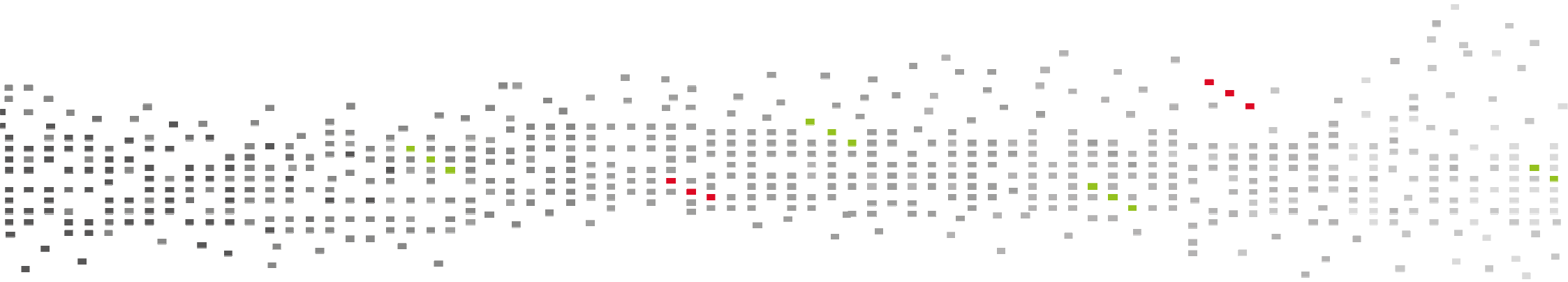


CHALLENGES OF THE EMERGING IOT SECURITY ARENA

Jacques FOURNIER, PhD, HDR
Senior Scientific Advisor
jacques.fournier@cea.fr

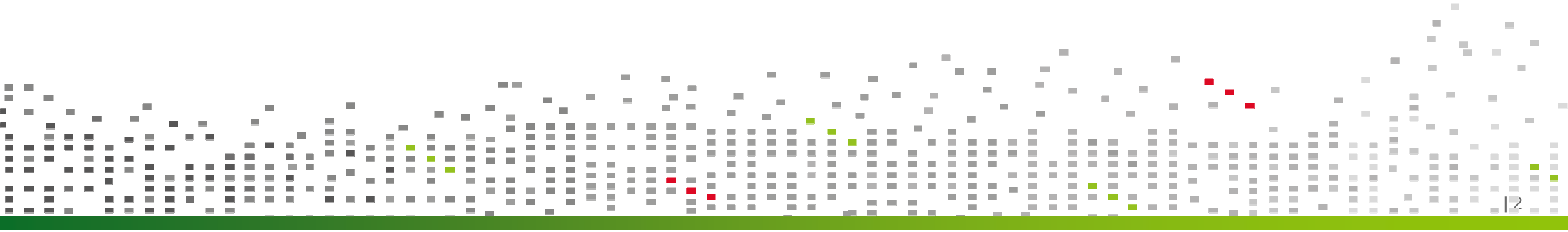
Alain MERLE, PhD
Strategic Marketing Manager
alain.merle@cea.fr

OVERVIEW

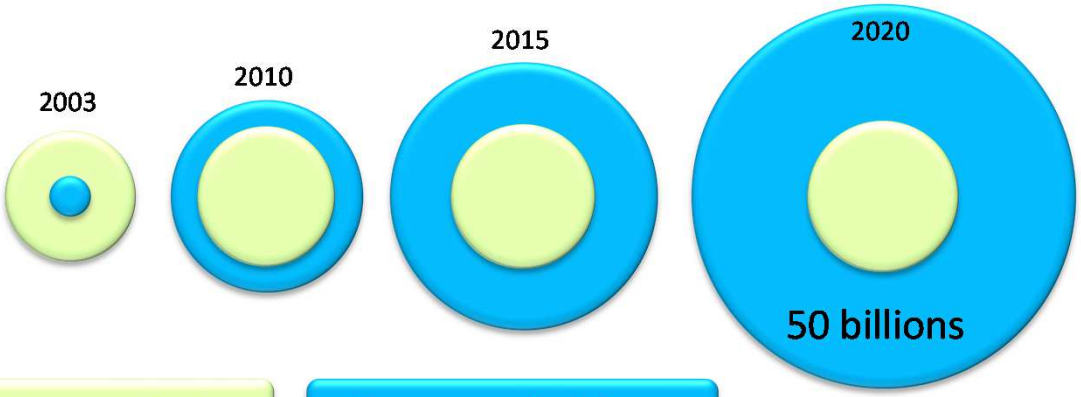
THE IOT (SECURITY) HYPE

HARDWARE SECURITY CHALLENGES FOR THE IOT

ADDRESSING THE IOT HARDWARE SECURITY CHALLENGES



2015 - 2020: THE IOT HYPE



Worldwide population

Connected objects

Source: CISCO, AT&T

Smart Homes

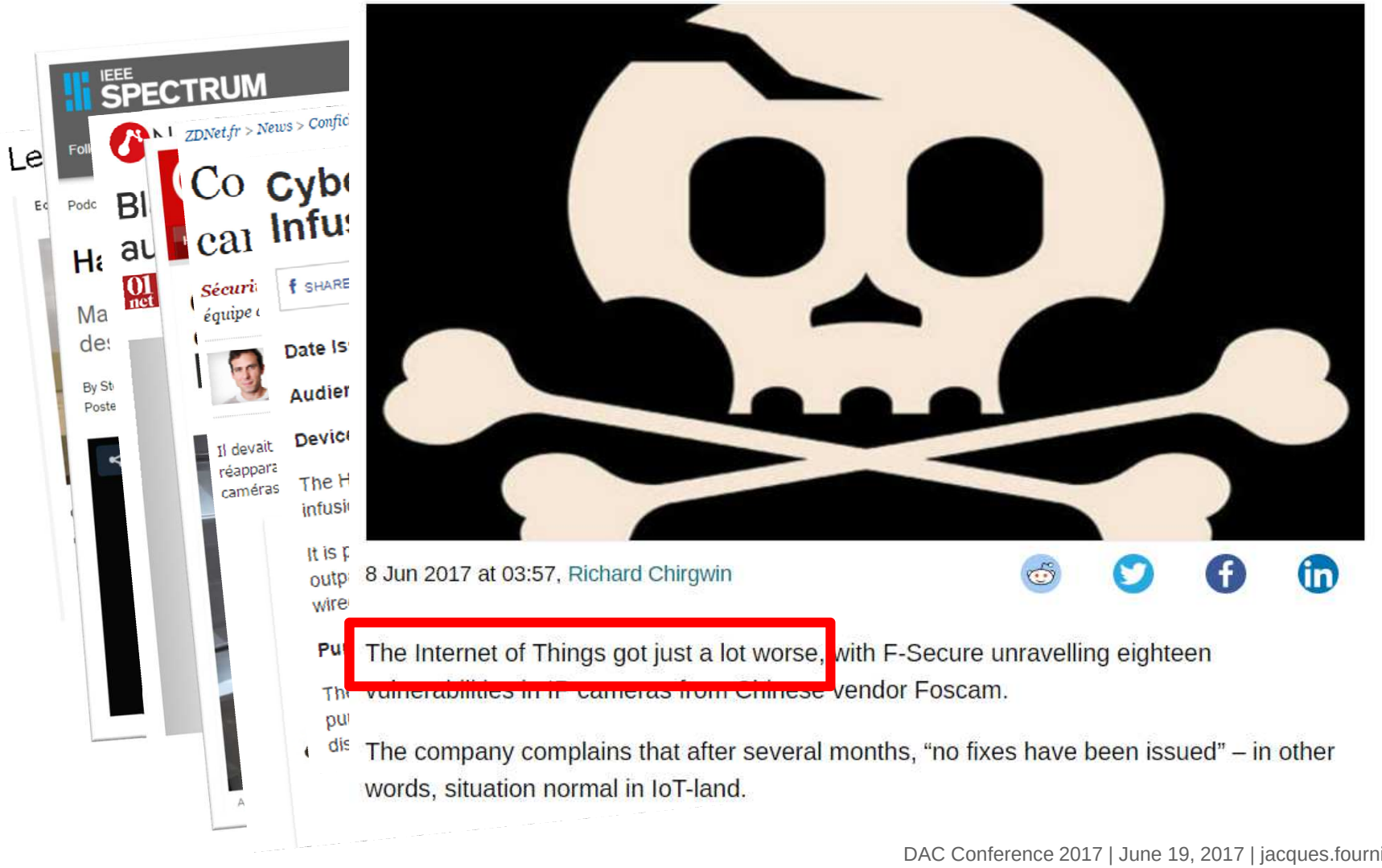
Intelligent transport system

Business environment

Logistics and retail environment

Health monitoring system

SECURITY: A SOCIETAL CHALLENGE



SOME RECENT NEWS…?

- **Attacks which are more and more impressive and concrete**

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

Major cyber attack disrupts internet service across Europe and US

- **DDOS attack on Dyn's DNS servers**
  - Access to 100s websites denied for several hours (GitHub, Twitter, Netflix, AirBnb…)
  - Some countries entirely disconnected (Liberia)
  - More than 1 million infected devices
  - > **1TBps**!

Attacking the infrastructure thru the node

IoT Goes Nuclear:
Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*

http://iotworm.eyalro.net/iotworm.pdf

- **Attack on Philips' HUE lamp**
  - Combined attack exploiting vulnerability in the Zigbee stack implementation, side channel against implemented crypto and non secure SW update
  - Chain reaction of « self infecting

Attacking the node

OVERVIEW

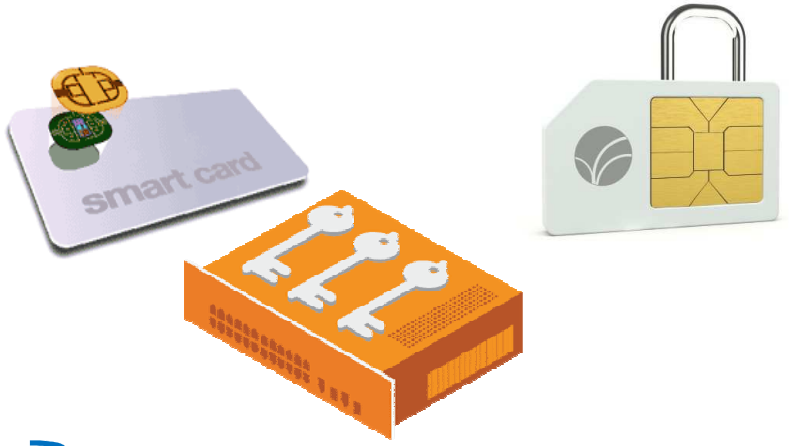
THE IOT (SECURITY) HYPE

HARDWARE SECURITY CHALLENGES FOR THE IOT

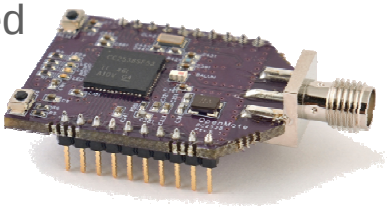
ADDRESSING THE IOT HARDWARE SECURITY CHALLENGES

FROM DEDICATED SECURE CIRCUITS TO SECURED IOT NODES

- **« Traditional » dedicated secure circuits**
  - embed a large proportion of security features
  - have a short life span
  - are manufactured in fully controlled fabs
  - often work in isolation



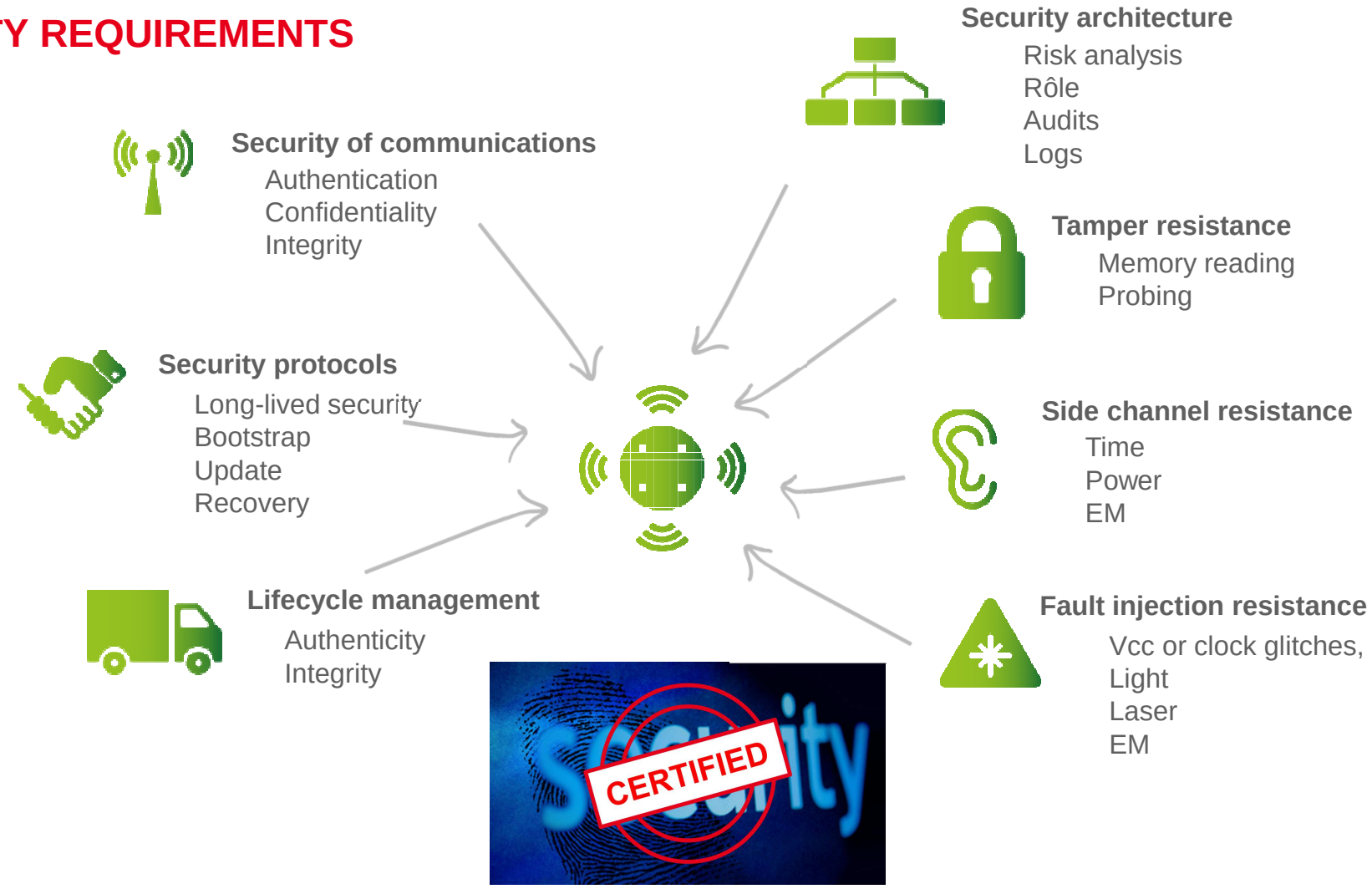
- **IoT nodes' requirements are more complex**
  - Power and performance constraints
  - Often have a long lifespan
  - Complex supply chains
  - Highly connected



« One-solution-does-it-all »?

Portfolio of security IPs for secure SoCs!

SECURITY REQUIREMENTS



By technology, architecture & embedded SW

IOT NODES' SECURITY CHALLENGES

- Trusted hardware / counterfeiting in a contexte of complexe supply chains
- Low power, fast cryptographic primtives for confidentiality, integrity, authenticity & privacy
- Massive deployment & on-the-field management
- Long lived security
- Secure update of devices
- Secure against physical attacks
- Protocols for end-to-end security

Adapting security for optimum trade-off between security, performance, power & cost

OVERVIEW

THE IOT (SECURITY) HYPE

HARDWARE SECURITY CHALLENGES FOR THE IOT

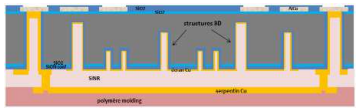
ADDRESSING THE IOT HARDWARE SECURITY CHALLENGES

ADDRESSING SECURITY REQUIREMENTS

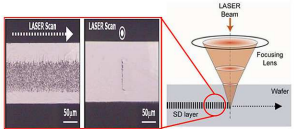
Security architecture

Use of EBIOS risk analysis tools

Tamper resistance



Backside protection
Optical shields
Mechanical protections

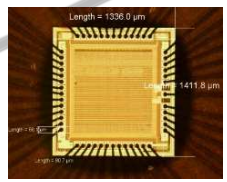


Security of communications

New cryptographic IPs (light weight crypto, Pairings, QS crypto)

Side channel resistance

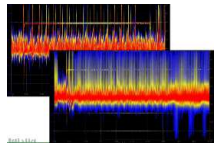
Side channel resistant crypto



ASIC "Double-Dual" Prototype:

- AES-128 / CBC mode enable / Encrypt only
- Number of gates: ~30000
- 128-bit datapath → 11 clk cycles per encryption

Dynamic code recompilation



Security protocols

Secure update mechanisms
Remote (anonymous) attestation
Software/IP binding

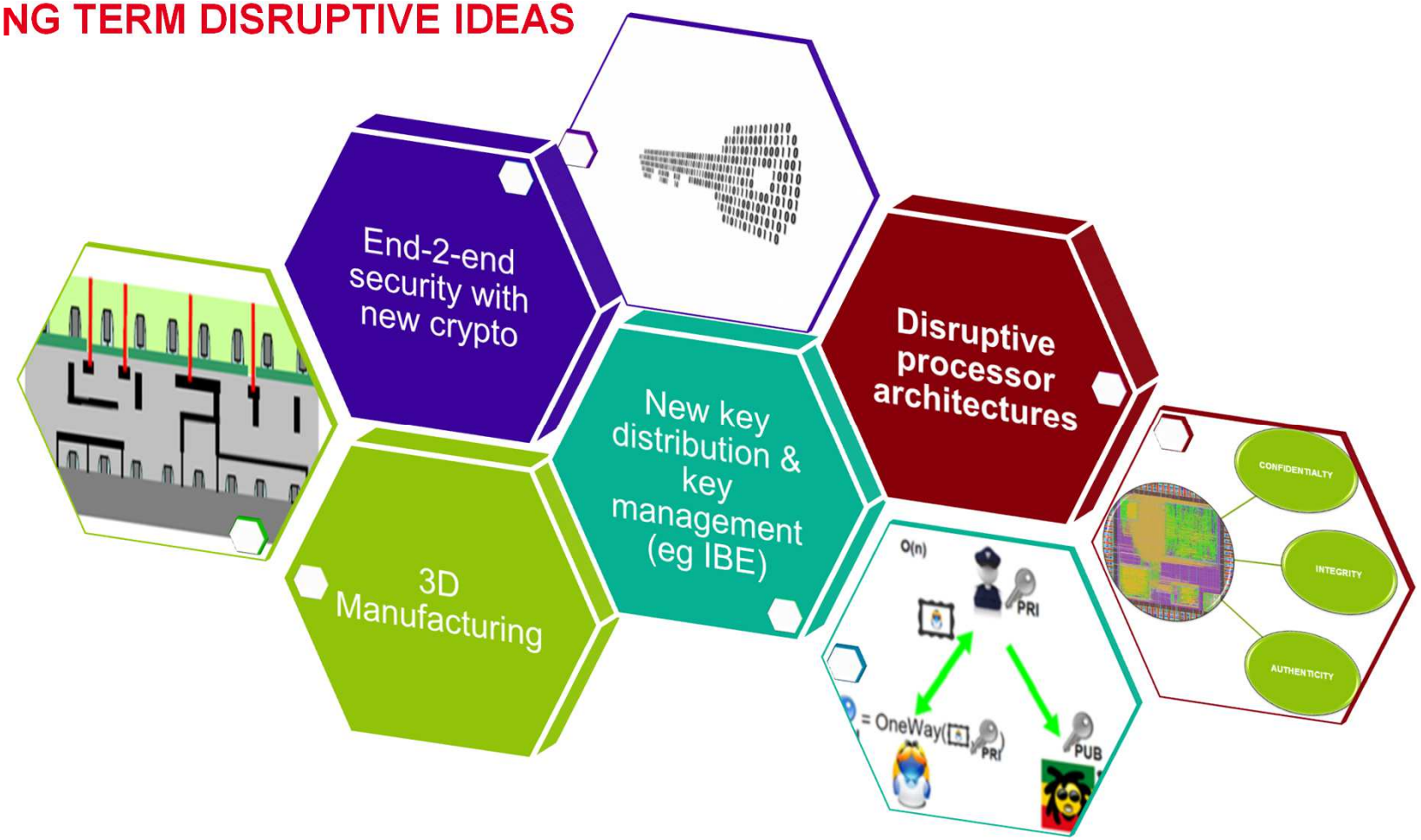
Lifecycle management

Authentication IPs (eg PUFs)
Counterfeit detection mechanisms
Trojan horse insertion

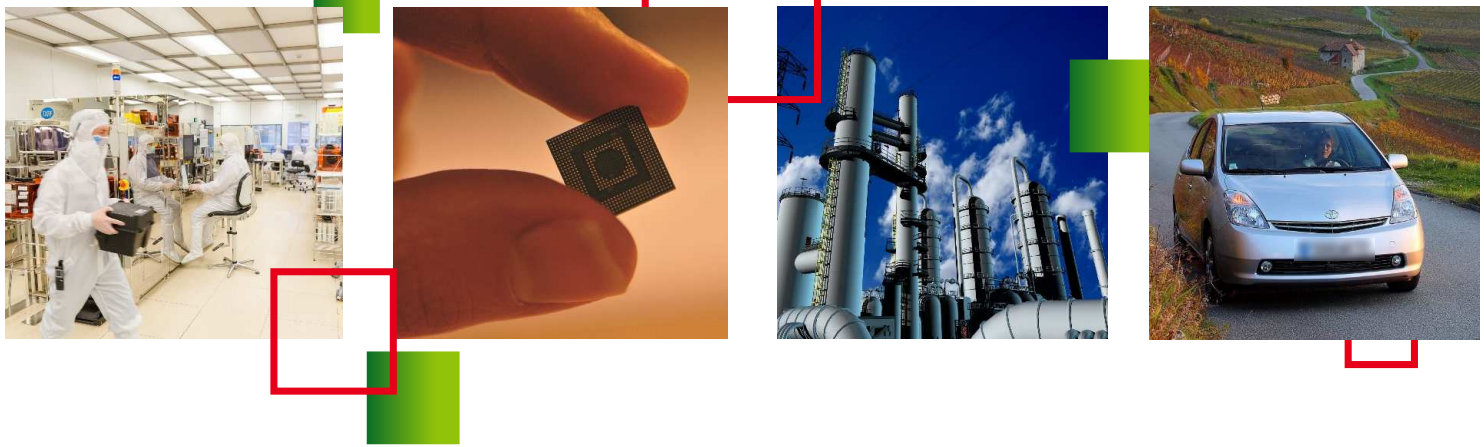
Fault injection resistance

Fault resistant crypto
Fault resistant processors
Error detecting mechanisms

SOME LONG TERM DISRUPTIVE IDEAS



Taking into account the secure implementation & integration of those IPs



LETI proposes

Integrated & efficient security solutions

Security evaluation capabilities

to our partners for securing applications & systems