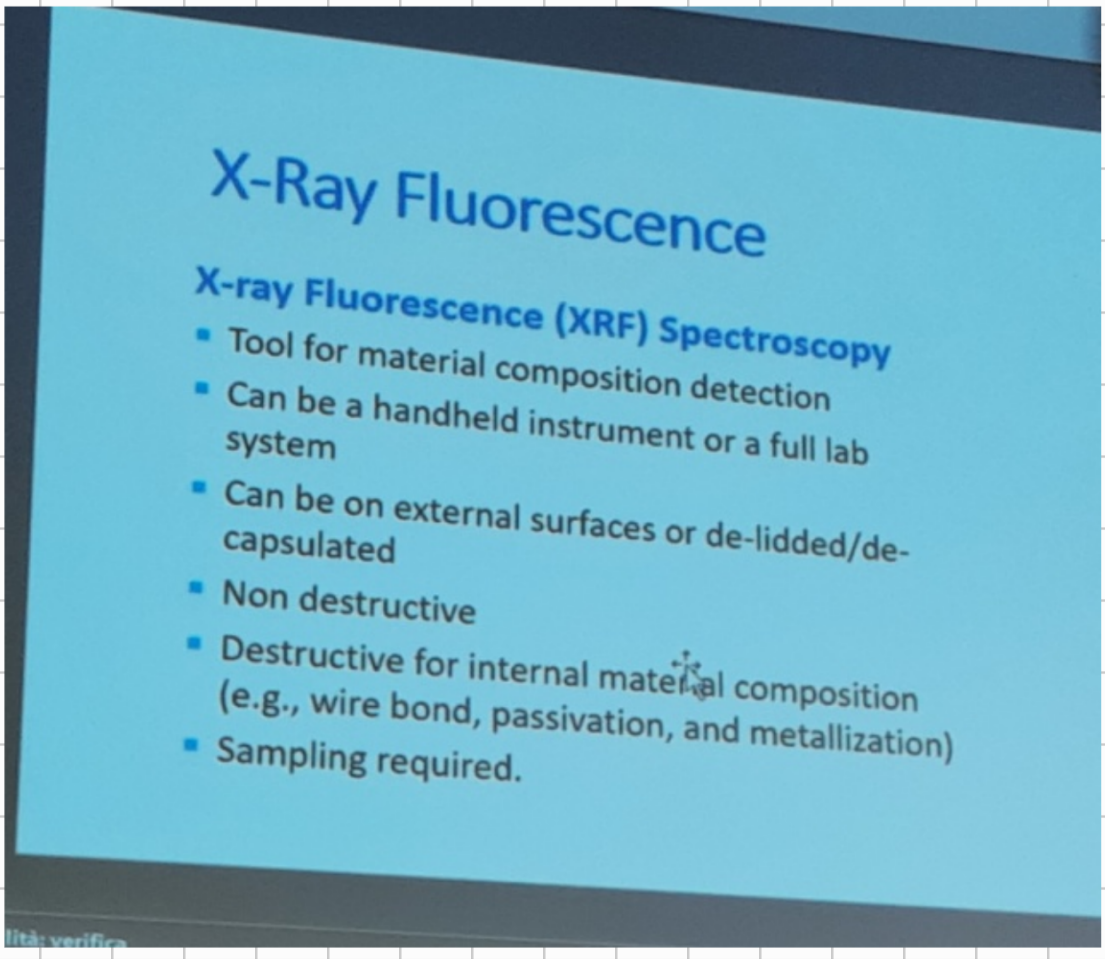
External Visual Inspection (EVI)

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. You have standards! You can claim to do EVA according to standards.

Burned markings from low quality laser

IDEA-STD-1010: Acceptability of Electronic Components Distributed in the Open Market is the first and leading quality standard for the visual inspection of electronic components and was designed as a technical resource to serve the electronic component industry regarding the detection of substandard and counterfeit components.

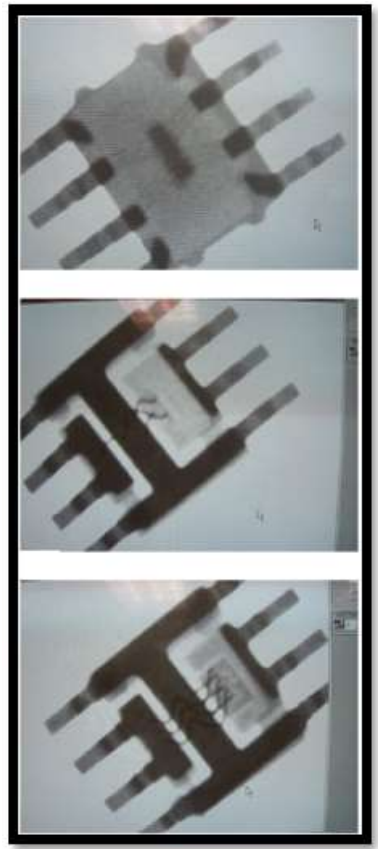

X-Ray Fluorescence
X-ray Fluorescence (XRF) Spectroscopy
Tool for material composition detection
Can be a handheld instrument or a full lab system
Can be on external surfaces or de-lidded/de-capsulated
Non destructive
Destructive for internal material composition (e.g., wire bond, passivation, and metallization)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

X-Ray Inspection

You can see if you have things inside the package, if the size is what you expect...

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



- The value of X-ray is increased when there is a known good OCM device available for comparison of internal details

1. **Die Size and Placement:**
    - Authentic components have a die (the actual silicon chip inside) that matches the manufacturer's specifications.
    - Counterfeits may have a smaller die, misalignment, or even no die at all (e.g., a dummy chip).
2. **Bond Wire Integrity:**
    - Bond wires connect the die to the package leads.
    - In counterfeit or cloned chips, these wires may be missing, misrouted, or inconsistently placed.
3. **Package and Lead Frame Differences:**
    - Counterfeit chips might use recycled or repainted packages, which could have different internal structures.
    - Voids, cracks, or inconsistencies in lead frames can indicate tampering or poor-quality manufacturing.
4. **Component Density and Layout:**
    - Genuine chips have well-organized internal layouts.
    - Cloned or overproduced parts might have different arrangements due to being fabricated in unauthorized facilities.

Low Power Visual Inspection

Sample 1	Sample 2	Sample 3	Sample 4	Sample 5
				

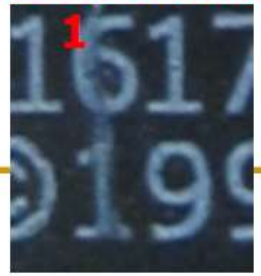
Observations:

All Samples look the same at Camera level

Except for :

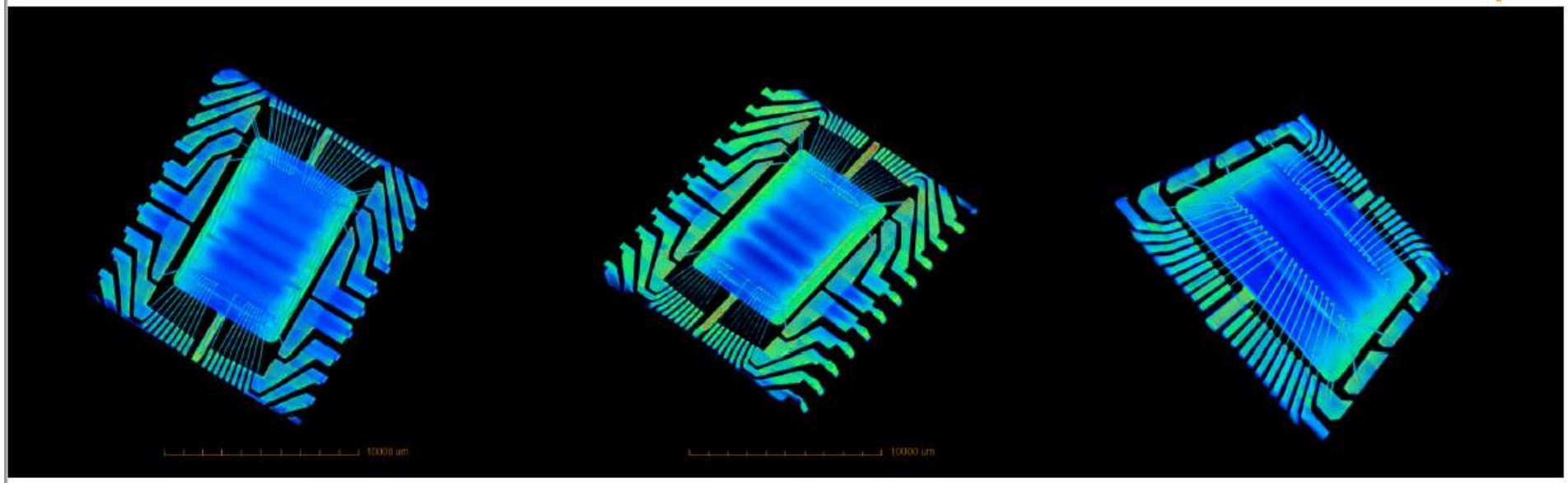
Sample 3 has a scratch on markings starting with U

Sample 2 scratch on marking over numbers 6 and 1

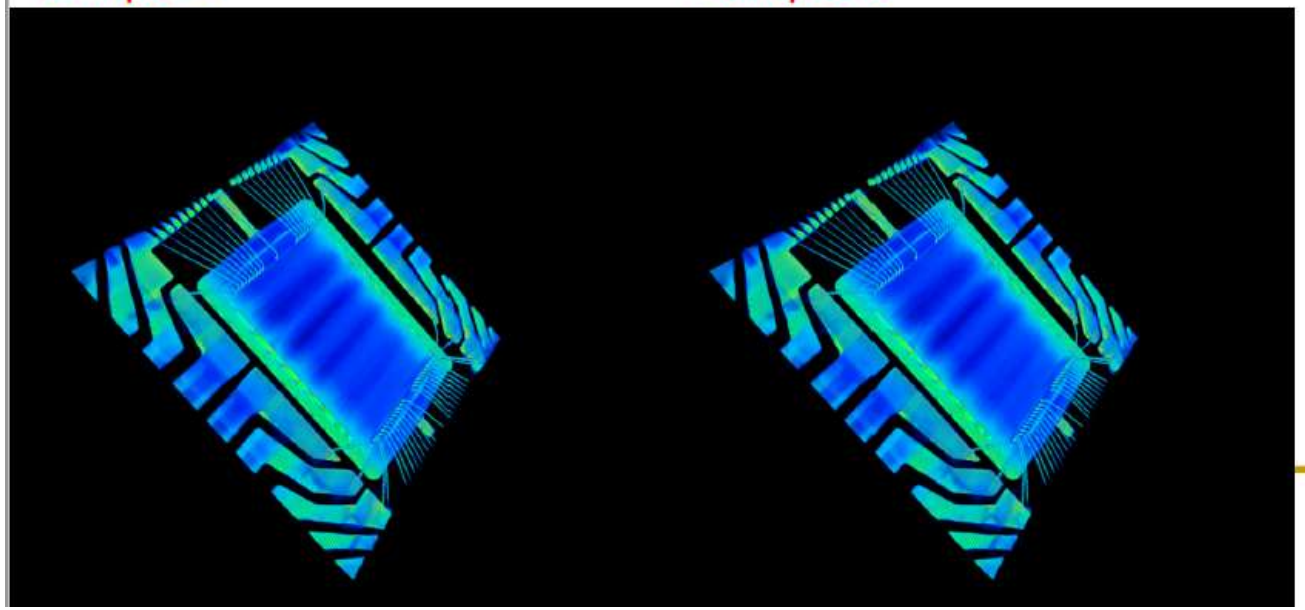


3D X-ray Tomography

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)

Thanks for your attention
Any questions so far?