Hardware Security and Trust:
Where We Are and Where We Should Go

Giorgio DI NATALE

LIRMM

CNRS advancing the frontiers

TRUDEVICE

cost

EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY

What is COST?

1

- COST is the oldest and widest European intergovernmental framework for transnational Cooperation in Science and Technology

2

- For more than 45 years COST has **supported networking** of research activities across all its Member countries

3

- COST is open to all disciplines, to all novel and ground-breaking S&T ideas

COST Countries

- The 27 EU Member States
- EU Acceding & Candidate Countries
  - Croatia
  - Former Yugoslav Republic of Macedonia
  - Iceland
  - Turkey
- Other Countries
  - Bosnia and Herzegovina
  - Republic of Serbia
  - Norway
  - Switzerland
- COST Cooperating States
  - Israel

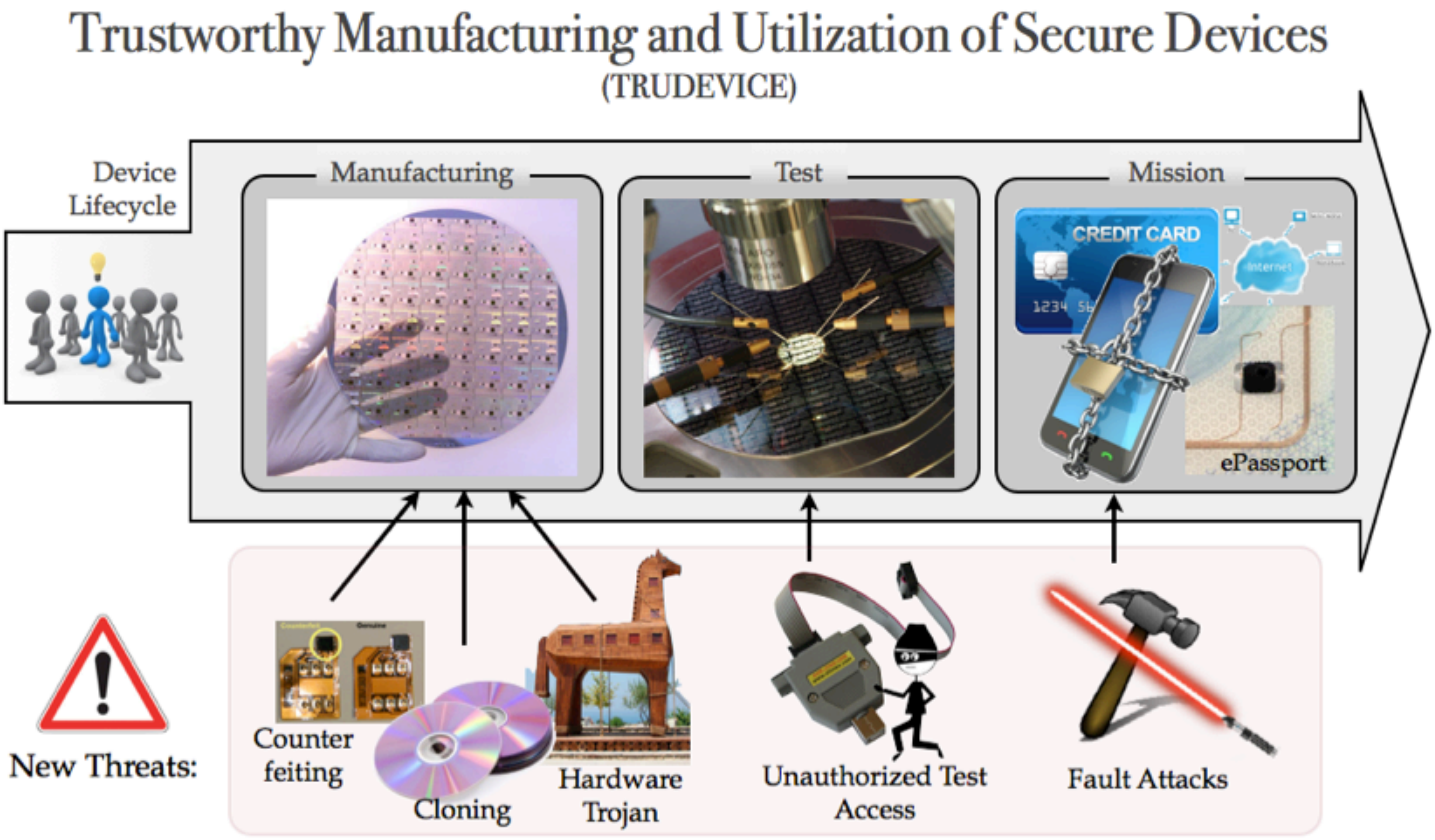
What can be done in a COST Action

- Meetings
- Short Term Scientific Missions
  - Allow a researcher (especially early-stage) to go to an institution in another COST country to foster cooperation
  - Duration: from 5 days up to 3 months
- Training Schools

TRUDEVICE

- **Scientific targets**: to develop new design and manufacturing flows for the production of secure integrated circuits
- **Networking**: to create a new community composed of academic, industrial and public organizations

TRUDEVICE


Trustworthy Manufacturing and Utilization of Secure Devices
(TRUDEVICE)
Device Lifecycle
Manufacturing
Test
Mission
CREDIT CARD
ePassport
New Threats:
Counter feiting
Cloning
Hardware Trojan
Unauthorized Test Access
Fault Attacks

Action's Research Areas

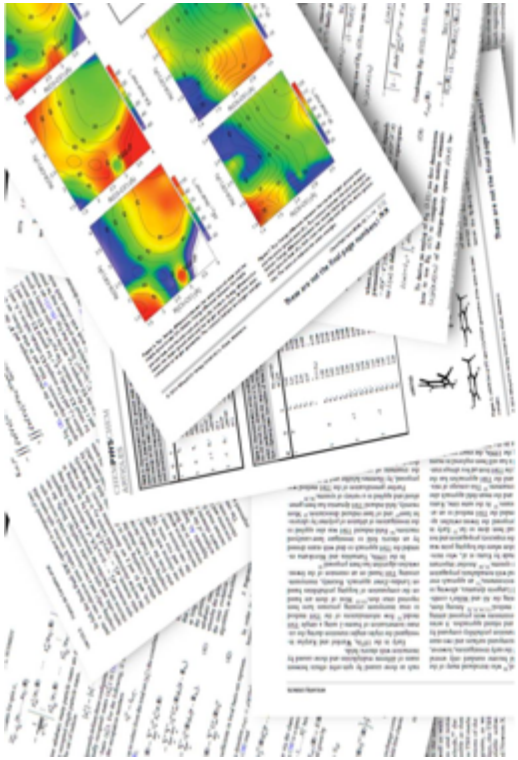
- Area 1: Manufacturing test of secure devices
- Area 2: Trustworthy manufacturing of secure devices
- Area 3: Fault attack detection and protection
- Area 4: Reconfigurable devices for secure functions
- Area 5: Validation, Evaluation, and Fault Injection

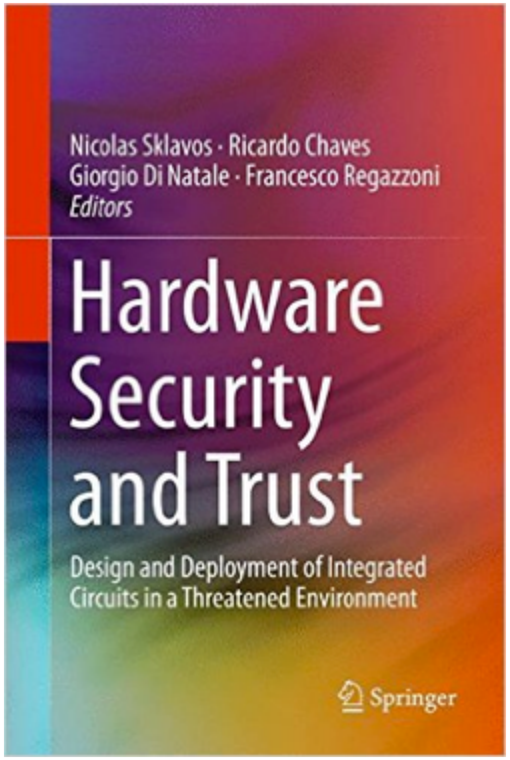
TRUDEVICE: from 12/12/2012

- 6 workshops
  - Avignon (FR), Freiburg (DE), Amsterdam (NL), Grenoble (FR), Saint Malo (FR), Dresden (DE)
- 1 final conference
  - Barcelona (ES)
- 2 training schools
  - Lisbon (PT) and Leukerbad (CH)
- 39 Short Terms Scientific Missions

Scientific Results

More than 400 papers





Thanks to many people

Where we are…

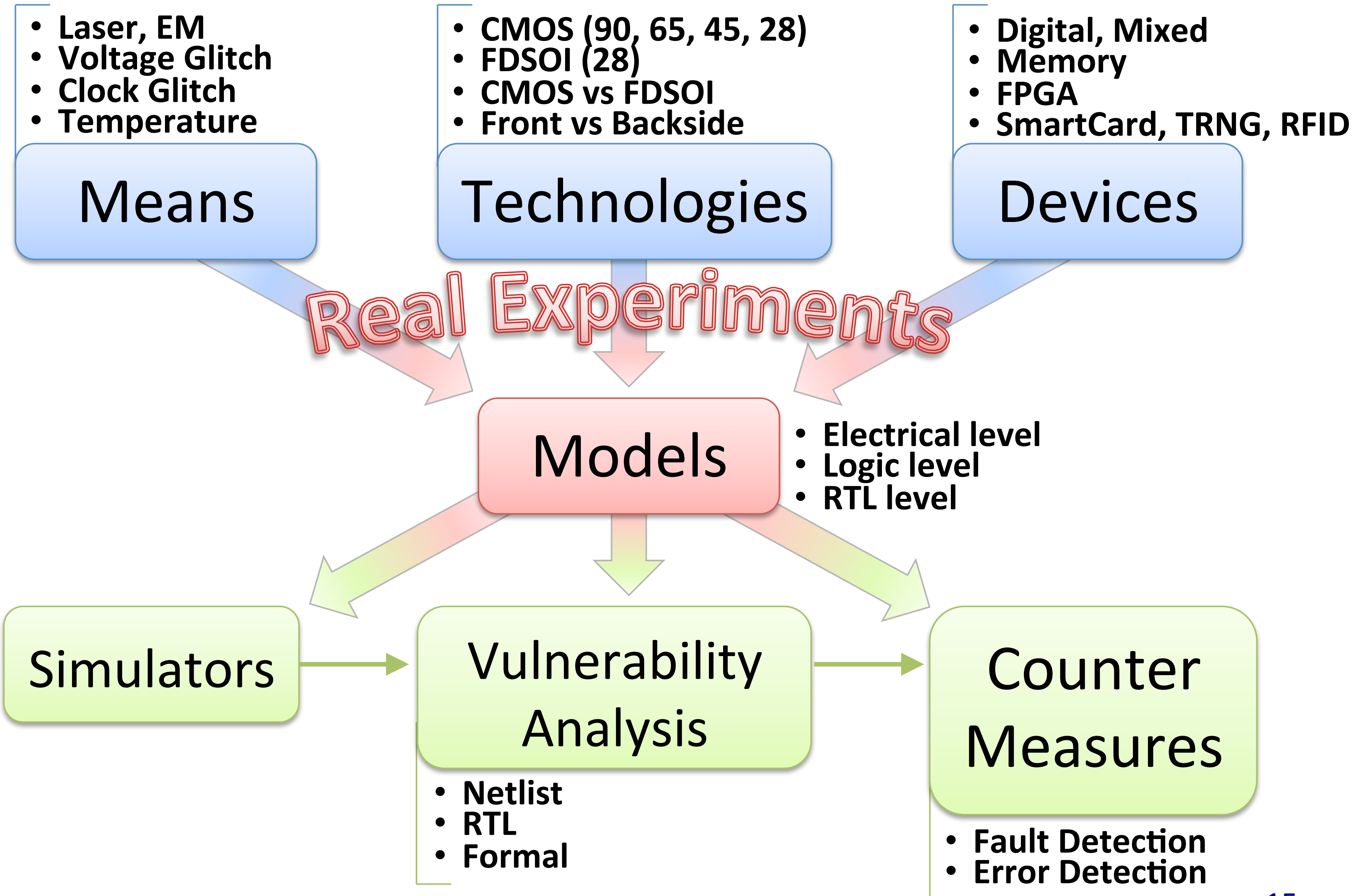
Action's Research Areas

- Area 1: Manufacturing test of secure devices
- Area 2: Trustworthy manufacturing of secure devices
- **Area 3: Fault attack detection and protection**
- Area 4: Reconfigurable devices for secure functions
- **Area 5: Validation, Evaluation, and Fault Injection**

Fault Attacks

- Forcing an error in a circuit implementing a cryptographic function in order to discover a secret
- Historically, many papers tried to adapt the classical “fault tolerance” (for reliability/radiation)
- However, malicious faults are different!

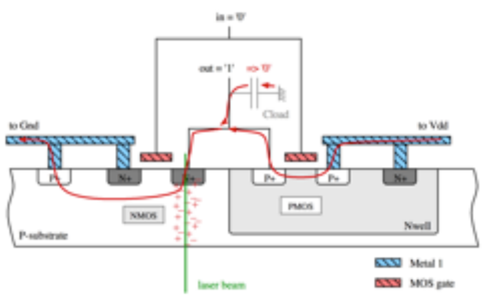
Fault Attacks

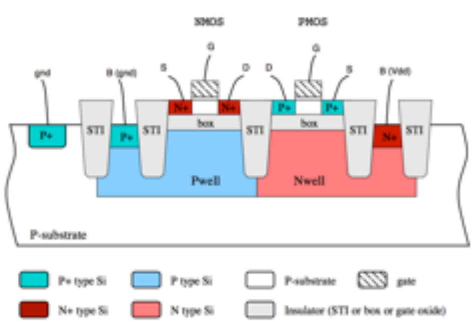


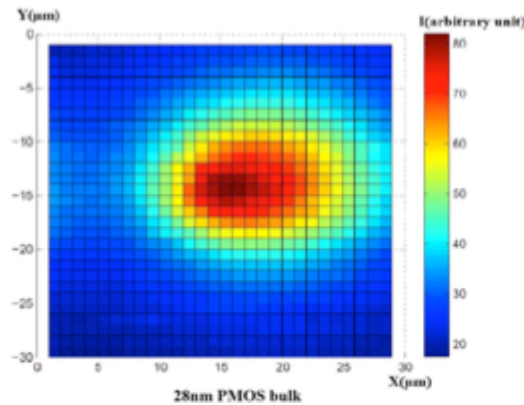
Injections:
CMOS vs FDSOI

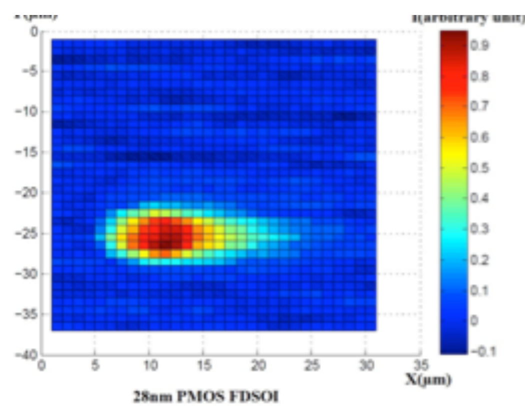
Figure of merits of 28nm Si technologies for implementing laser attack resistant security dedicated circuits

2015 IEEE Computer Society Annual Symposium on VLSI



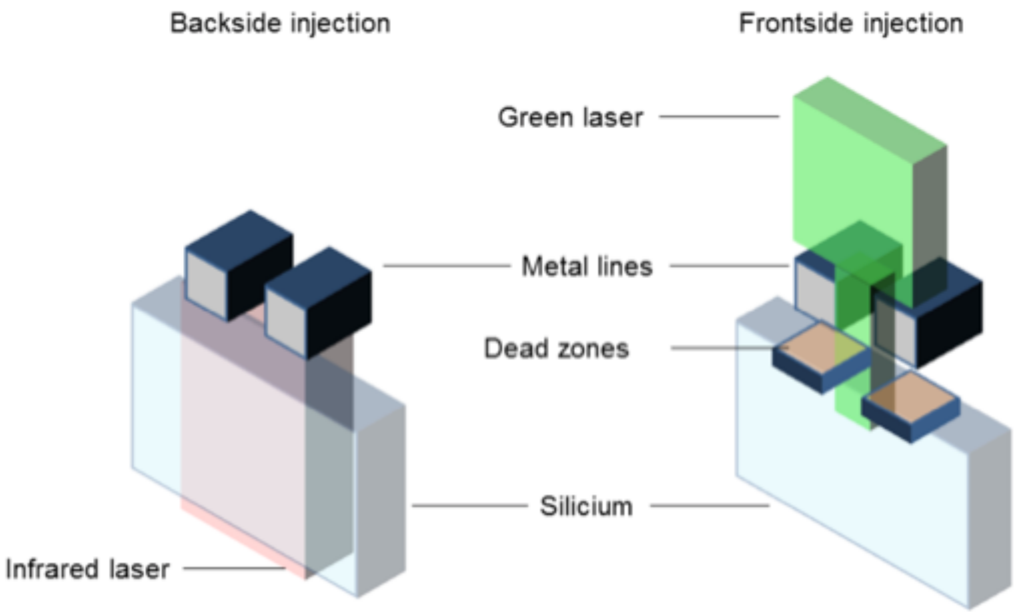


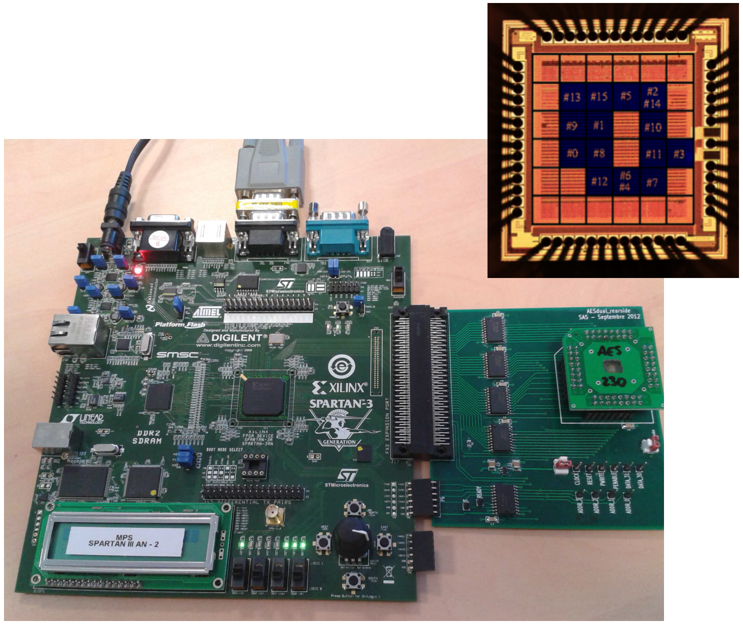




Injections:
Frontside vs Backside

Front-side vs backside laser injection: a comparative study
ACM Transactions on Embedded Computing Systems, Vol. 9, No. 4





Injections:
RFID

A Combined Design-Time/Test-Time Study of the Vulnerability of Sub-Threshold Devices to Low Voltage Fault Attacks
IEEE Trans. on Emerging Topics in Computing, Vol. 2, Issue 2, 2014

- Low-cost fault injection attack for RFID
- Based on voltage glitch to cause setup time violations
- Real chip (65-nm, working in subthreshold voltage range)
- Results:
  - It is possible to inject exploitable faults
  - It is possible to identify the most critical parts of the circuit

Injections:
TRNG with EM

Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator
COSADE 2012

- RO-based TRNG (with 50 Ros)
- EM injection allows
  - to influence the frequency
  - to control the monobit bias of the TRNG output
  - even when low power electromagnetic fields are exploited.

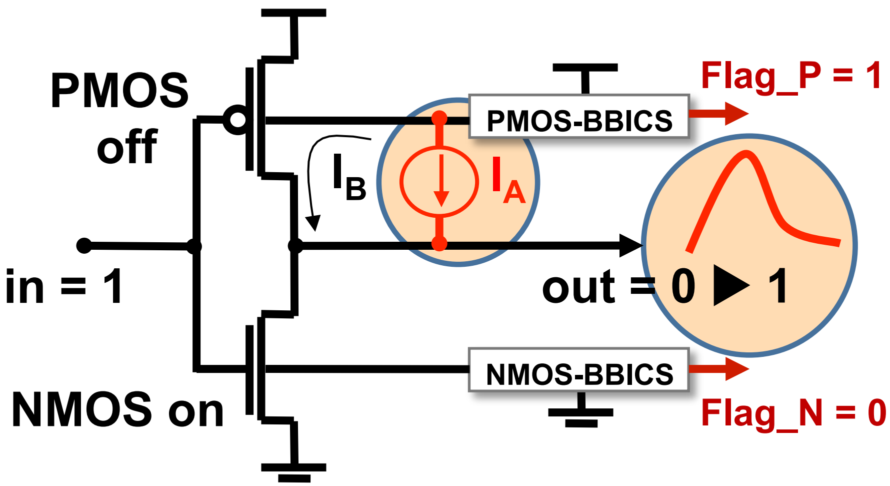
Modeling Laser Attacks:
RTL Level

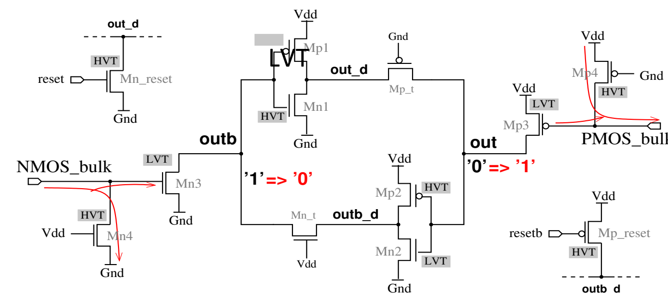
`A Multiple Fault Injection Methodology based on Cone Partitioning towards RTL Modeling of Laser Attacks`
`DATE 2014`

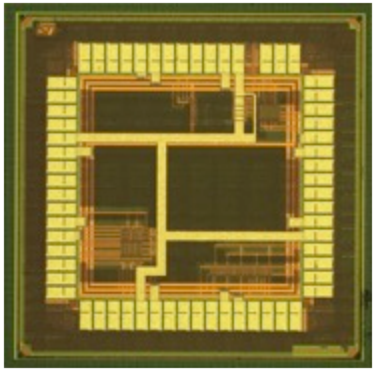
- A methodology to reduce the fault space of laser injection campaigns
- Based on:
  - locality characteristic of laser fault
  - partitioning of the RTL description of the circuit
- Results are more representative of laser attacks than random bit injection

Fault Detection:
Bulk Built-In Current Sensor

Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents
IOLTS 2015

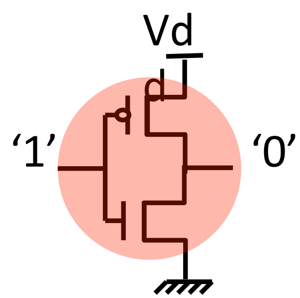


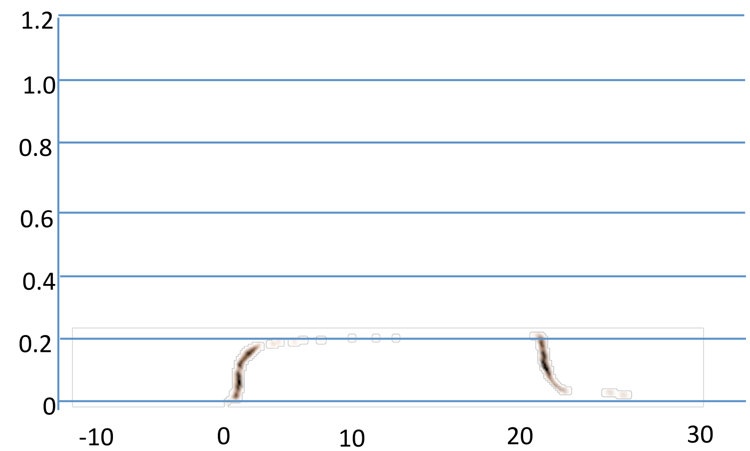




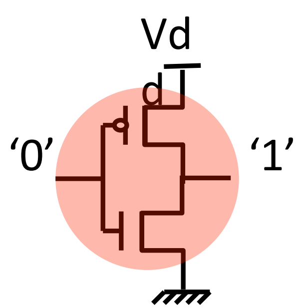
CNRS LIRMM

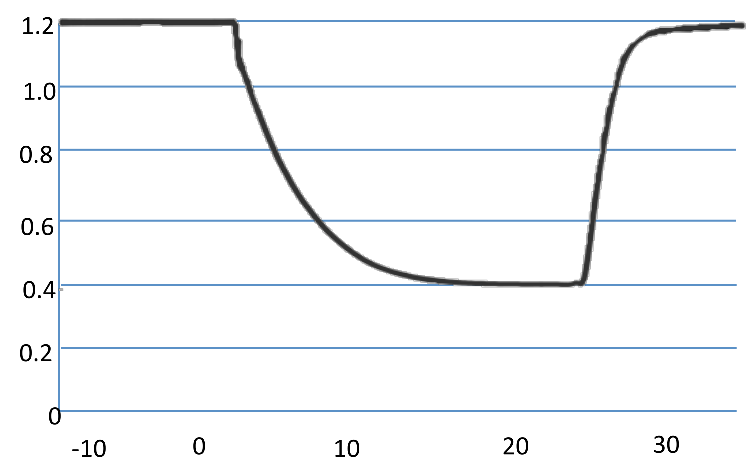
Fault Detection:
Laser Detector



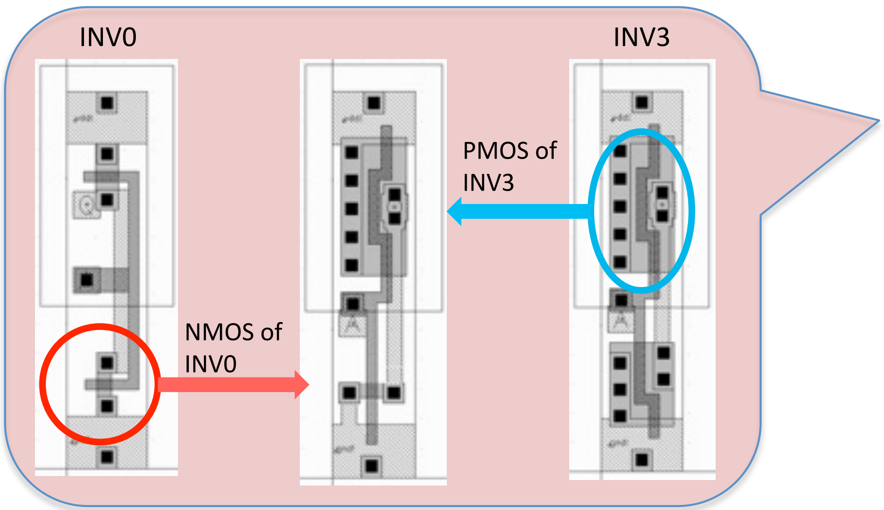


Laser spot = 3.25μm
Laser power = 1.0w
Technology = 90nm ST

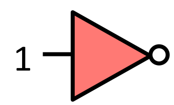


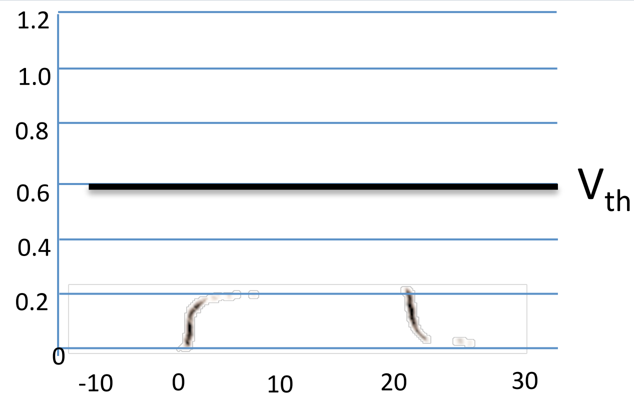


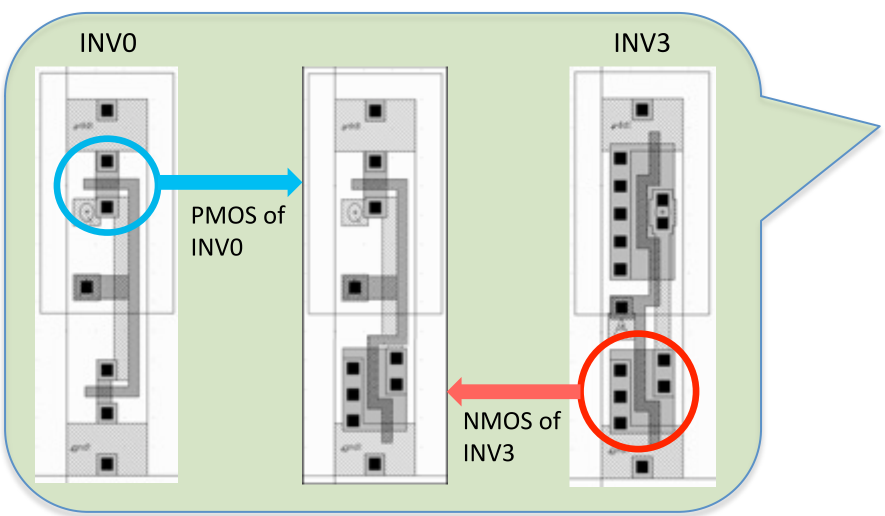
Fault Detection:
Laser Detector



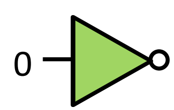
S_INVP3

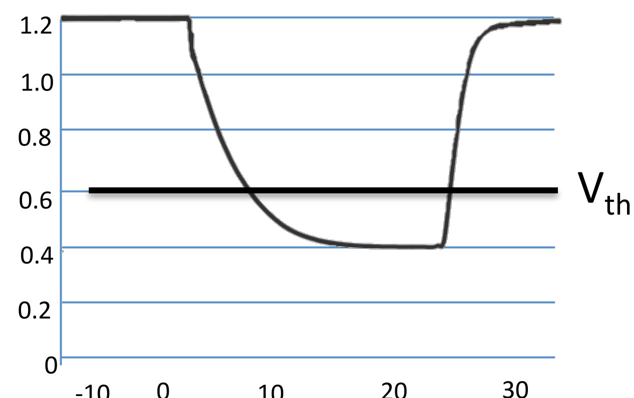






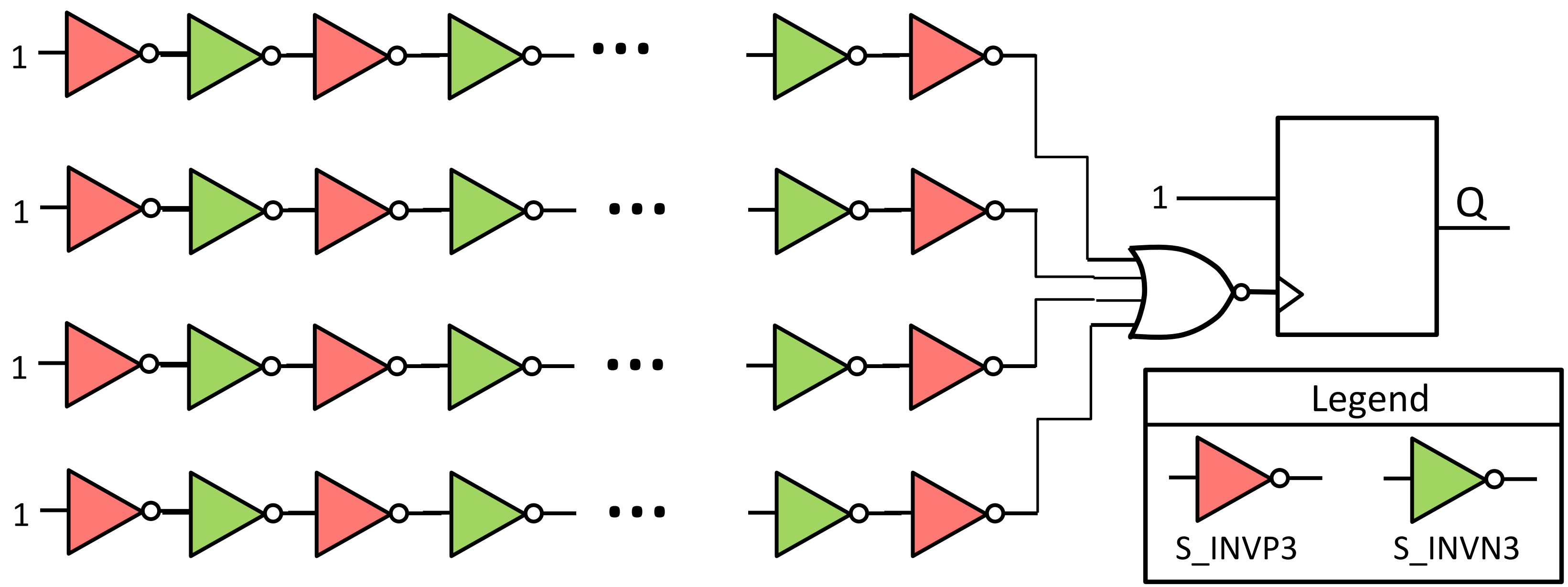
S_INVN3





Fault Detection:
Laser Detector

Customized Cell Detector for Laser-Induced-Fault Detection,
IOLTS 2014



Error Detection:
Use of codes

Relations Between the Entropy of a Source and the Error Masking Probability for Security-Oriented Codes
IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 63, NO. 1, JANUARY 2015

- Error detection/correction codes are usually designed for uniformly distributed codewords, i.e., for codes that have maximal entropy.
- In practice, the code-words are not uniformly distributed
- → their entropy is smaller and their efficiency in detecting attacks degrades

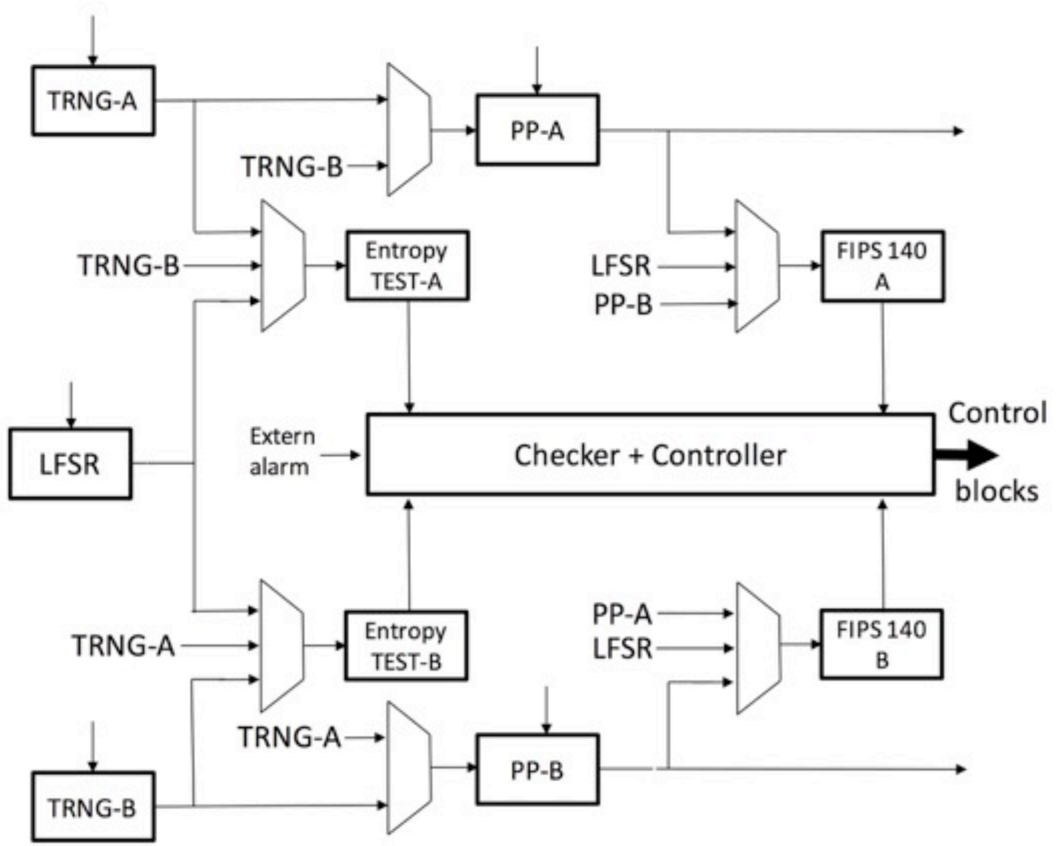
Error Detection:
Use of codes

Protecting Cryptographic Hardware against Malicious Attacks by Nonlinear Robust Codes
2014 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems

- Fault-based attacks against cryptographic circuits must be addressed by techniques that are different from approaches designed for random transient faults
- Systematic investigation of robust error-detecting codes that specifically target malicious attacks and guarantee minimal bounds on detection probability

Error Detection:
For a TRNG

Towards a Dependable True Random Number Generator With Self-Repair Capabilities
IEEE Transactions on Circuits and Systems I: Regular Papers



Where we should go…

Computing evolution

Big challenges ('60s)

- Science
- Business
- Military

People ('80s)

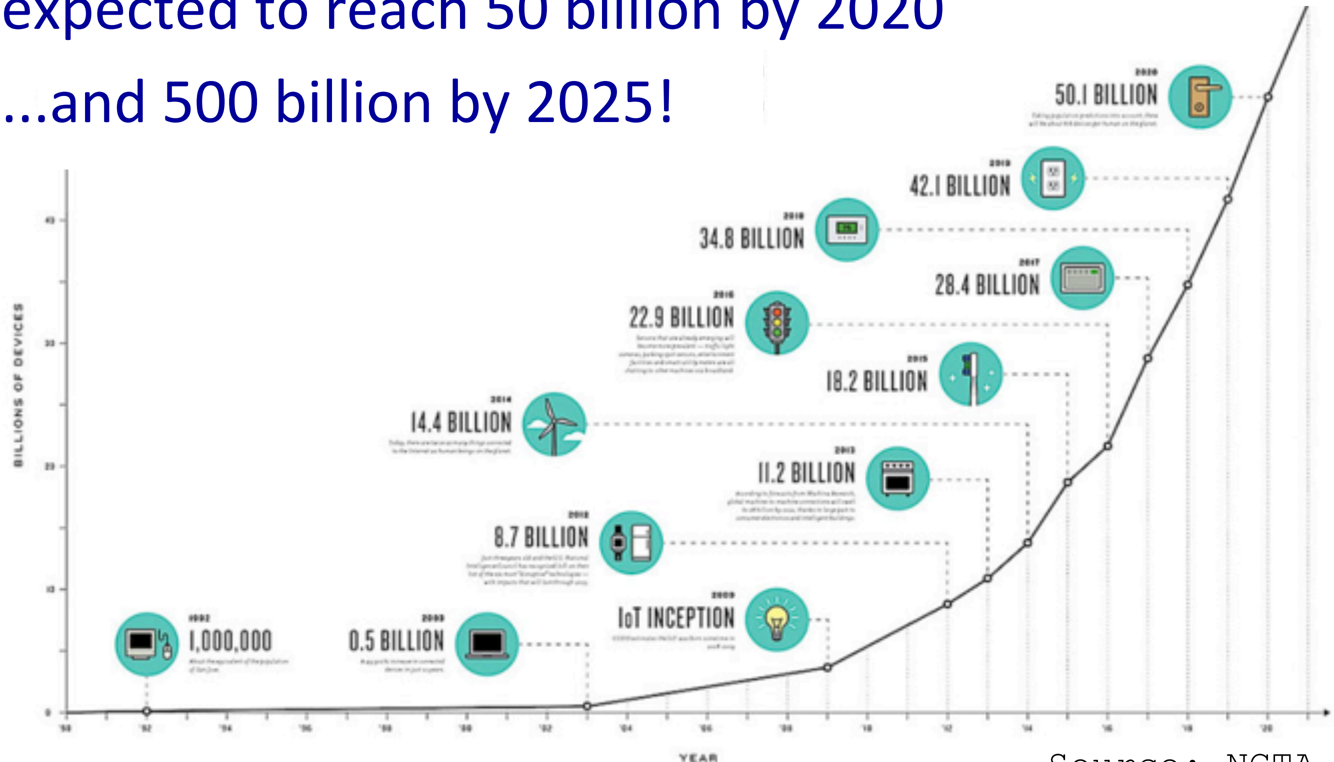
- Work
- Office
- Games

Things + People (today)

- Quality of life

Scenario

- The number of connected devices is growing rapidly
  - expected to reach 50 billion by 2020
  - ...and 500 billion by 2025!



Source: NCTA

(Good) Properties of IoT devices

- Innovative
- With the goal of improving the quality of life

(Challenging) Properties of IoT devices

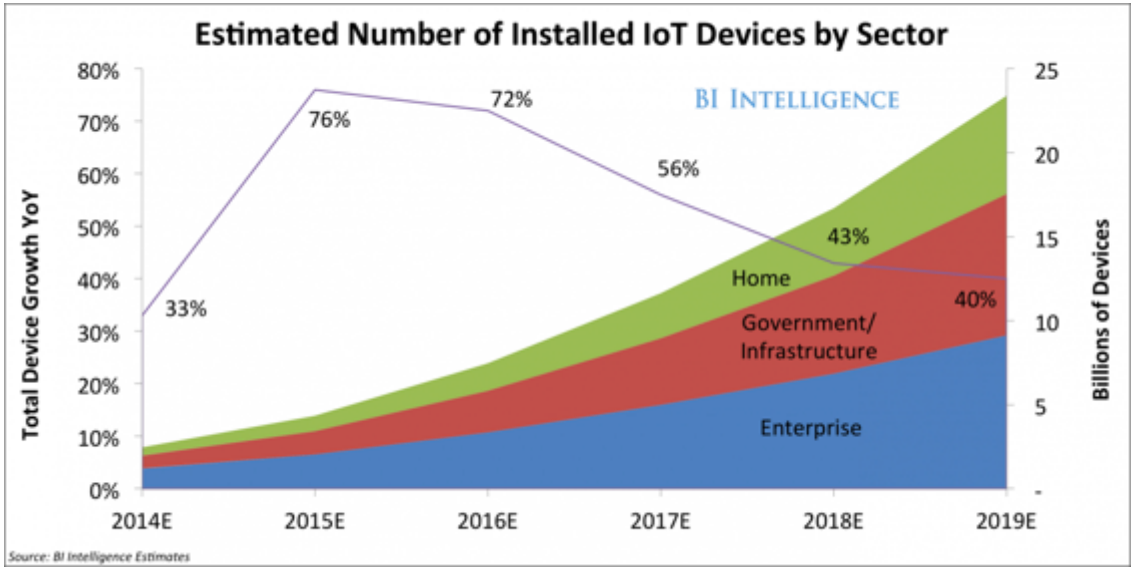
- Limited resources
  - Costs limitation
  - Power/Energy limitations
- Short Time-to-Market
  - Shorter design/verification/test processes
- Fabricated by new and possibly unreliable companies

(Bad) Properties of IoT devices

- It increases the number of security risks
- Any security hole in a IoT device can become an entry point to the whole system
- Privacy issues

Examples of critical scenarios

- Industry and Logistic (e.g., packages with built-in RFID)
- Medical environments
- Smart cities
- Home devices
- Autonomous cars
- Wearable devices



Surveillance Camera Attack

- A massive Distributed Denial of Service (DDoS) attack slowed down major websites
  - Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times
- Target: Dyn (a major DNS host)
- Attack: a weakness in surveillance cameras, that allowed installing malicious software in more than 25000 cameras!

CNRS LIRMM

Car attack

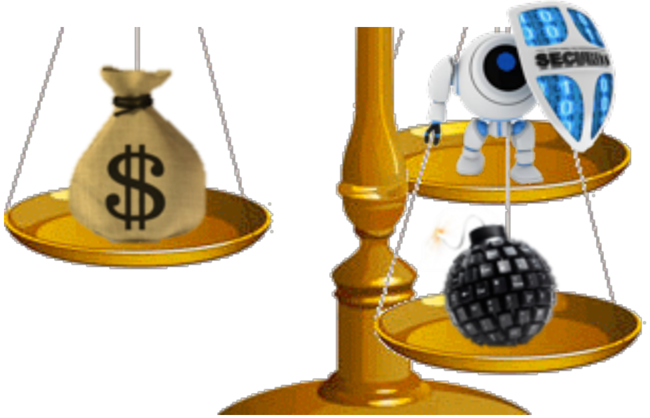
- A security hole in FCA's Uconnect internet-enabled software allows hackers to remotely access the car's systems and take control

- Google is developing a platform to connect cars to Internet
  - To lock or unlock vehicles, start the engine or even monitor vehicle performance from a computer or smartphone

What is security?

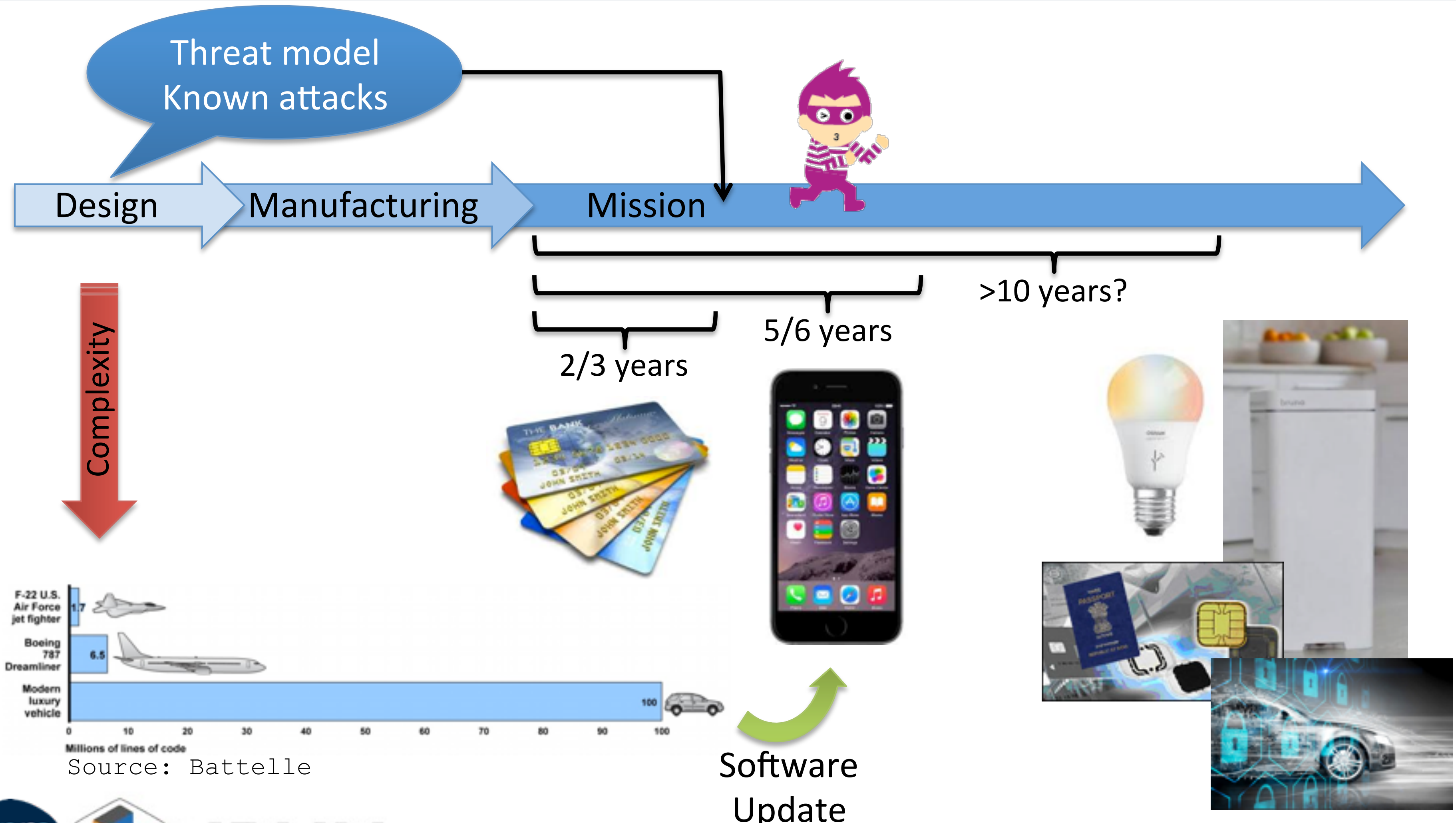
- It has to do with an asset that has some value
- From the dictionary: the state of being free from **threat**
  - Depends on what are you protecting your asset from (the threat)
- How to guarantee security?
  - Implementing countermeasures

Asset – Threat – Countermeasure

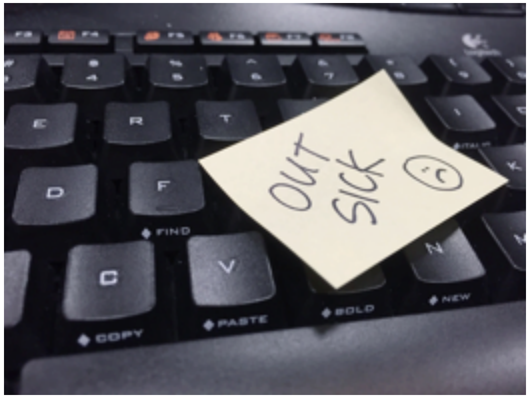


- Countermeasures are build upon a threat model
- The cost of the attack must be worth the asset
- The countermeasure must be cheaper than the loss of the asset
- Successful attacks:
  - Not modeled (i.e., new attacks)
  - Exploiting bugs or weaknesses

Where is the problem ?

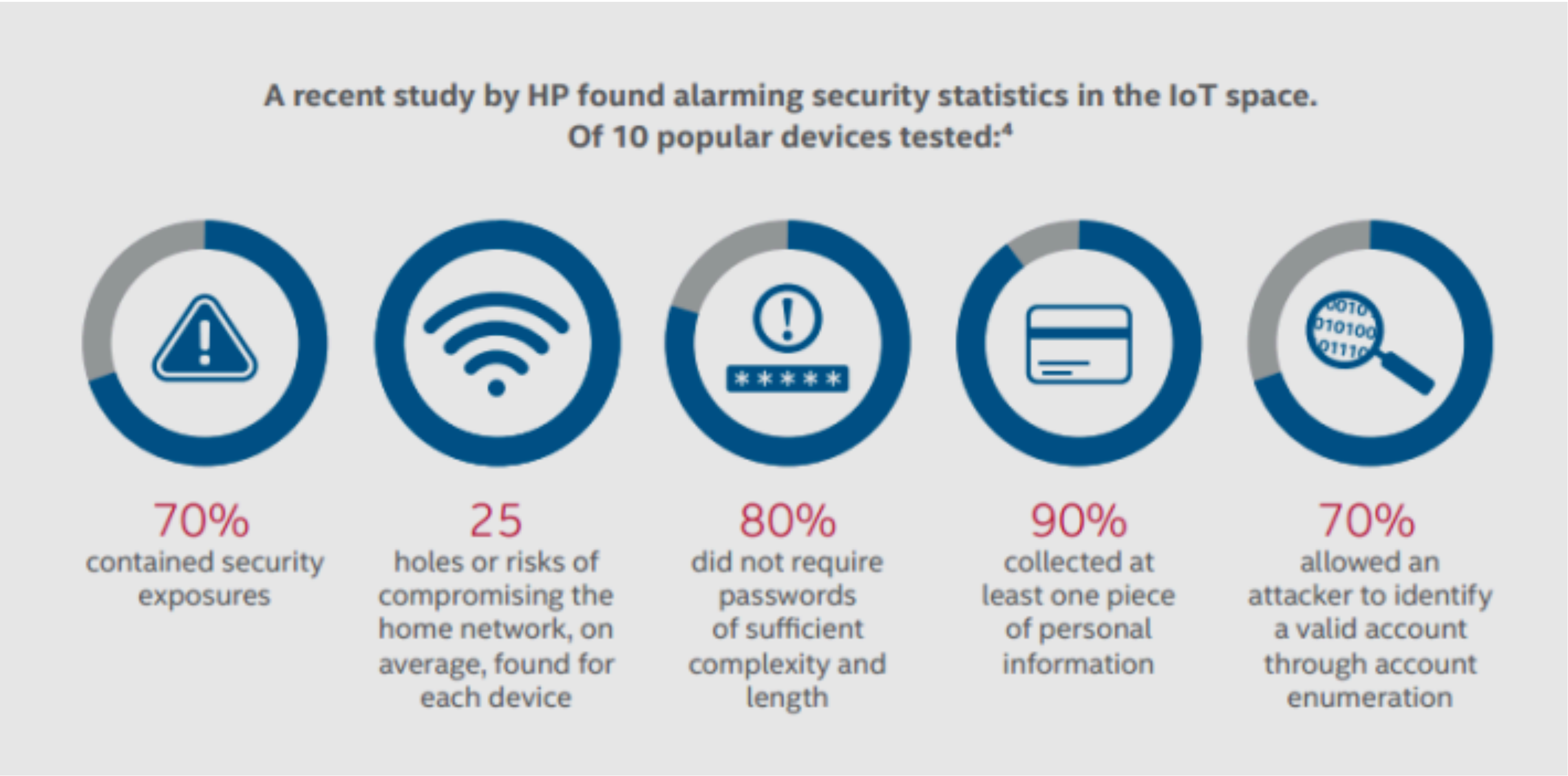


What can we expect?



- Plenty of "sick" devices:
  - Unsecure
    - Because new attacks are invented
    - Because too complex (i.e., bugs)
    - With bad settings
  - Without support/update
    - Because of unreliable companies
    - Because of lack of maintenance
  - Built with the intention of performing attacks
    - Malicious Hardware Devices

Some data



http://www.androidauthority.com/what-is-the-internet-of-things-592491/

Where to look for solutions?

- At all levels (hardware, firmware, software)
- For all devices
  - Things (sensors, actuators, devices)
  - Communication Infrastructures (routers, gateways)
  - Servers, Cloud

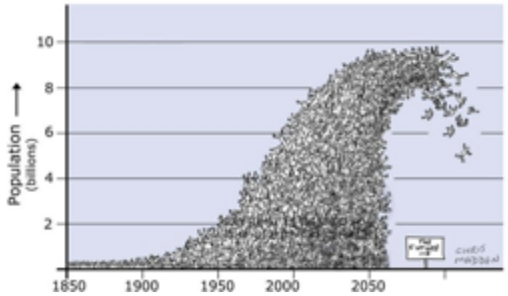
Research directions

- New EDA tools
- New standards
- Open Hardware
- More awareness

Conclusion

- Security is a competition
  - Attack vs Countermeasures

- With IoT we have to expect some of the devices not to be able to run fast enough



- New solutions and paradigms are required!

COST
EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY

TRUDEVICE