Week 13: Lecture B

Hardware Testing

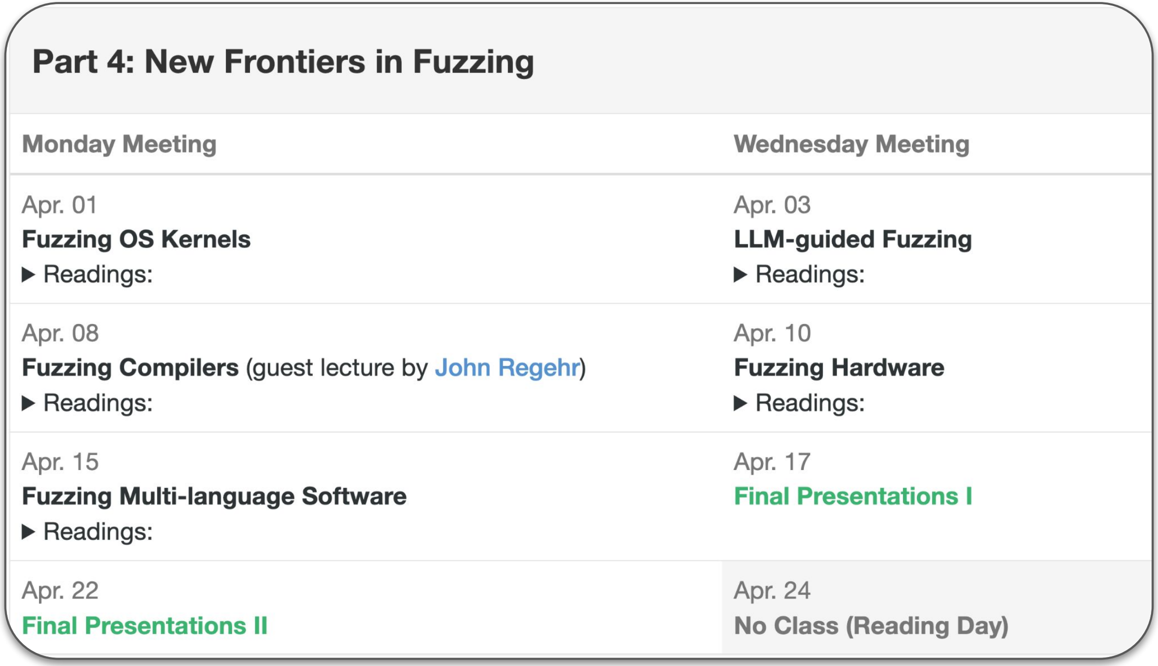
Wednesday, April 10, 2024

How are semester projects going?

Making progress?

Stuck?

The Next Few Weeks



Part 4: New Frontiers in Fuzzing

Monday Meeting	Wednesday Meeting
Apr. 01 **Fuzzing OS Kernels** ▶ Readings:	Apr. 03 **LLM-guided Fuzzing** ▶ Readings:
Apr. 08 **Fuzzing Compilers** (guest lecture by John Regehr) ▶ Readings:	Apr. 10 **Fuzzing Hardware** ▶ Readings:
Apr. 15 **Fuzzing Multi-language Software** ▶ Readings:	Apr. 17 **Final Presentations I**
Apr. 22 **Final Presentations II**	Apr. 24 **No Class (Reading Day)**

Recap: Project Schedule

- **Apr. 17th & 22nd:** final presentations
  - ~~15-20~~ **5-minute** slide deck and discussion
  - What you did, and why, and what results

- We have 26 teams…
  - So, 13 teams per two days
  - **5 minute presentation each**
  - One-minute audience Q&A
  - Keep the details tight!

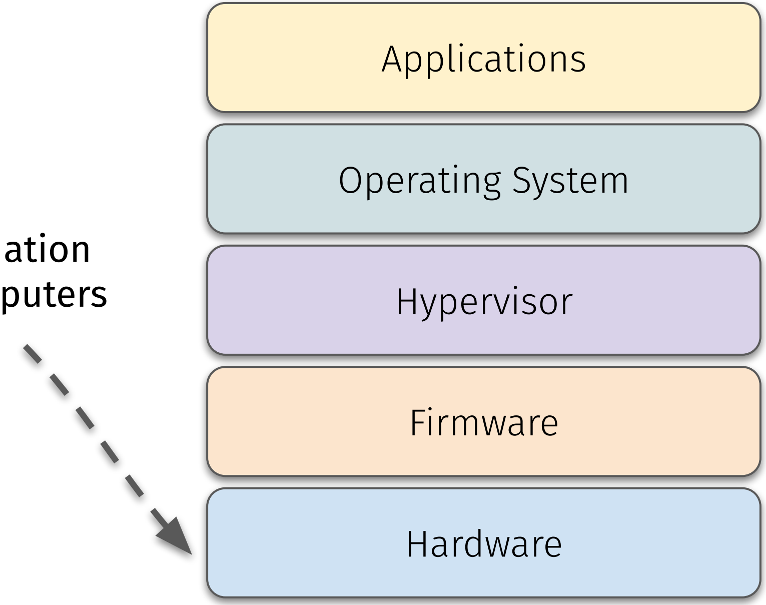
- What's most important:
  - High-level technique
  - Challenges and workarounds
  - Key results (bugs found, other successes, etc.)

Questions?

Hardware Security and Testing

Hardware

The foundation of our computers



Applications

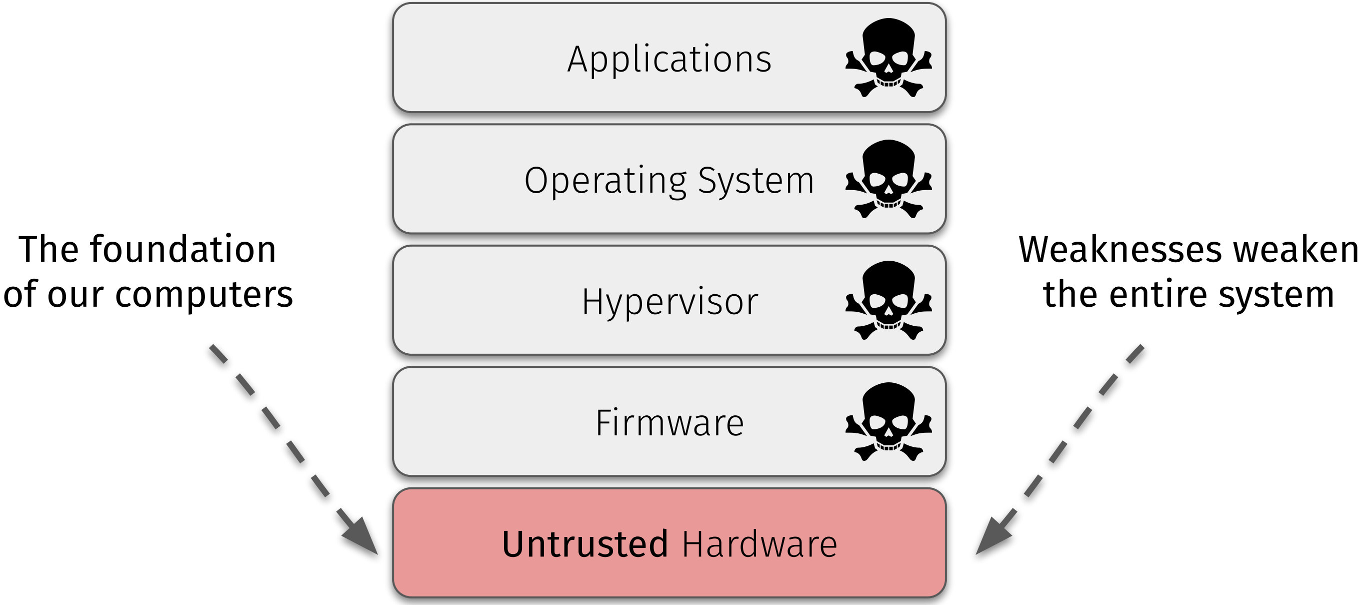
Operating System

Hypervisor

Firmware

Hardware

Hardware



The foundation of our computers

Applications

Operating System

Hypervisor

Firmware

Untrusted Hardware

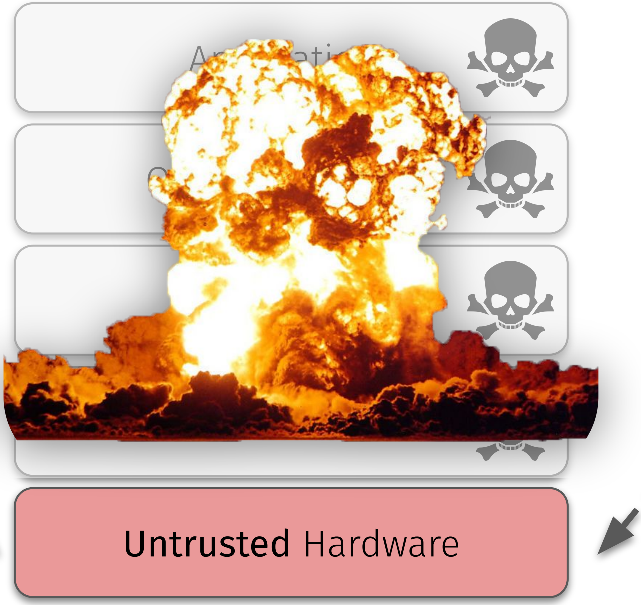
Weaknesses weaken the entire system

Hardware

FORESHADOW

The foundation of our computers

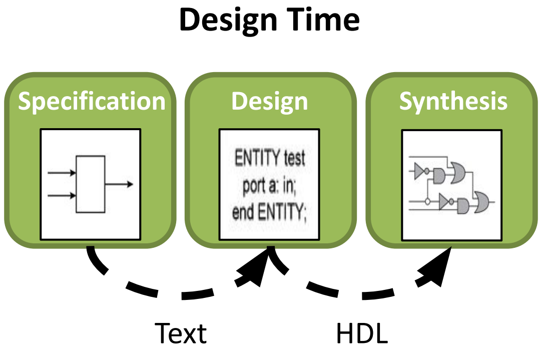
MELTDOWN



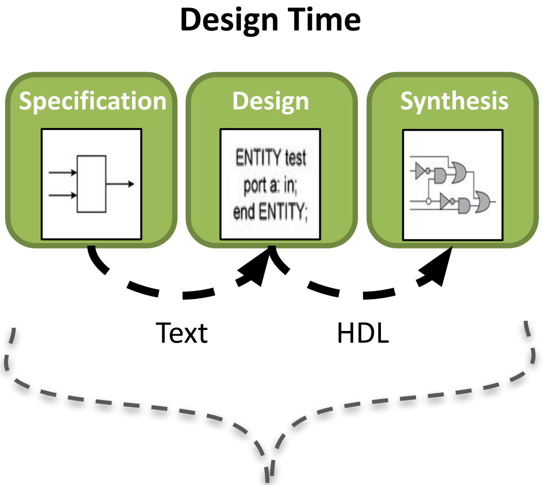
Weaknesses weaken the entire system

SPECTRE

Creating Hardware

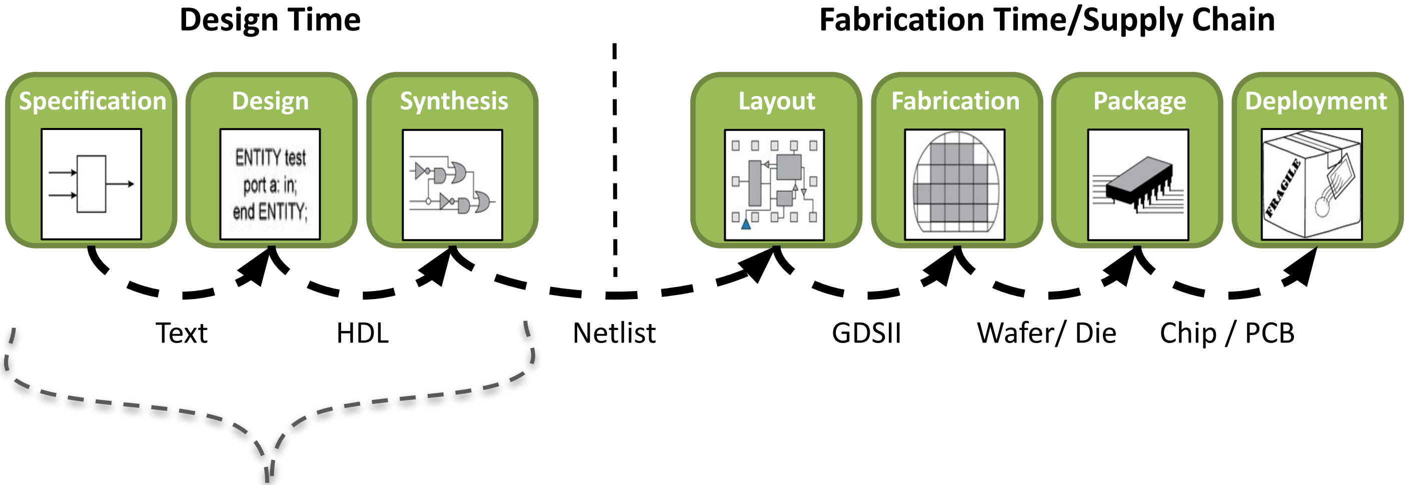


Creating Hardware



Similar to software design

Creating Hardware



Design Time

Fabrication Time/Supply Chain

Specification

Design

Synthesis

Layout

Fabrication

Package

Deployment

Text

HDL

Netlist

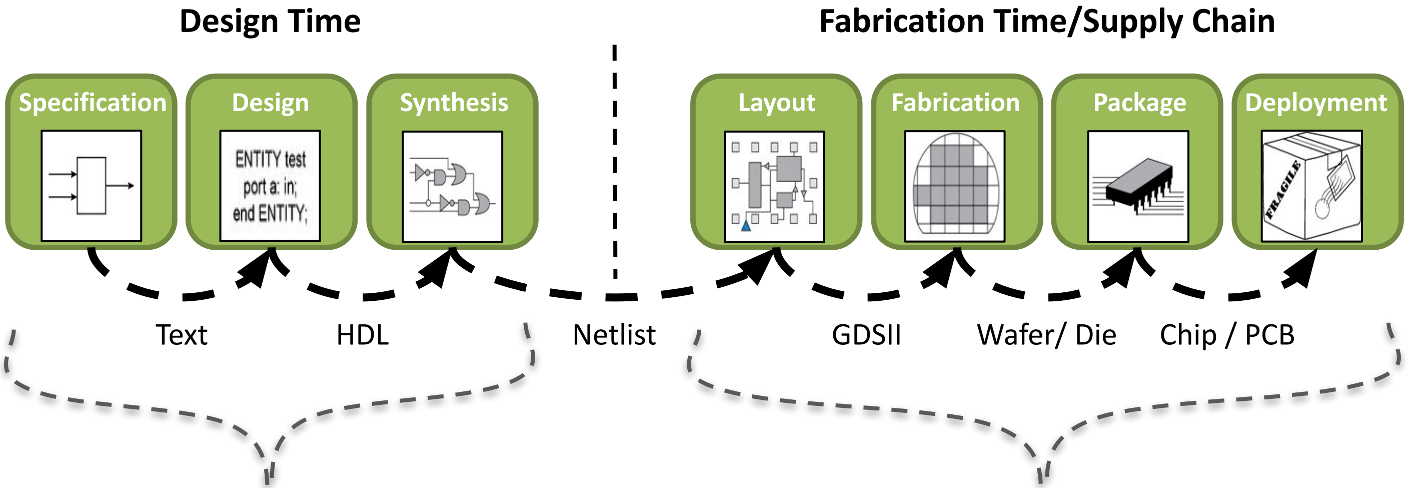
GDSII

Wafer/ Die

Chip / PCB

Similar to software design

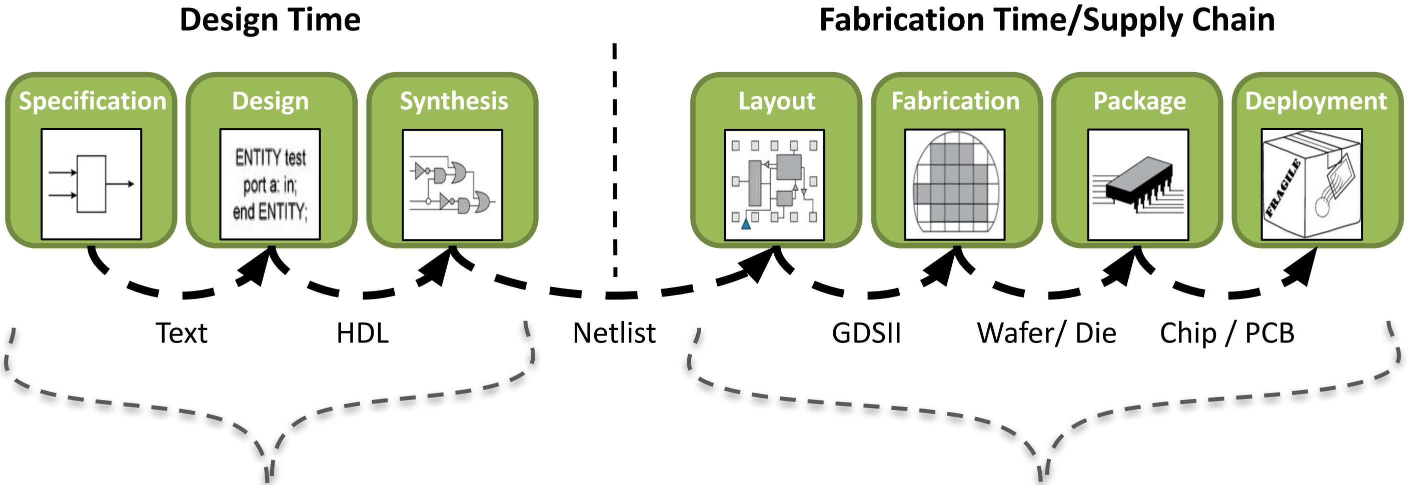
Creating Hardware



Similar to software design

Required to build a physical device

Creating Hardware



Similar to software design

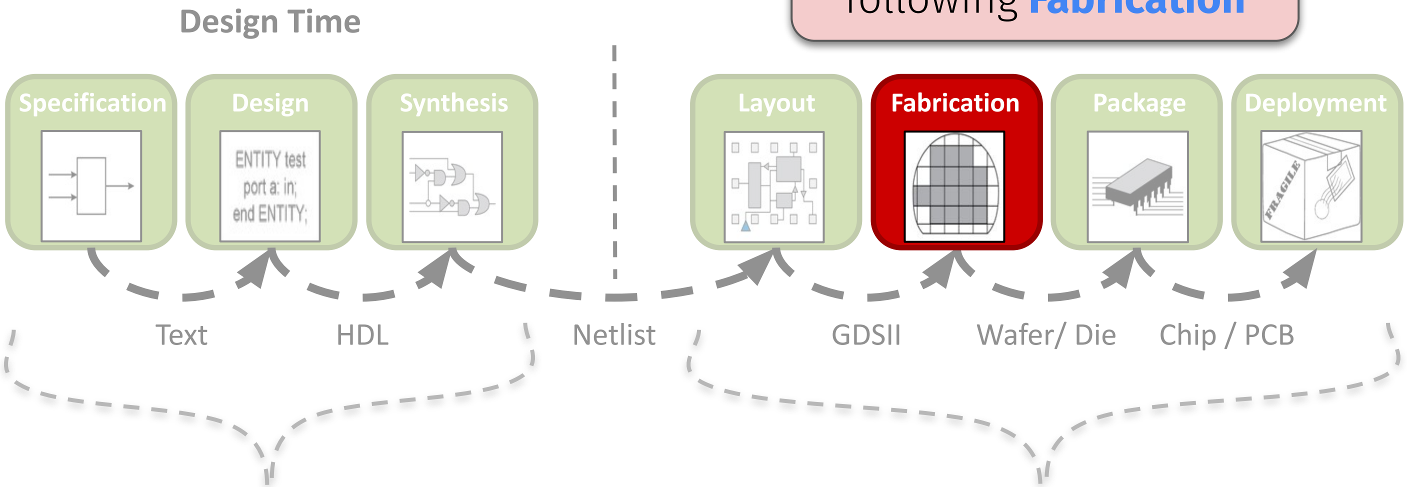
Verification

Required to build a physical device

Testing

Hardware Bugs

Cannot be **patched** following **Fabrication**



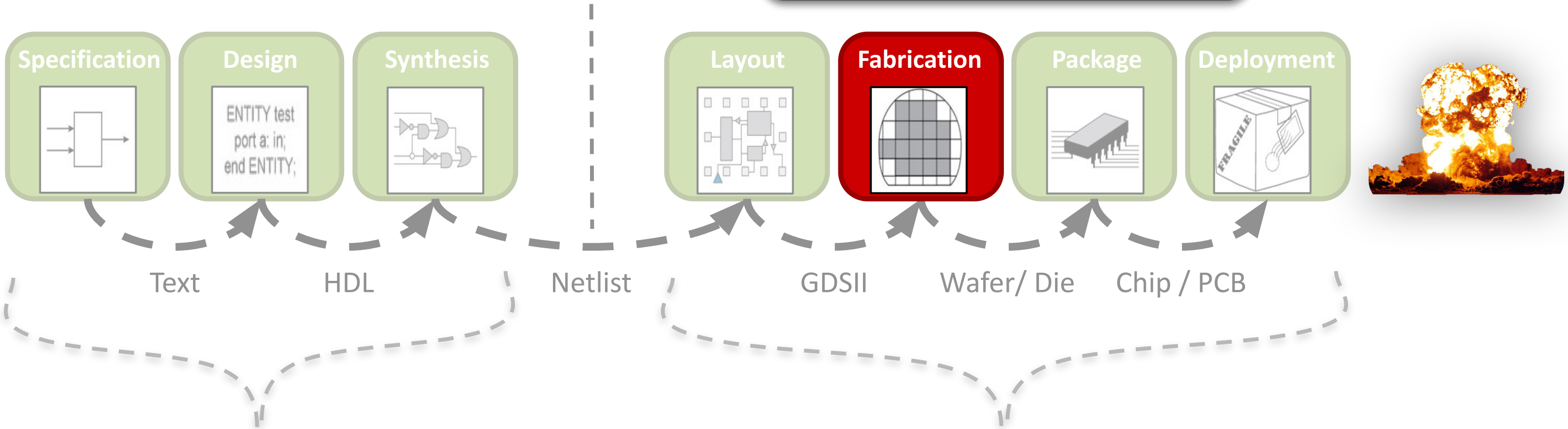
Similar to software design
Verification

Required to build a physical device
Testing

Hardware Bugs

Cannot be **patched**
following **Fabrication**

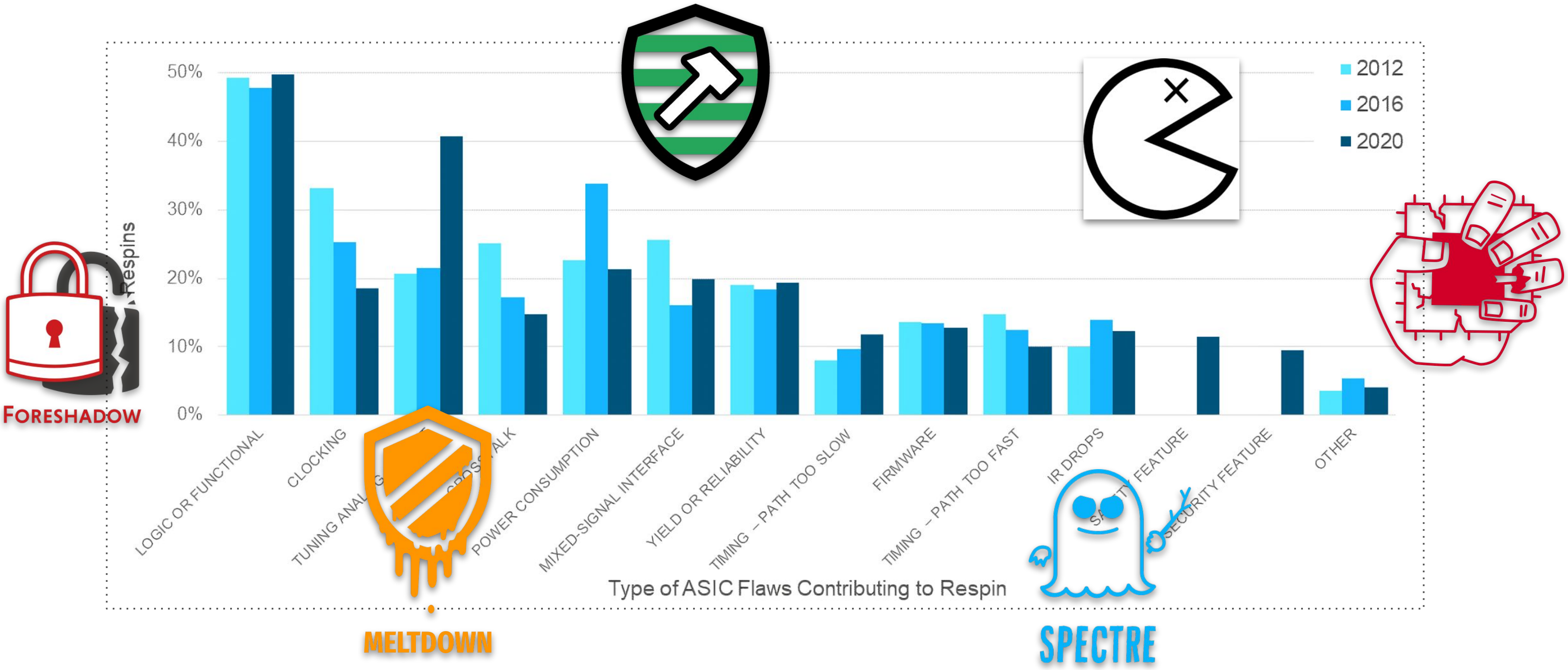
Design Time



Similar to software design
Verification

Required to build a physical device
Testing

Hardware Bugs

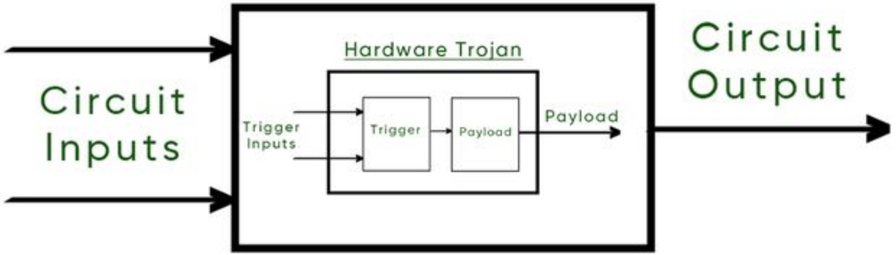


Hardware Trojans

- **Trojan Horse:**
  - **???**

Hardware Trojans

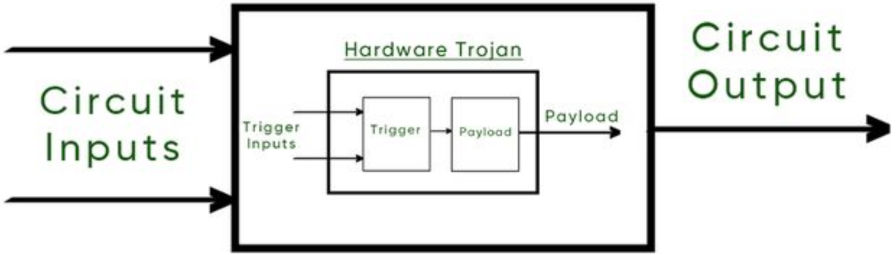
- **Trojan Horse:**
  - Attack pre-inserted into chip
  - Will be **exploited** at **run time**
  - **Remotely triggered** by attacker



Hardware Trojans

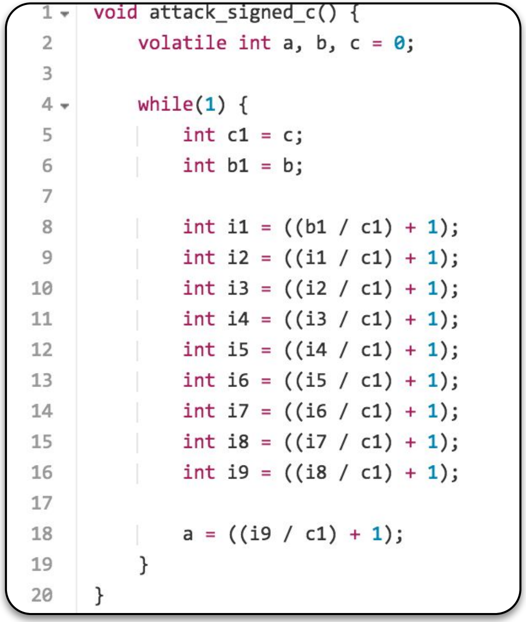
- **Trojan Horse:**
  - Attack pre-inserted into chip
  - Will be **exploited** at **run time**
  - **Remotely triggered** by attacker

- **Ideal characteristics:**
  - Small
  - Stealthy
  - Controllable



Hardware Trojans

- **Trojan Horse:**
  - Attack pre-inserted into chip
  - Will be **exploited** at **run time**
  - **Remotely triggered** by attacker
- **Ideal characteristics:**
  - Small
  - Stealthy
  - Controllable
- **Engineering a trigger**



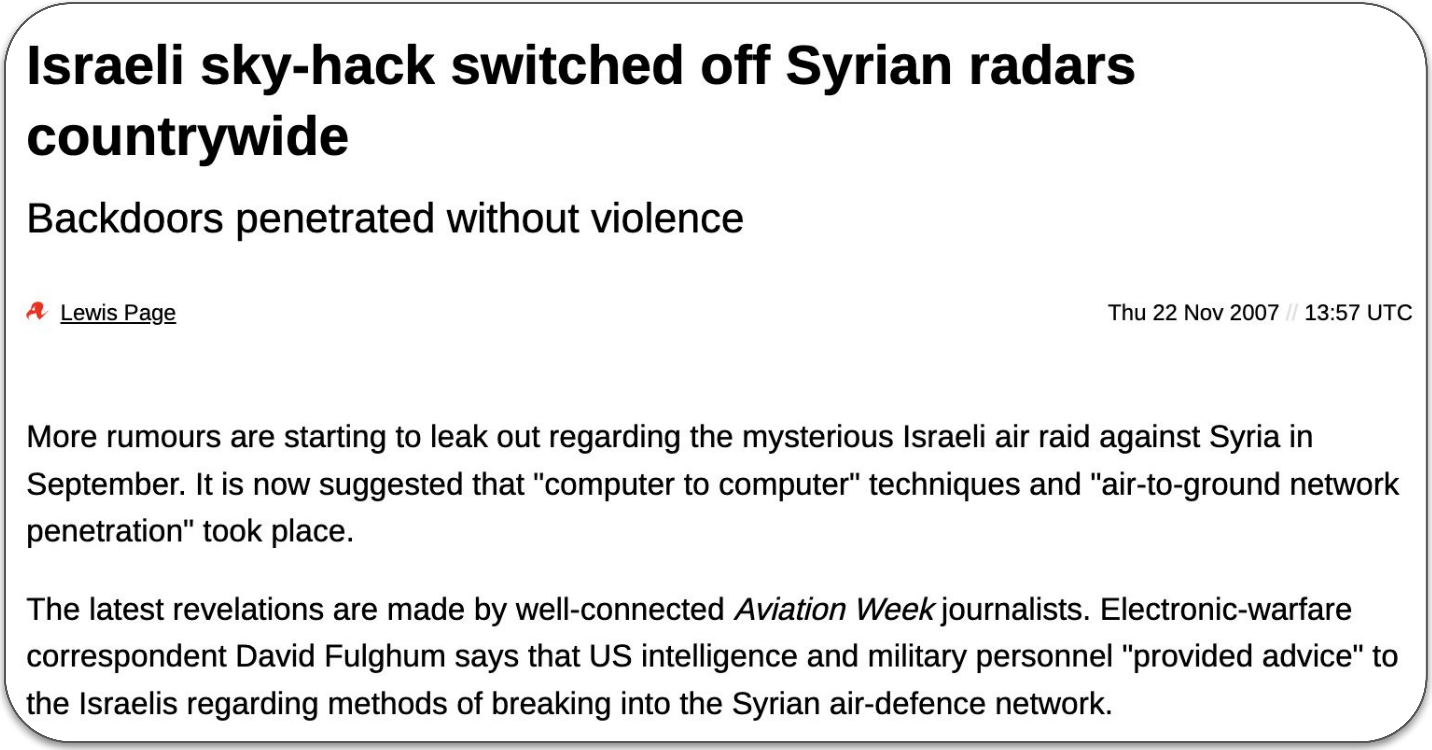
```
void attack_signed_c() {
    volatile int a, b, c = 0;

    while(1) {
        int c1 = c;
        int b1 = b;

        int i1 = ((b1 / c1) + 1);
        int i2 = ((i1 / c1) + 1);
        int i3 = ((i2 / c1) + 1);
        int i4 = ((i3 / c1) + 1);
        int i5 = ((i4 / c1) + 1);
        int i6 = ((i5 / c1) + 1);
        int i7 = ((i6 / c1) + 1);
        int i8 = ((i7 / c1) + 1);
        int i9 = ((i8 / c1) + 1);

        a = ((i9 / c1) + 1);
    }
}
```

Division sets div-by-zero flag

Addition resets div-by-zero flag

Software state will affect **analog state**!

Hardware Trojans



Israeli sky-hack switched off Syrian radars countrywide

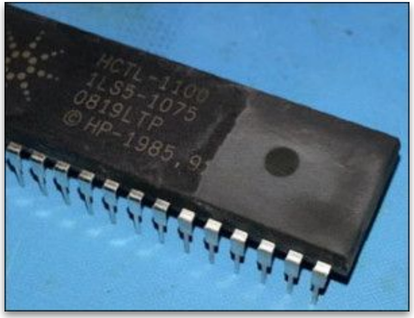
Backdoors penetrated without violence

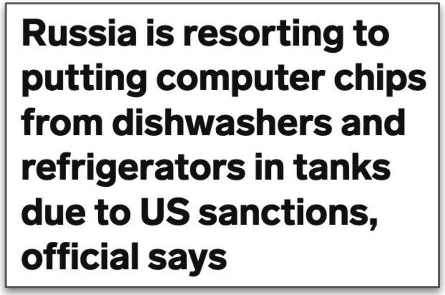
Lewis Page Thu 22 Nov 2007 // 13:57 UTC

More rumours are starting to leak out regarding the mysterious Israeli air raid against Syria in September. It is now suggested that "computer to computer" techniques and "air-to-ground network penetration" took place.

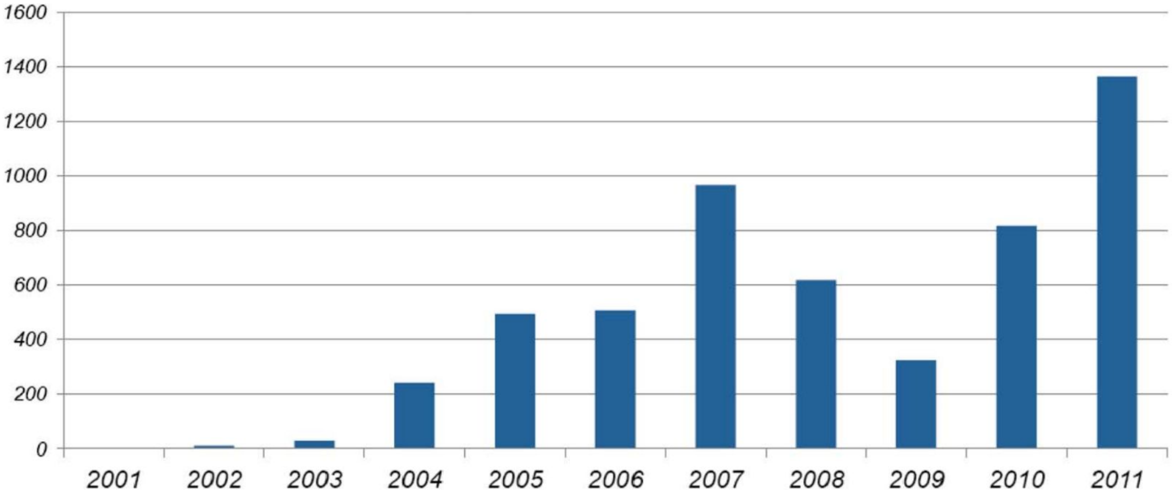
The latest revelations are made by well-connected *Aviation Week* journalists. Electronic-warfare correspondent David Fulghum says that US intelligence and military personnel "provided advice" to the Israelis regarding methods of breaking into the Syrian air-defence network.

Recycled and Counterfeit Hardware



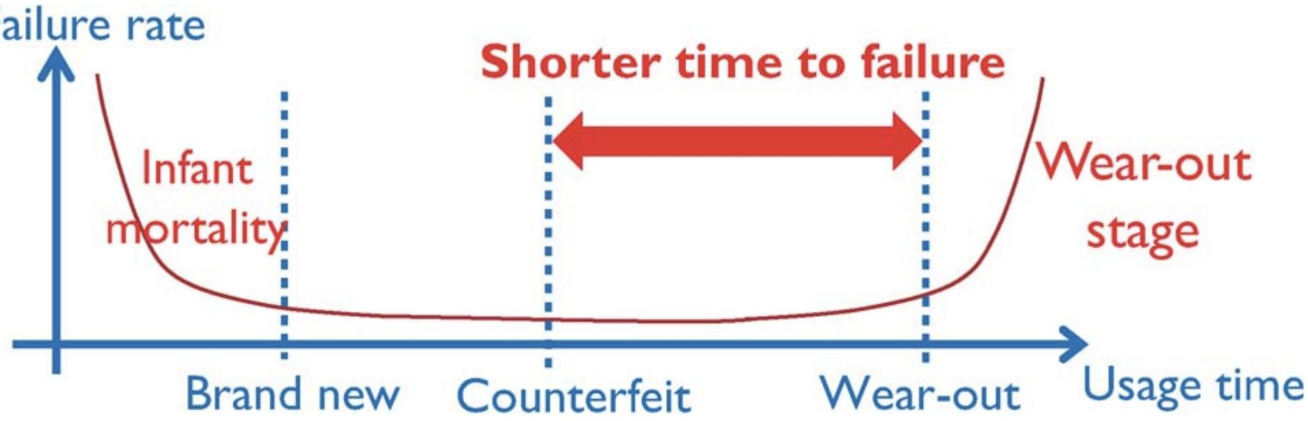

Russia is resorting to putting computer chips from dishwashers and refrigerators in tanks due to US sanctions, official says

Guin *et al*.: Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain



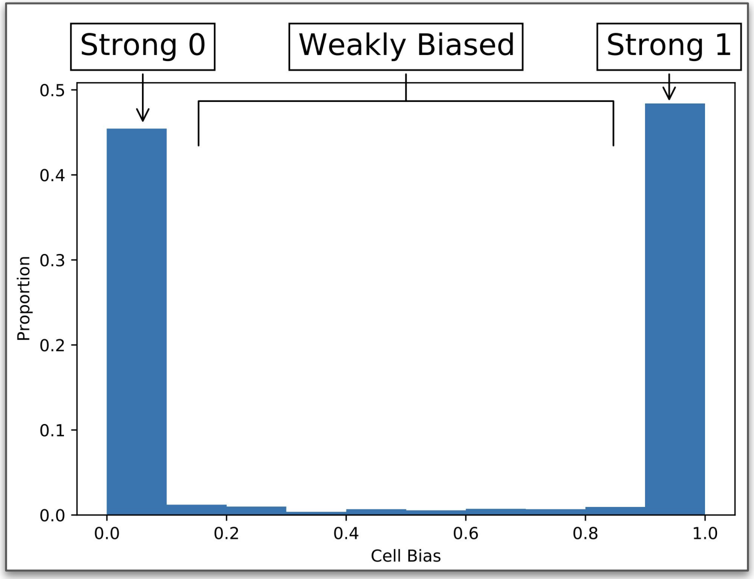
Recycled and Counterfeit Hardware

- **Counterfeit** and **recycled chips** have a **shorter lifespan**
  - Absolutely dangerous for security-critical use cases



Recycled and Counterfeit Hardware

- **Counterfeit** and **recycled chips** have a **shorter lifespan**
  - Absolutely dangerous for security-critical use cases

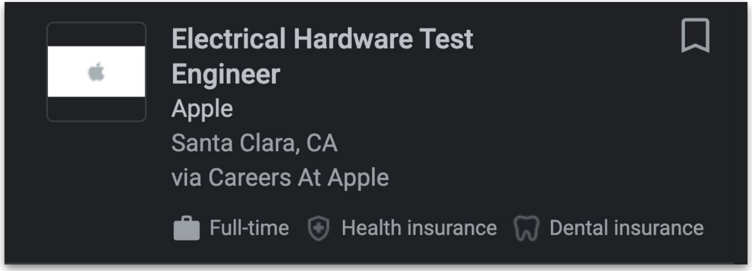


Secure Hardware

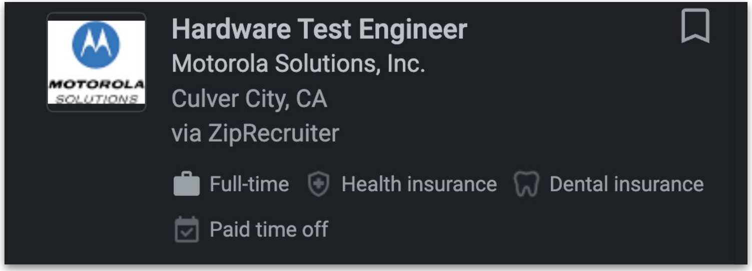
- **Can we ever know for sure that a chip is secure?**

Hardware Testing

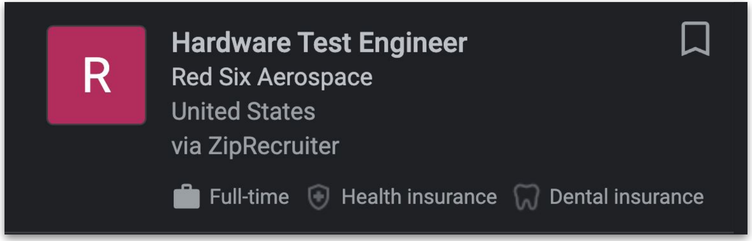
- One of the highest-paid (and steep-learning-curve) careers in testing
  - **Spoiler:** it’s even harder than testing software


Electrical Hardware Test Engineer
Apple
Santa Clara, CA
via Careers At Apple

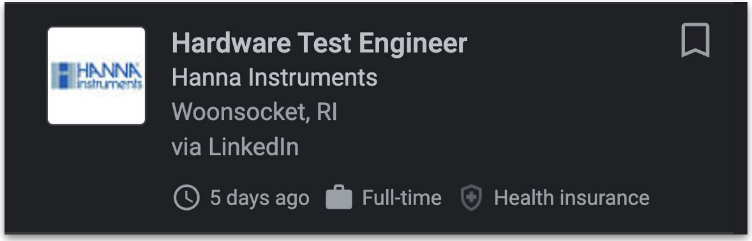
Full-time · Health insurance · Dental insurance


Hardware Test Engineer
Motorola Solutions, Inc.
Culver City, CA
via ZipRecruiter

Full-time · Health insurance · Dental insurance · Paid time off


Hardware Test Engineer
Red Six Aerospace
United States
via ZipRecruiter

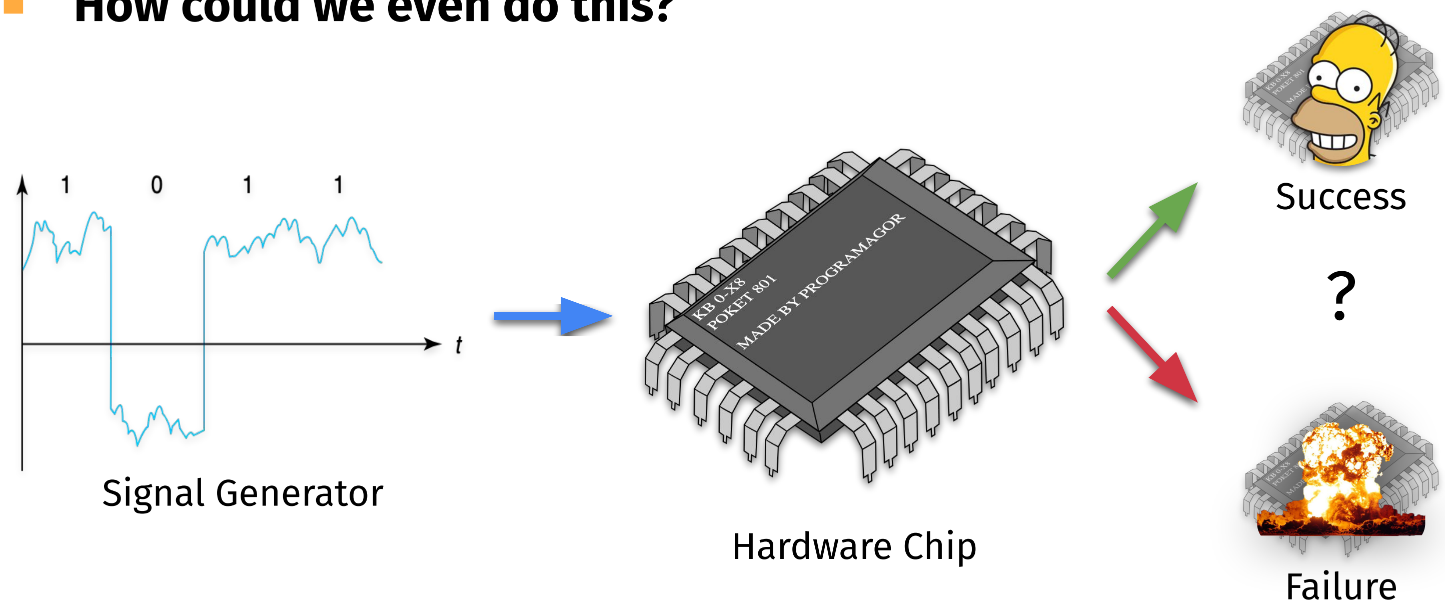
Full-time · Health insurance · Dental insurance


Hardware Test Engineer
Hanna Instruments
Woonsocket, RI
via LinkedIn

5 days ago · Full-time · Health insurance

Testing Hardware Physically

- **How could we even do this?**



Signal Generator

Hardware Chip

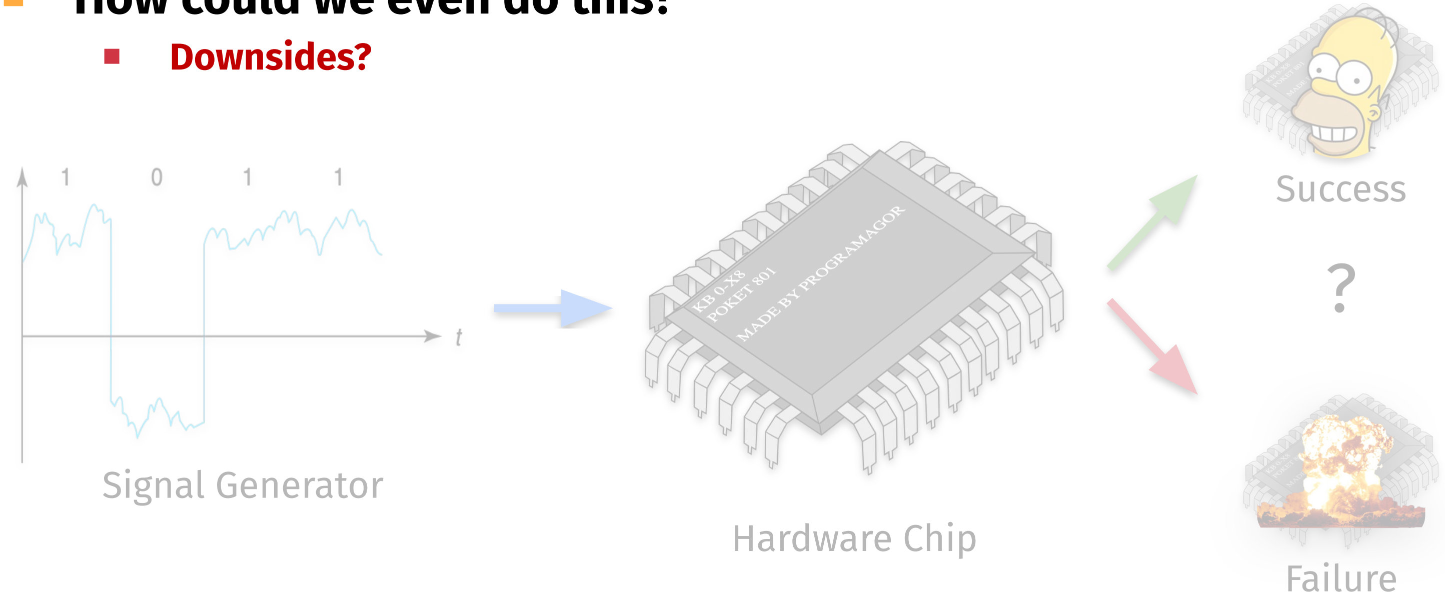
Success

?

Failure

Testing Hardware **Physically**

- **How could we even do this?**
  - **Downsides?**



Signal Generator

Hardware Chip

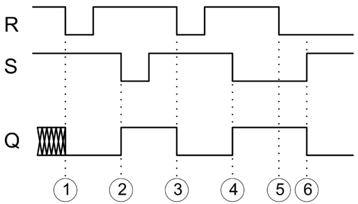
Success

?

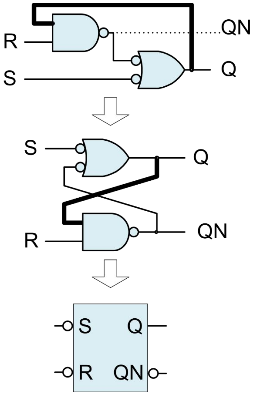
Failure

Testing Hardware Pre-Silicon

- **Idea:** apply testing to the HDL (Hardware Description Lang.)
  - E.g., Verilog
- Benefits over physical testing?



1. Q is undefined until R is asserted
2. Q → ‘1’ when S is asserted
3. Q → '0' when R is asserted
4. Q → '1' when S is asserted
5. Q stays at '1' when S & R asserted
6. Q → '0' when R asserted, S de-asserted



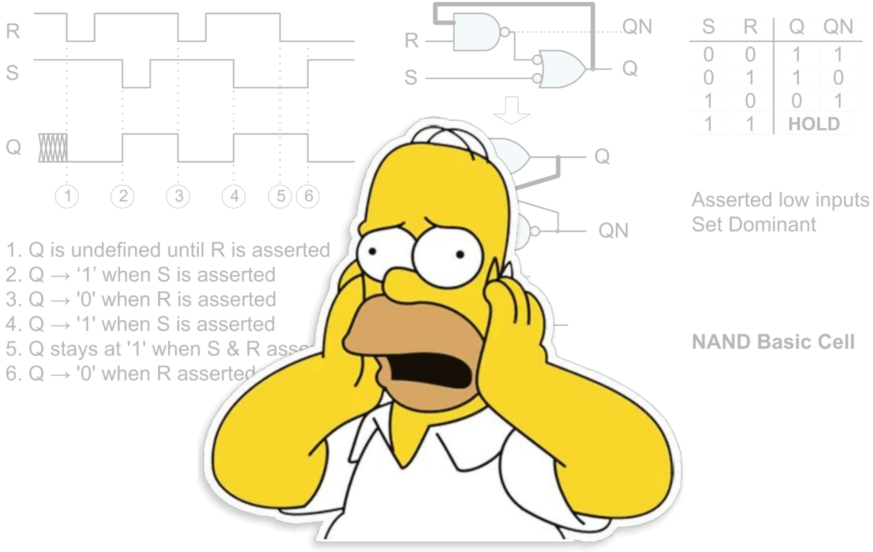
S	R	Q	QN
0	0	1	1
0	1	1	0
1	0	0	1
1	1	HOLD	

Asserted low inputs
Set Dominant

NAND Basic Cell

Testing Hardware Pre-Silicon

- **Idea:** apply testing to the HDL (Hardware Description Lang.)
  - E.g., Verilog
- Benefits over physical testing?
  - **Downsides?**

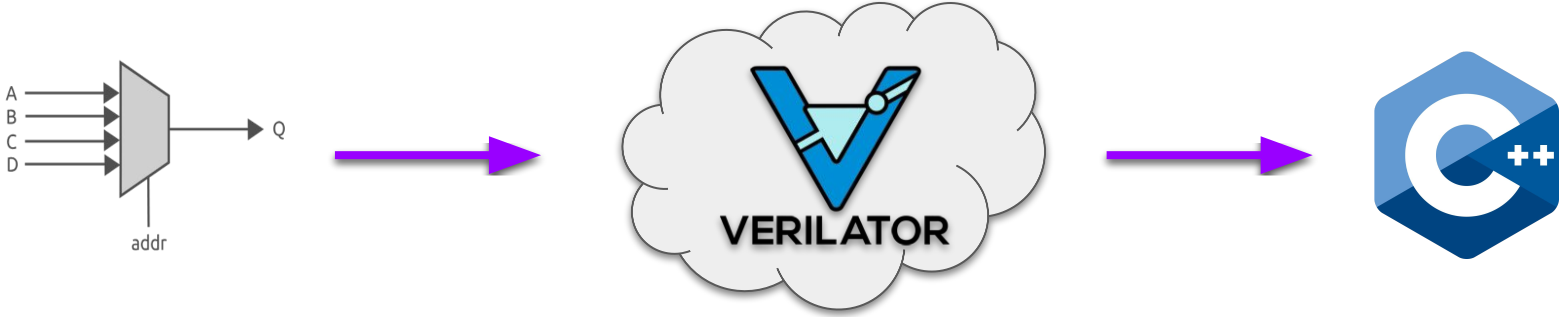


1. Q is undefined until R is asserted
2. Q → '1' when S is asserted
3. Q → '0' when R is asserted
4. Q → '1' when S is asserted
5. Q stays at '1' when S & R asse
6. Q → '0' when R asserted

S	R	Q	QN
0	0	1	1
0	1	1	0
1	0	0	1
1	1	HOLD	

Enter the Simulation

- **Idea:** “translate” HDL to a more workable representation (e.g., C++)



- Benefits?
    - **Downsides?**

Questions?