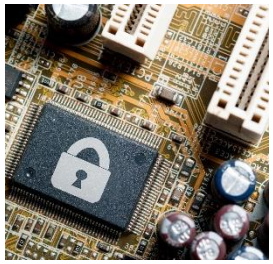


CYBERSECURITY AT CEA TECH : ASSESSMENTS AND SOLUTIONS

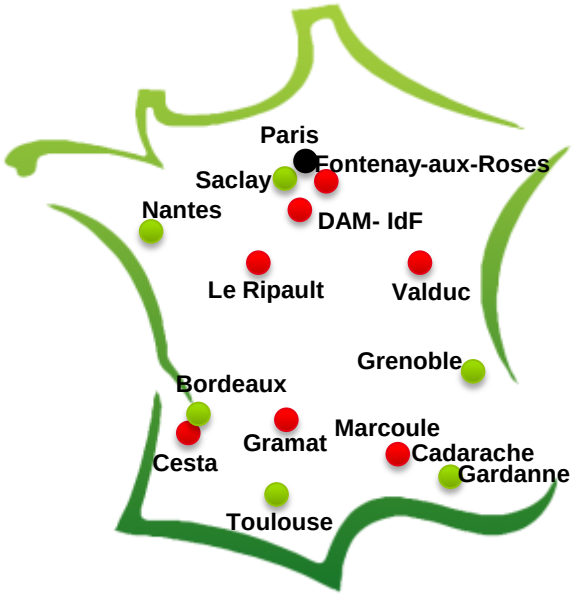
Alain MERLE, PhD
alain.merle@cea.fr

Florent KIRCHNER, PhD
Florent.kirchner@cea.fr

Assia TRIA, PhD
Assia.tria@cea.fr

CEA: FROM RESEARCH TO INDUSTRY

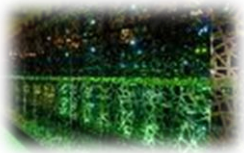
» 16 000 employees
» 10 research centers
» 4 regional extensions
» Budget of 4.3 billion €
» 650 patents/year
» 4000 publications/year
» 50 Joint Research Laboratory
» 150 startup creations in 30 years



Direction

Defense Security

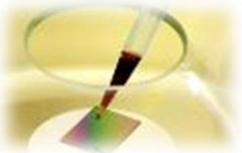
Military Applications Division



Nuclear Energy

Nuclear Energy Division

Key Enabling Technologies



Fundamental research

Materials Sciences Division
Life Sciences Division

Technology

Science

MISSION : To develop and disseminate new technologies for industry

- Annual operating budget of more than **€500 M**
- More than **50 HIGH-TECH START-UP** over the past 10 years
- **4,500 EMPLOYEES**
- **550 PRIORITY PATENT** applications per year par an

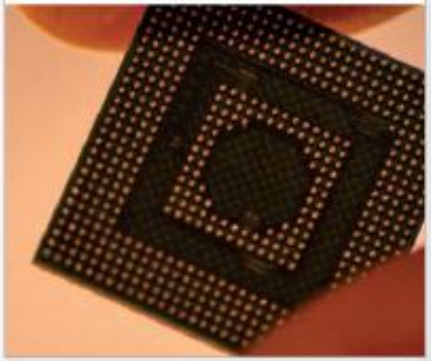
- **Our CUSTOMERS** :
  - ✓ **80 %** listed on the **CAC 40**
  - ✓ More than **500 SMBS**
  - ✓ **145 INTERNATIONAL CUSTOMERS**

World-class experts, « application » know-how and equipments

Micro- and nanoelectronics
7,000 sq. m. (clean rooms)
Staff: 800
Investment: €1 billion

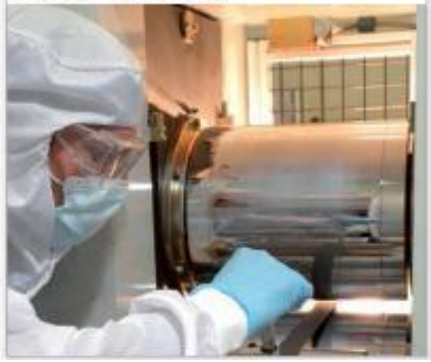
Nanocharacterization
2,500 sq. m.
Staff: 80
Investment: €30 million

Design
1,800 sq. m.
Staff: 100



Embedded systems
1,200 sq. m.
Staff: 180

Batteries
3,000 sq. m.
Staff: 200
Investment: €50 million

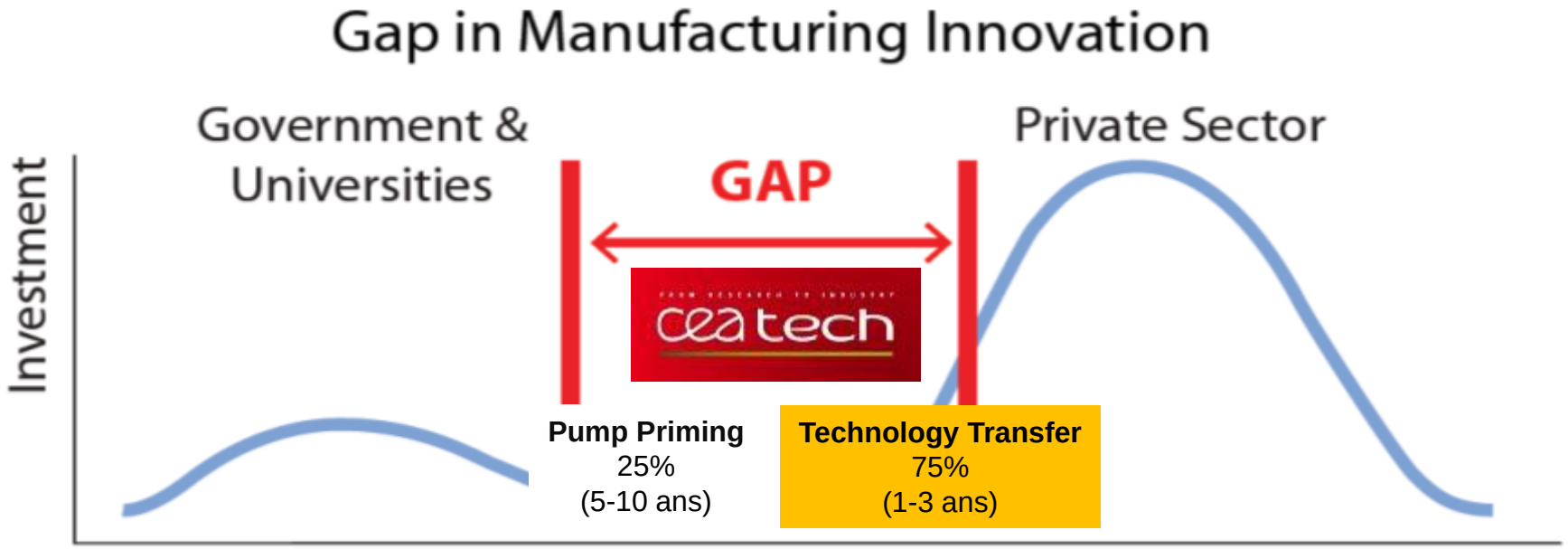


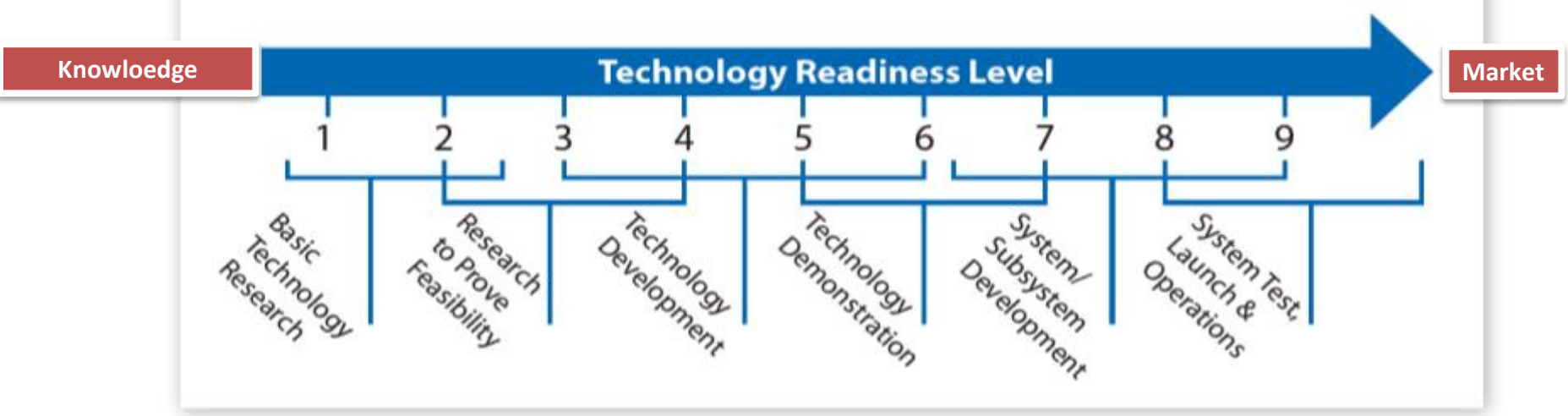
Solar
25,000 sq. m.
Staff: 360
Investment: €150 million

Clinatec
6,000 sq. m.
Staff: 100
Investment: €40 million

Advanced manufacturing
2,000 sq. m.
Staff: 200

CEA TECH: BRINGING COMPETITIVENESS TO OUR CUSTOMERS





Source: AMP Steering Committee

WHAT IS SECURITY?

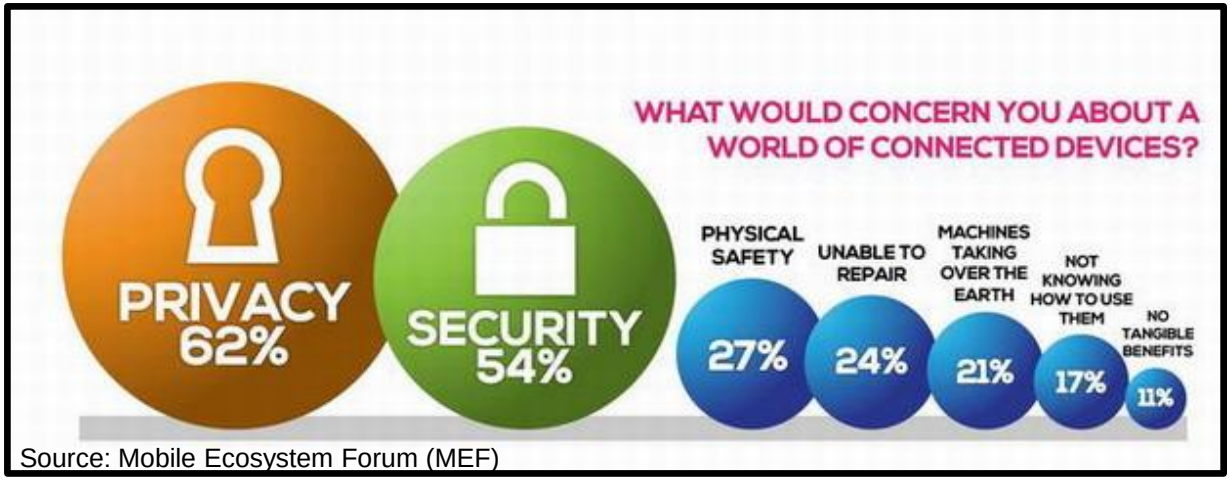
- **“The quality or state of being secure—to be free from danger”**
- **A successful organization should have multiple layers of security in place:**
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

SECURITY: A SOCIETAL CHALLENGE

Obstacles to the development of the market

Security | **Interoperability** | **Immaturity of the ecosystem**

Source: L'usine digitale
http://www.usine-digitale.fr/article/objets-connectes-les-chiffres-cles-du-marche-francais.N356834



Source: Mobile Ecosystem Forum (MEF)

Massive **adoption by citizens** relies on confidence on **security and privacy**

WHAT'S NEW: CYBERATTACKS ON THE REAL WORLD

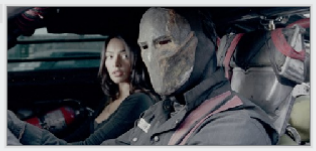
- 2007: Autodestruction of a generator in a power plant
- 2008: A polish teen derails a TRAM.
- 2010: STUXNET worm against the Iranian nuclear program
- 2010: Wireless sensors used for "carjacking"
- 2012: Risks on medical implants (pacemakers)

Le programme nucléaire iranien, cible de Stuxnet ?

Edition du 22/09/2010 Réagissez Partager

'Carjacking' for the twenty-first century.

Posted by Del in Articles, Cars - 12th August 2010



So the time has finally come when we are
total control of our vehicles. The trend to r
more on electronic devices to control ever
our cars is steadily increasing. From the r
mundane tasks of maintaining climate co
sending service reports to the dealer, our
longer the mechanical beasts of yesterye

Invented in the 30's but made viable in the
ECU (Electronic Control Unit) sits quietly monitoring sensors around your engine. This ECU controls e
from the air/fuel mixture to the ignition timing, providing a more dynamic method of controlling the perfo
efficiency of the engine. As technology has advanced, ECUs have become more complex and software
providing addition control of functions such as cruise control, transmission control, anti-skid brake, an
control.

Print Tweet J'aime 8

Polish teen derails tram after hacking train network

Turns city network into Hornby set

By John Leyden • Get more from this author

January 2008 11:56 GMT

donUses IBM BNTRackSwitch for HPC

AUSTRALIAN EDITION

SC MAGAZINE SECURE BUSINESS INTELLIGENCE

POPULAR: encase , investigati

HOME NEWS IN DEPTH REVIEWS EVENTS SC AWARDS

WHAT WE'RE FOLLOWING: AISA 2012 • Breakpoint • Ruxcon • Jobs • Print edition

Home / Security News / Hackers

Hacked terminals capable of causing pacemaker deaths

By Darren Pauli on Oct 17, 2012 12:33 PM
Filed under Hackers

Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.

Sources: Staged cyber attack rev
vulnerability in power grid

September 26, 2007 | From CNN's Jeanne Meserve

Share Twitter Email

Recommend 23 recommendations. S
what your friends reco

Researchers who launched an experimental cyber attack caused a generator to self-desti
alarming the federal government and electrical industry about what might happen if such
were carried out on a larger scale, CNN has learned.

Wireless Car Sensors Vulnerable to Hackers

Researchers figure out how to hijack sensor communications.

By Robert Lemos TUESDAY, AUGUST 10, 2010

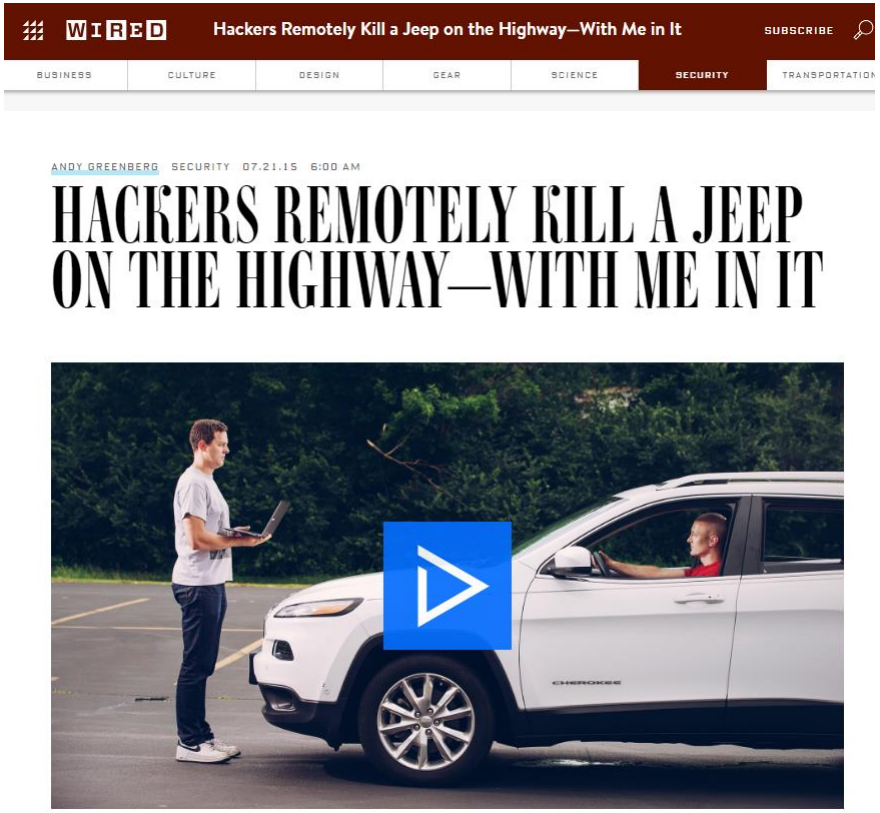
Hackers could 'hijack' the wireless pressure sensors built into many cars' tires, researchers have found. Criminals might then track a vehicle or force its electronic control system to malfunction, the University of South Carolina and Rutgers University researchers say.

Wireless kit: The equipment used to hijack a car's tire sensors included a laptop, a programmable radio

The team, which successfully hijacked two popular tire-pressure-monitoring systems (TPMS), will describe the work at the USENIX Security conference in Washington, DC, this week.

The tire-sensor attack poses little immediate risk to drivers. However, in recent months, research groups have identified other security weaknesses in vehicle electronics systems. As automakers add more powerful computers to cars, and connect those computers to critical components, in-car systems will need to be secured against hackers, experts warn.

CYBERSECURITY: A RISK FOR SAFETY



SECURITY: DEFINITIONS

Confidentiality

Objective	Attack types	Recent attacks	Protection
Ensuring that information is secret	Intrusion, Worms, hacking, …	AREVA, MASTERCARD, SONY, …	Cryptography, Smartcards, Dedicated Circuit (TPM)

Integrity

Objective	Attack types	Recent attacks	Protection
Ensuring that a system is not modified	Worms, trojans…	Payment terminal in UK, Stuxnet	Cryptography, Trusted computing

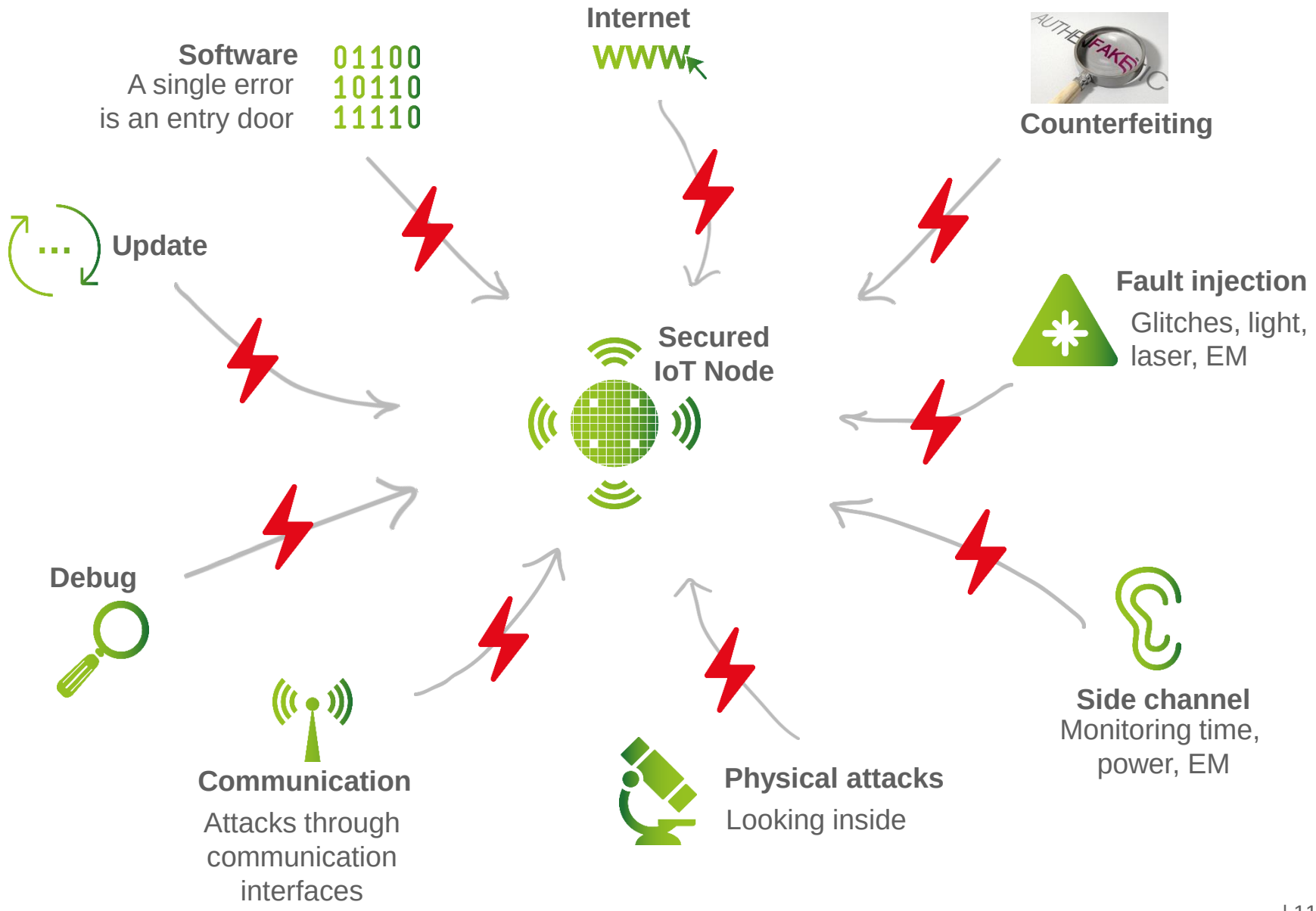
Availability

Objective	Attack types	Recent attacks	Protection
Ensuring availability of a system	Denial of service, Anonymous	Estonia, Anonymous	Very difficult ! Some protection for web sites

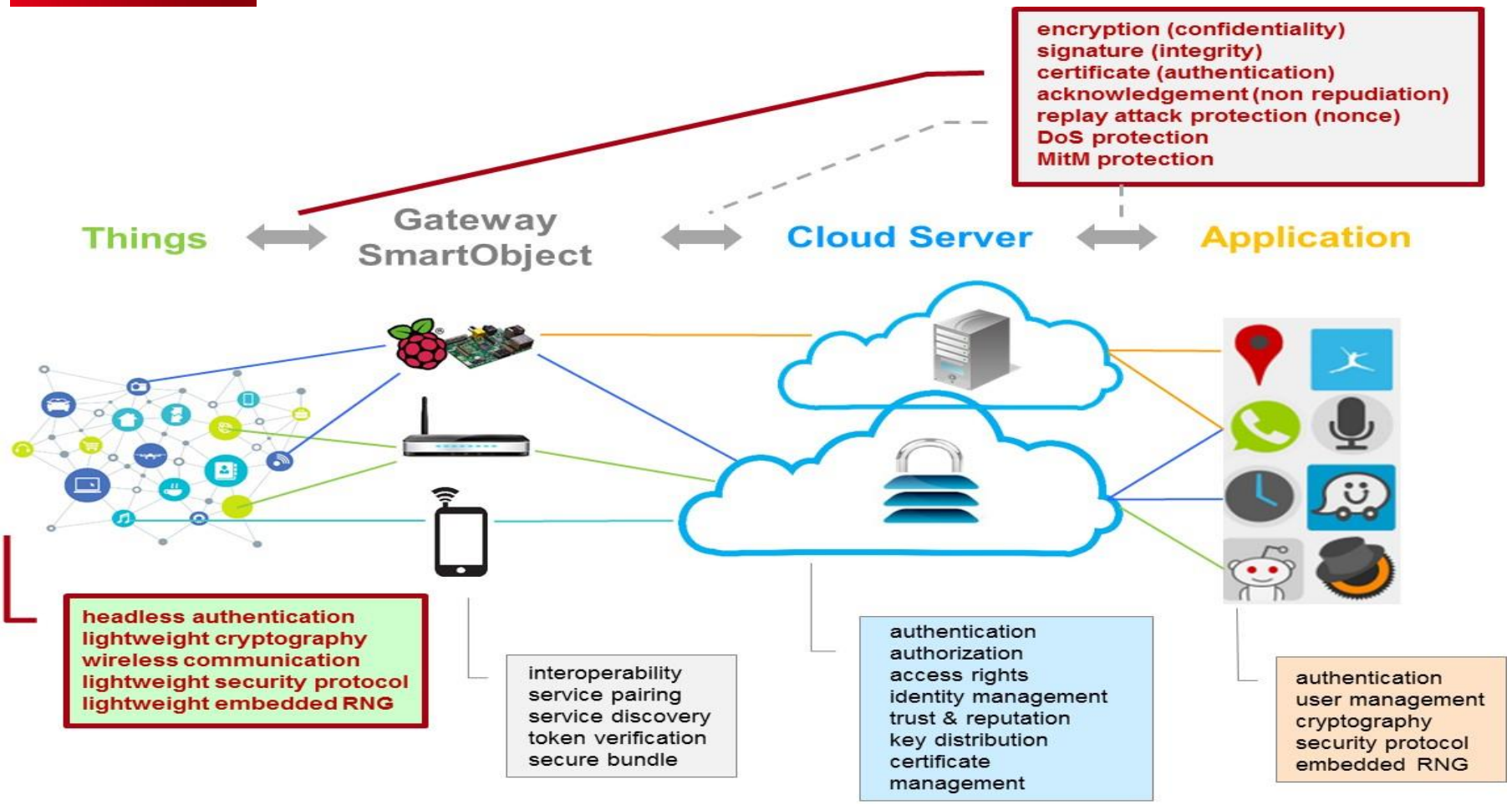
Authenticity

Objective	Attack types	Recent attacks	Protection
Ensuring the user/component is the right/genuine one	Cloning	Pay TV, Counterfeiting	Smartcards, Secured devices

SECURITY IS COMPLEX



CRYPTOGRAPHY IS COMPLEX



- **Key management: Bootstrap, Update, Recovery**
- **Intrinsic resistance**
  - Moore's law: increasing key size (DES, TDES, AES 128, AES 256)
  - Quantum computer : killing asymetric cryptography

SECURITY OF COMMUNICATIONS

Secured by Cryptography

Channel is secured….

But, if an attacker has a physical access, he can extract the keys

SECURITY REQUIREMENTS

Security of communications
- Authentication
- Confidentiality
- Integrity

Tamper resistance
- Memory reading
- Probing

Security protocols
- Bootstrap
- Update
- Recovery

Side channel resistance
- Time
- Power
- EM

Lifecycle management
- Authenticity
- Integrity
- Update

Fault injection resistance
- Glitches,
- Light
- Laser
- EM

By technology, architecture & embedded SW

NEED FOR A OBJECTIVE MEASURE AND LABEL

Looking backwards

Efficiency of the Evaluation/Certification schemes for Smartcards

Common Criteria

No Security standard for emerging markets

Needs expressed:

- Industrial systems
- Medical devices
- Automotive
- IoT
- Biometrics
- Home appliances
- …

Key elements for the future

Standard & trustworthy Certificates

CEA-TECH'S RESEARCH AXIS

Secured ICs

New protection schemes

PUF, Shielding, Sensors, Architectures…

ICs for IoT

Low Power, Low cost, Efficient protections

Adapted cryptography « Zero Power » Protections

Security IPs

Security by Design

Cyberphysical systems

System security

Safety, Security & Privacy by design

More security

Best tradeoff

Security everywhere

Security for everything

INNOVATIVE SOLUTIONS

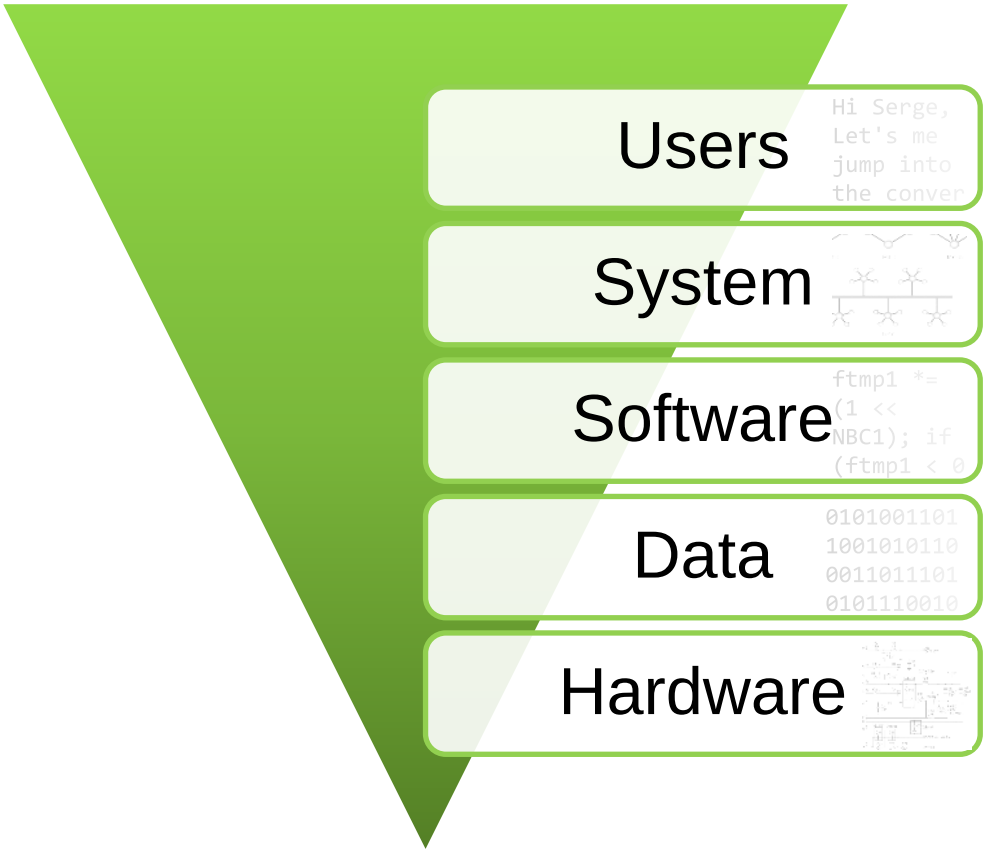
OUR PROMISE

- **Establish strong guarantees for the security of systems**
- **Based on cutting-edge mathematical techniques and reasoning capabilities**
- **In automotive, avionics, connected objects, drones, health, IT, smart grids, …**

THE CHANGE WE SEEK TO MAKE

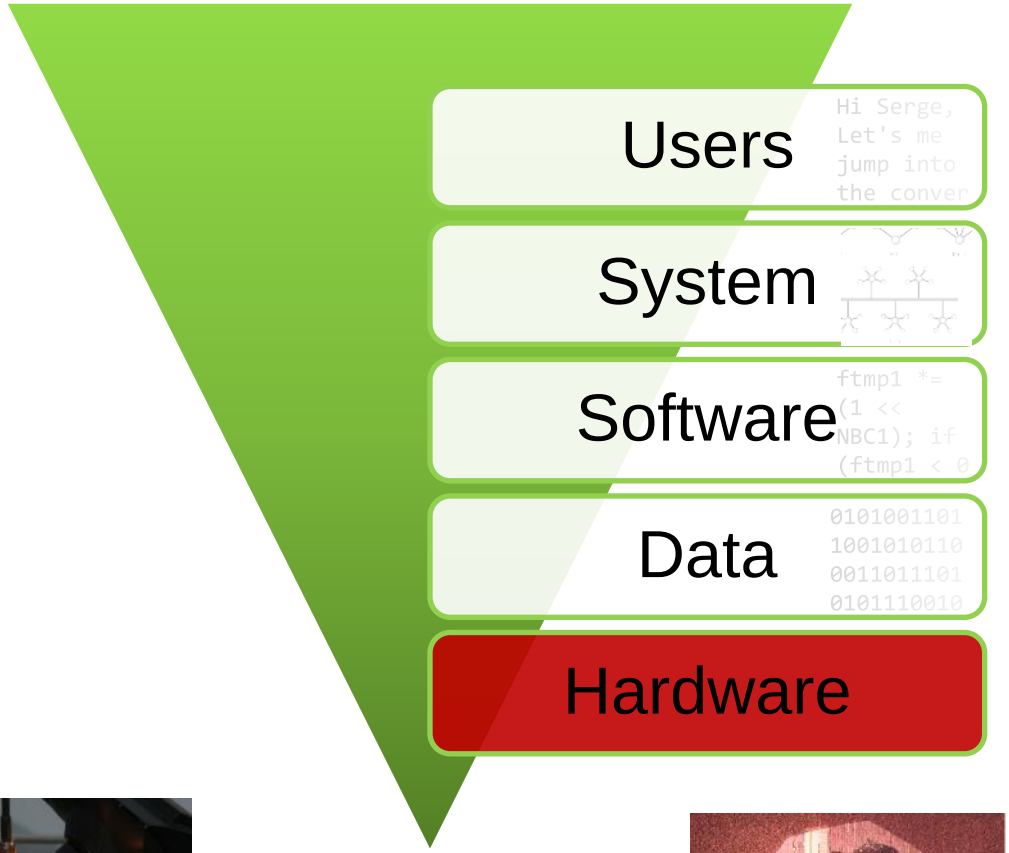
- **Develop highly innovative solutions to industrial challenges**
  - Communication services
  - Intrusion detection systems
  - Cryptographic techniques
  - Data analysis for privacy
  - Source code assessment and verification
  - Malware analyses
  - System-level risk analyses
- **Transfer next-generation components and tools to technical teams**

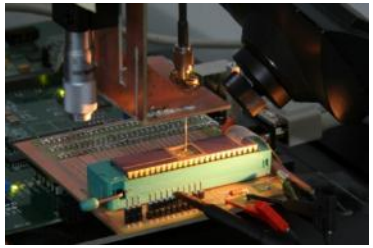
WE HELP OUR PARTNERS DELIVER HIGH-CONFIDENCE SYSTEMS

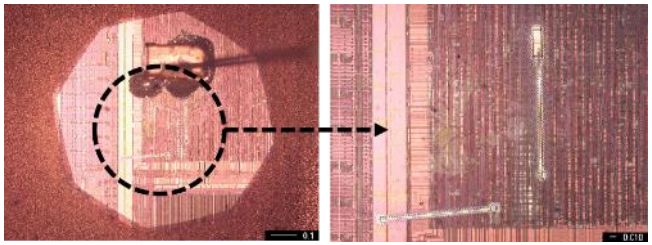


“Trustworthy computing (with software) cannot exist until we have trustworthy hardware to build it on”

Dr. Dean Collins, Deputy Director, DARPA


Users
Hi Serge,
Let's me
jump into
the conver
System
Software
ftmp1 *=
(1 <<
NBC1); if
(ftmp1 < 0
Data
0101001101
1001010110
0011011101
0101110010
Hardware

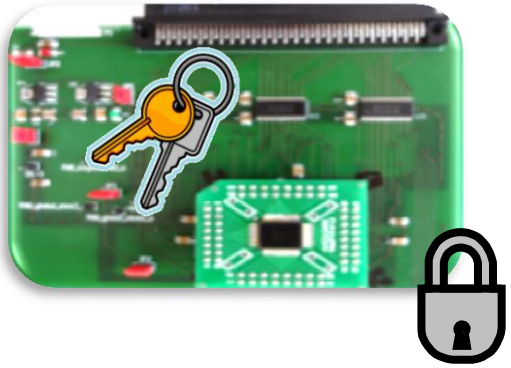




ATTACKS ON SECURE DEVICES

Cryptanalysis

RC5,
MIFARE,
Brute force attacks,
Etc.

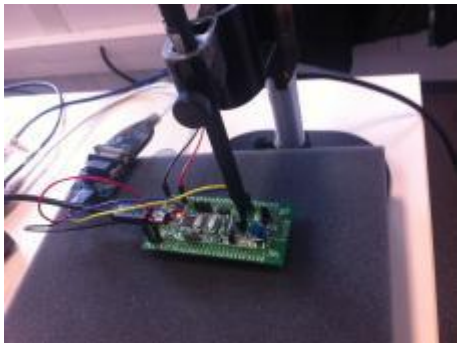


Software attacks

Buffer overflows,
Brute force attacks,
Attacks on protocols
Etc.

Hardware attacks

Extremely powerfull thanks to the direct access to the component:

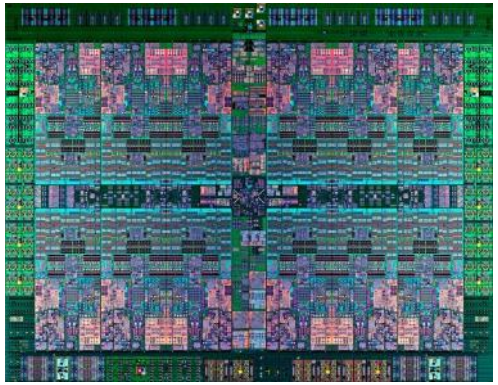


Example:
AES-128 key cracking in minutes on a 32-bit unsecure microcontroller

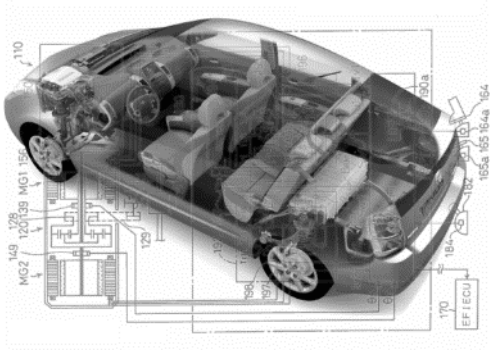
HARDWARE SECURITY

- **Secure design of components and systems**
- **Strong links with telecommunications**

- **Tradeoff**
  - Security level
  - Power consumption
  - Size / volume
  - Cost



Tamper resistant chip design

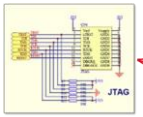


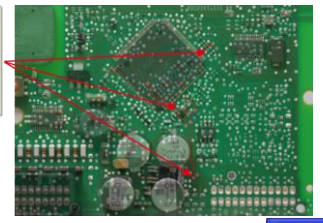
Cost effective solution

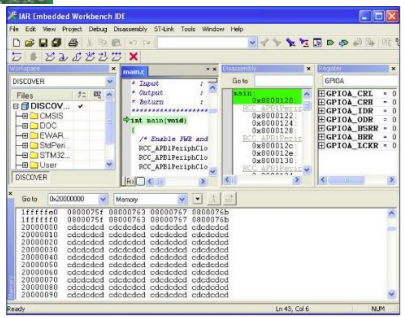
IoT dedicated cryptography

Ultra low cost pairing

HARDWARE SECURITY

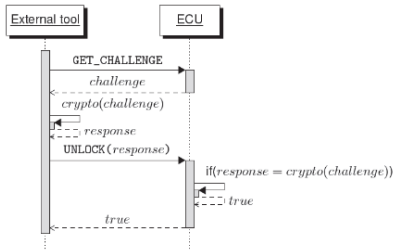






- **Debug ports exploits**
  - JTAG, USB, UART, SPI…ports
  - Read/write memory space
  - Access MCU internal registers
  - Control execution
  - Code injection

- **Debug port protections**

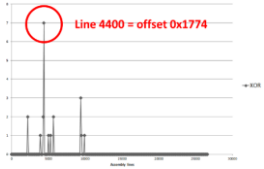


- **CAN/CCP exploits**
  - The CANApe ECU debug tool

- **Alternative boot**
  - Exploiting MCU interfaces
  - PCB-level protections

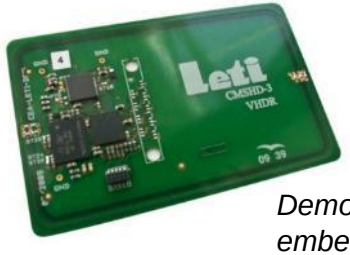
Boot mode selection pins		Boot mode	Aliasing
BOOT1	BOOT0		
X	0	User Flash memory	User Flash memory is selected as the boot space
0	1	System memory	System memory is selected as the boot space
1	1	Embedded SRAM	Embedded SRAM is selected as the boot space

- **Firmware protection**
  - Cryptographic protections against reverse engineering
  - Software-based code injection protections



LIGHTWEIGHT CRYPTOGRAPHIC IMPLEMENTATIONS

- **Different cryptology methods**
  - Elliptic curves, stream ciphers, lattice based, …
- **System integration targets**
  - FPGA
  - Microcontrollers
  - Mixed architectures
- **Optimizations**
  - Time: throughput, latency
  - Digital footprint
  - Memory size
  - Power budget



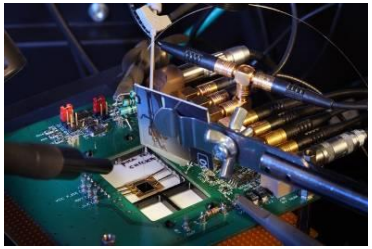
Demonstrator of embedded cryptography in a contactless card

Implementation of lightweight asymmetric cryptographic primitives in the IoT nodes deployed in smart-cities

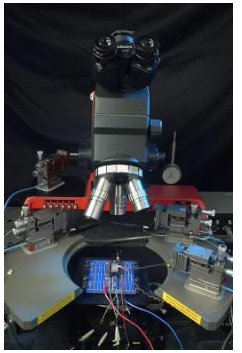
EVALUATION PLATFORMS

- More than 15 dedicated, home-made, test benches

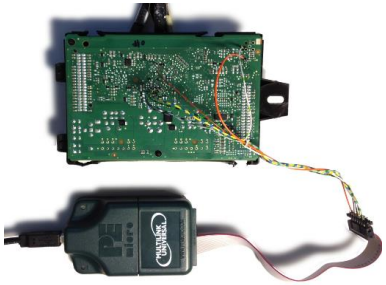
Nano-Characterization Platform



Side Channel Platform



Physical attacks Platform

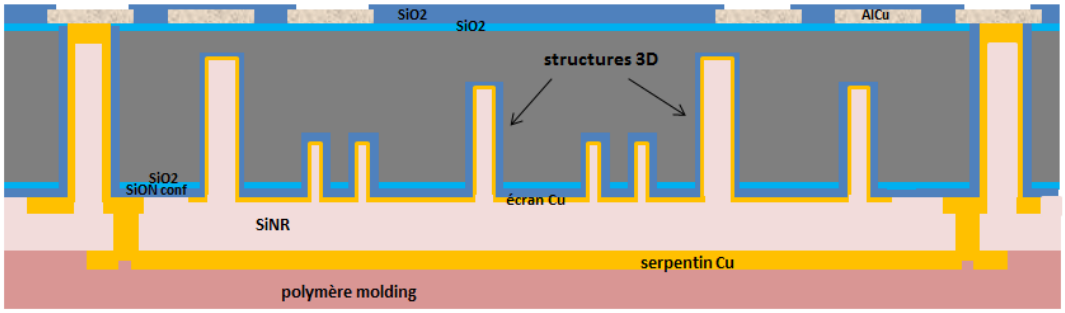


J-TAG Platform

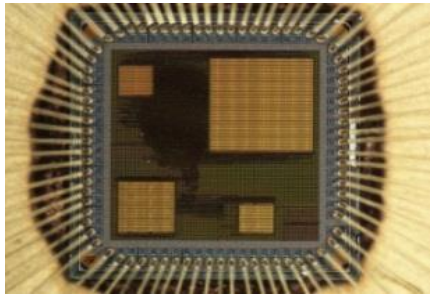
Fault injection Platform

Software analysis Platform (LIST)

- **Challenges: Low resources**
  - Adapted cryptography (Stream cypher, ECC, …)
  - Reduce the Nb of counter-measures
  - Choose low resources ones: from active to passive
  - New protections



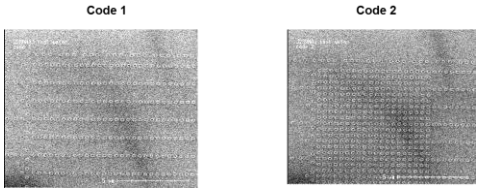
Shielding (Patented)



Architectures

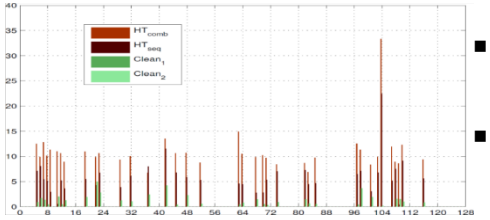
- Dual rail encoding
- Masking
- Fault detection
- Sensors

Unique ID



E Beam

PUF



- Trojan / Clones detection
- Authenticity

EXAMPLES

NFC

- Listening (more than 20m)
- Relay attacks

Smartphones

- DPA (EM) on a Cryptolib

Biometrics

- Fake fingers spoofing

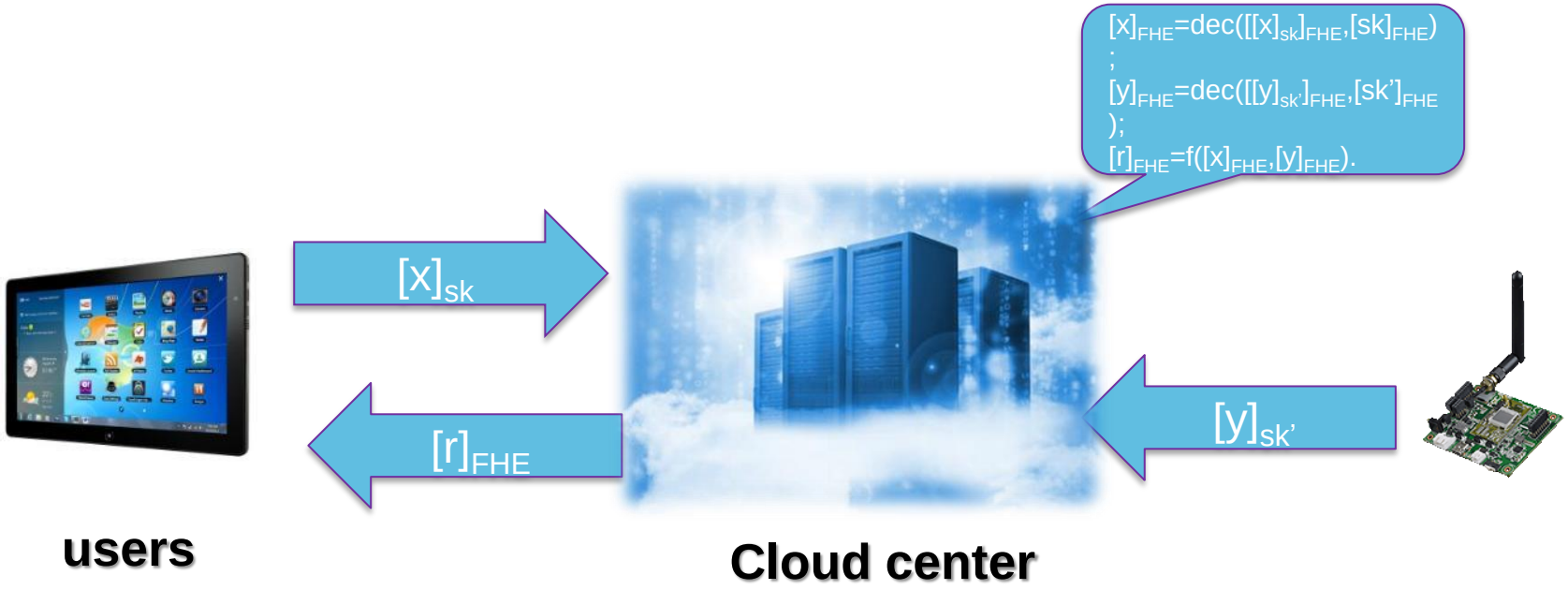
- Users
- System
- Software
- **Data**
- Hardware

PRIVACY

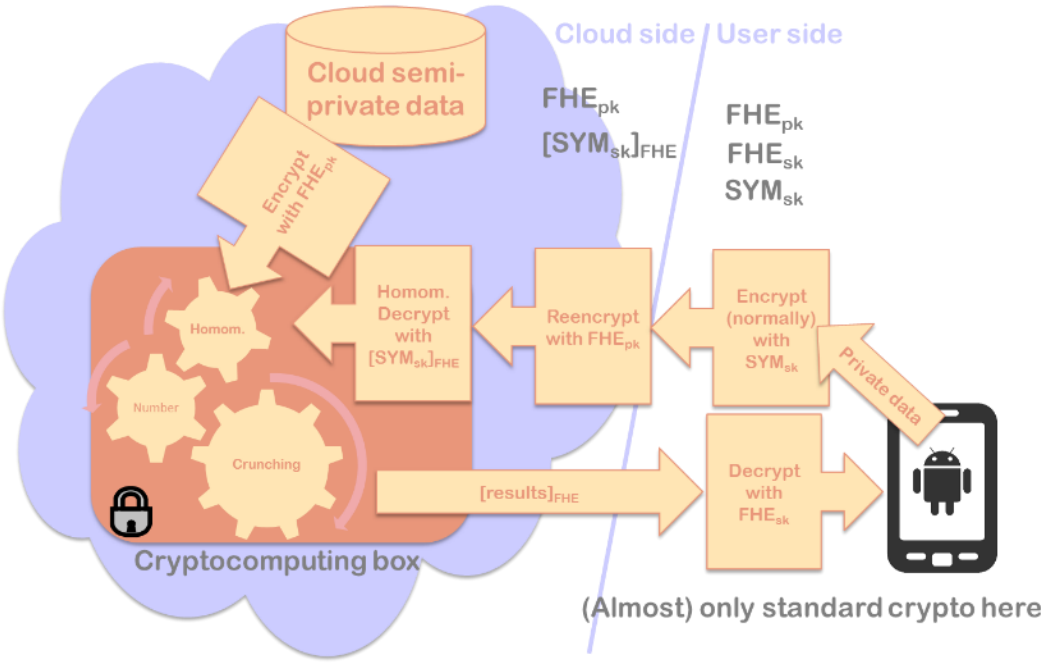
- **Many supports can tell so much**
  - Obvious : e-ID / Internet / RFID / Localization
  - Less obvious: IoT / WSN / Wireless / Side-channel
  - Cross-channel tools: aggregation / data mining
- **Raise partners awareness**
- **Provide protections**
- **Research activities**
  - Anonymity
  - Untraceability
  - Unlinkability
  - Pseudonimization
  - Next generation e-ID documents
  - Secure protocols for the IoT
  - Contactless systems
  - And generally embedded systems

HOMOMORPHIC ENCRYPTION

The cloud computers can process data &/or perform calculations from users and IoT sensor nodes without revealing the data



Perform blindly a medical diagnosis (Cardiovascular disease risk factors)



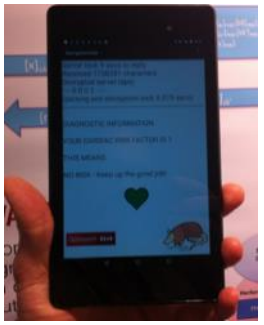
SETUP

- The Android tablet sends the encrypted private user health data
- The server receives and homomorphically « transcripts »
- The server homomorphically executes the diagnostic algorithm and sends back the encrypted answer to the tablet.
- the tablet is the only party able to decrypt and thus interpret the server reply

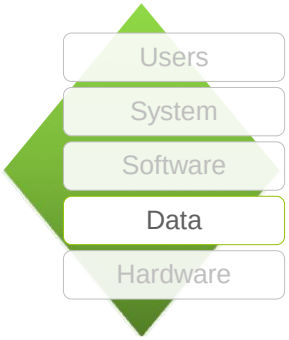
PERFORMANCES

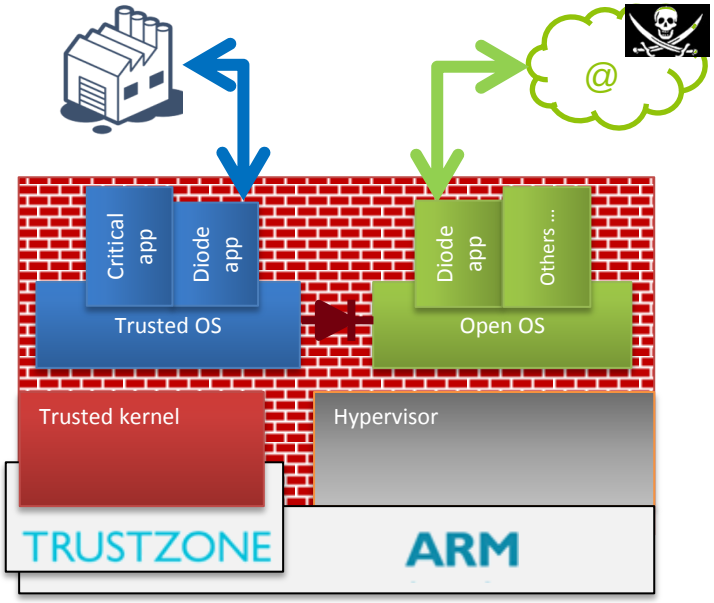
- 3.3 secs for program execution on the server
- < 4 secs RTD towards servers.

Prototype



SECURE EXECUTION ENVIRONMENTS
ADVANCED CRYPTOGRAPHY





Protect the confidentiality and integrity of computations even in case of compromission

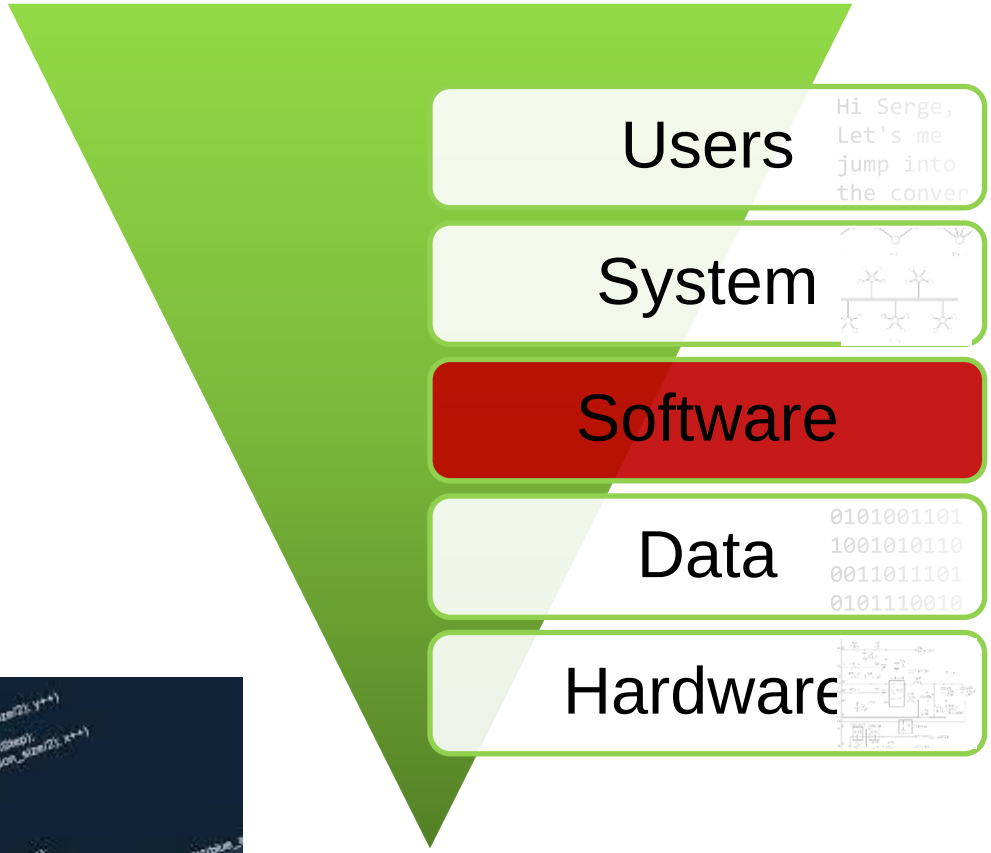
- **HW/SW partitioning of a trusted functionality**
- **Spatial and temporal security by design of the execution environment**
- **Fully homomorphic encryption SDK for cloud computation scenarios**

Atos THALES

Feasible industrial implementations of homomorphic encrypted computations

KRONO-SAFE

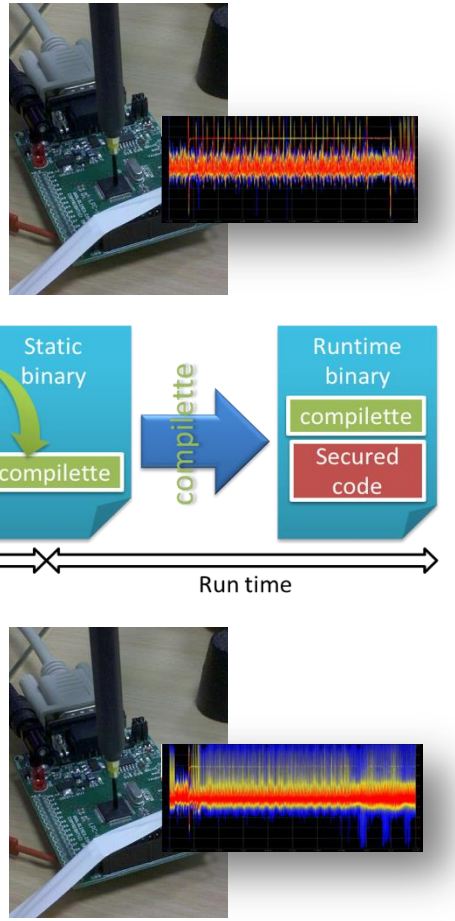
Implementation of a high-reliability, high-performance operating system


Users
Hi Serge,
Let's me
jump into
the conver
System
Software
Data
0101001101
1001010110
0011011101
0101110010
Hardware

SECURE COMPILATION

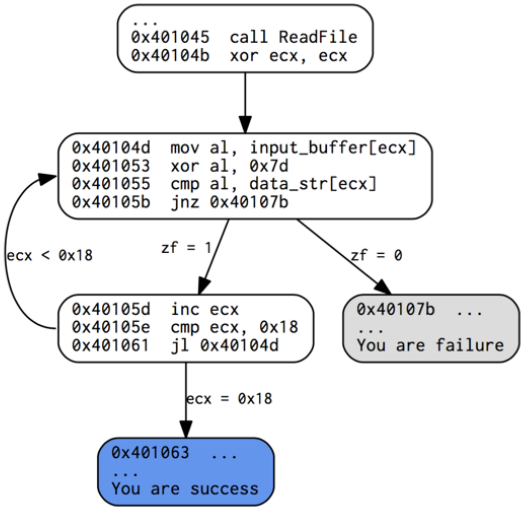
How to generate components that are protected against reverse engineering-based attacks?

- **Runtime code generation using code polymorphism techniques**
- **deGoal static compilation phase**
- **Compilette runtime generator**
- **fast code generation & tiny memory footprint**



MALWARE ANALYSIS

Perform flawless binary code analysis based on mathematical reasoning: simulation, static analysis and symbolic execution.



DGA

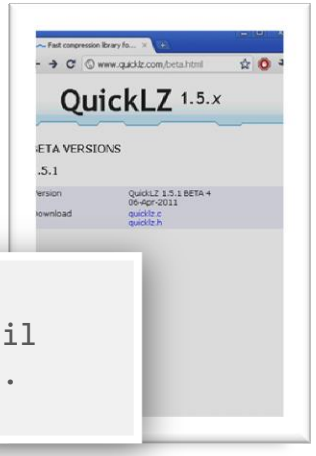
Pre-integration of an exhaustive malware analysis engine into an advanced security toolbox

EXHAUSTIVE VULNERABILITY DETECTION

Verify the source code in critical components for "advanced vulnerabilities"

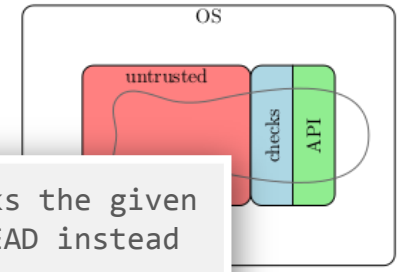
- **Complete detection of the most common vulnerability classes**
- **Providing mathematical guarantees for a security perimeter**
- **Advanced verifications: API security policy checks, information flow analysis, runtime monitoring, …**

frama C Software Analyzers




```
Fixed a condition where
QLZ_MEMORY_SAFE could fail
detecting corrupted data.
[CWE-120]
```

EMC² facebook AGFA




```
ZVMReadHandle checks the given
buffer with PROT_READ instead
of PROT_WRITE.
[CWE-120]
```

ZEROVM

NIST National Institute of Standards and Technology U.S. Department of Commerce

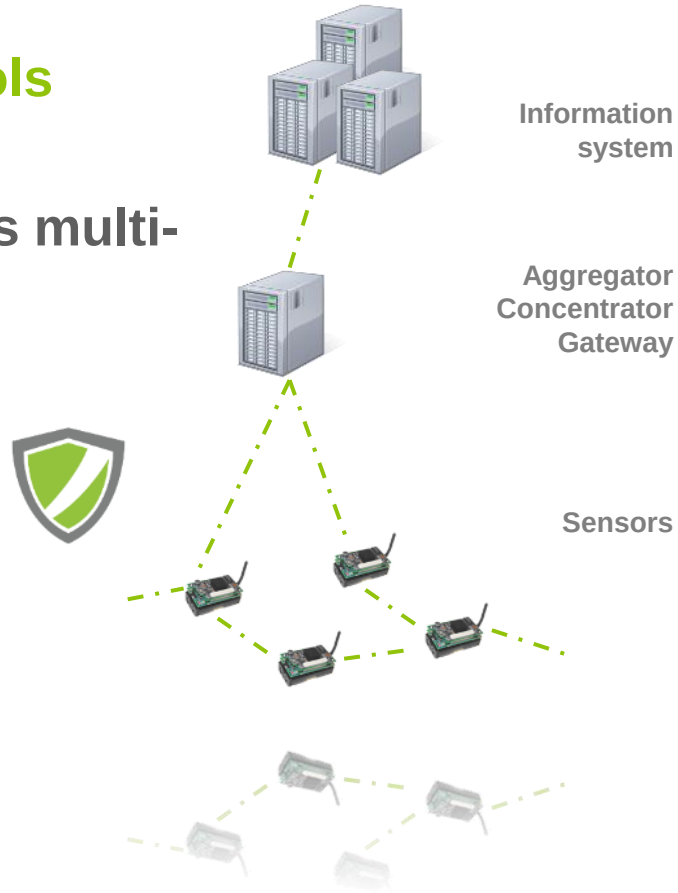
Software analysis tool reaches the highest "Ockham Criteria" for vulnerability detection

- Users
- System
- Software
- Data
- Hardware

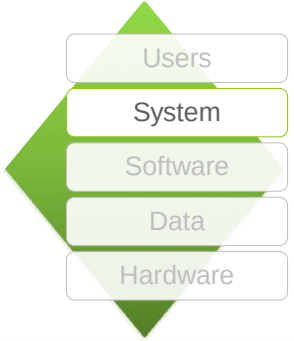
INDUSTRIAL NETWORK PROTOCOL ANALYSIS

What if we need high-integrity assessment of our network protocols?

- **Analyze threats on industrial protocols**
- **Implement attacks on wired / wireless multi-protocol industrial sensor networks**
- **Tailored tools and testbeds**
- **Propose security solutions within certification constraints**

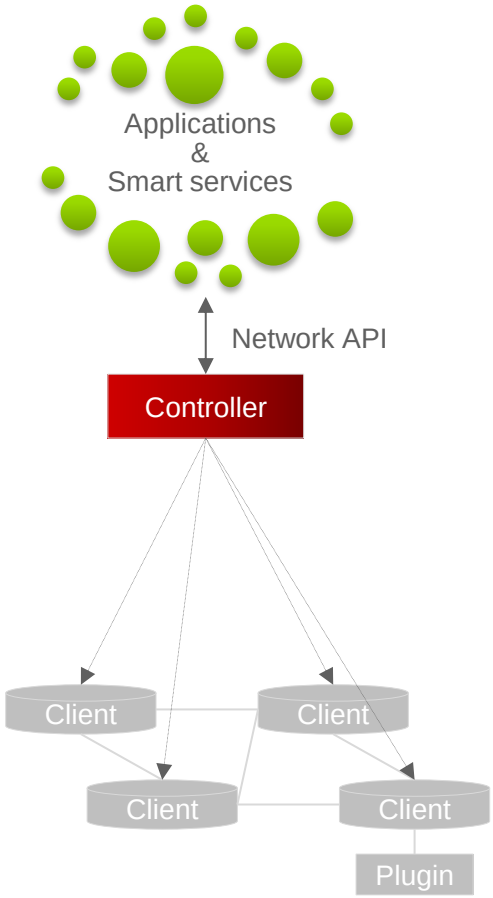


COGNITIVE NETWORK SECURITY



Reconfigure the network automatically in reaction to cyberattacks

- **The NEON platform for Software-Defined Networking**
  - Smart data routing
  - Fast infrastructure reconfiguration for new tasks
  - Fast deployment of network protocols and services
  - Intrusion detection & dynamic reconfiguration of security services
  - Mobile networking (5G)
- **Adaptative resilience to threats from inside and outside the network**
- **Blueprint for Pan-European Resilient Critical Infrastructures based on LTE Communications**



AIRBUS DEFENCE & SPACE

Countering attacks with SDN-based intrusion detection and network reconfiguration

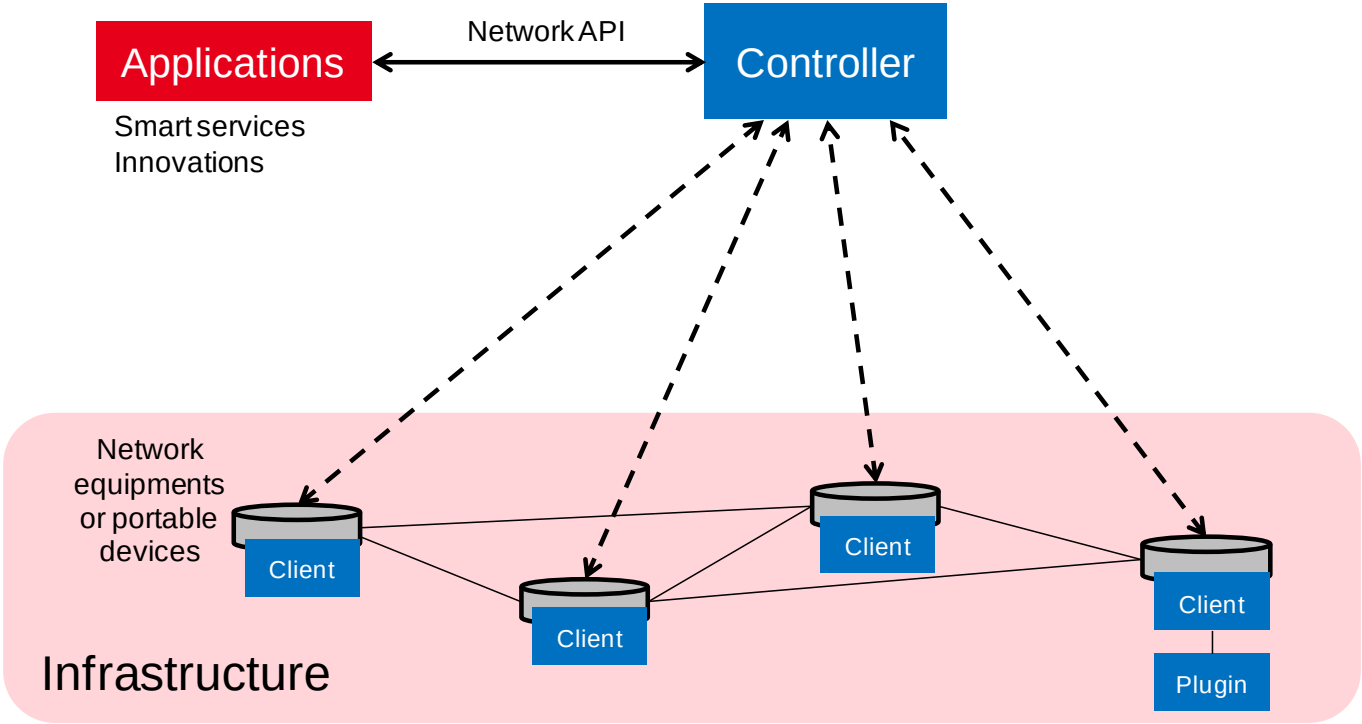
NEON ➔Trusted networks Software-Defined Networking

Software technology enabling smart management and control of network infrastructures / equipment / devices (NEON)

- Fast and easy control of **equipment / devices**, **network interfaces**, **traffic**, **network resources** and **network services**
- Interworking with **OpenFlow** protocol + **additional Southbound protocol**
- Applicable to linux-based equipment and end-terminals (e.g. Android devices)

Applications

- Smart data routing
- Fast infrastructure reconfiguration for new tasks
- Fast deployment of network protocols and services
- Security: intrusion detection & dynamic reconfiguration of security services
- Mobile networking (5G)



NETWORK SECURITY

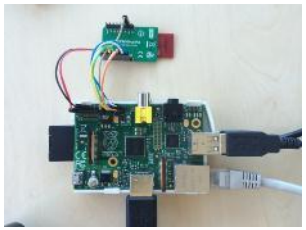
Can we ensure communications security in constrained networks?

- **Lightweight + strong IP security protocols**
  - Authentication & network access control
  - Dynamic key establishment
  - Secure software update
- **Scalable distributed IDS**
  - Lightweight data structures & footprint
  - Remote selection and configuration of monitoring nodes
- **Multi-layer security for increased robustness against attacks**

deRFmega128

deRFnode

Security software running on low-power platforms
(e.g. IEEE 802.15.4 platform from Dresden Elektronik)



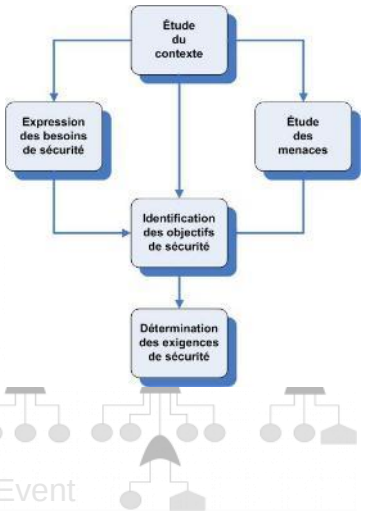
IDS software for 802.15.4 networks
(e.g. Raspberry Pi platform)

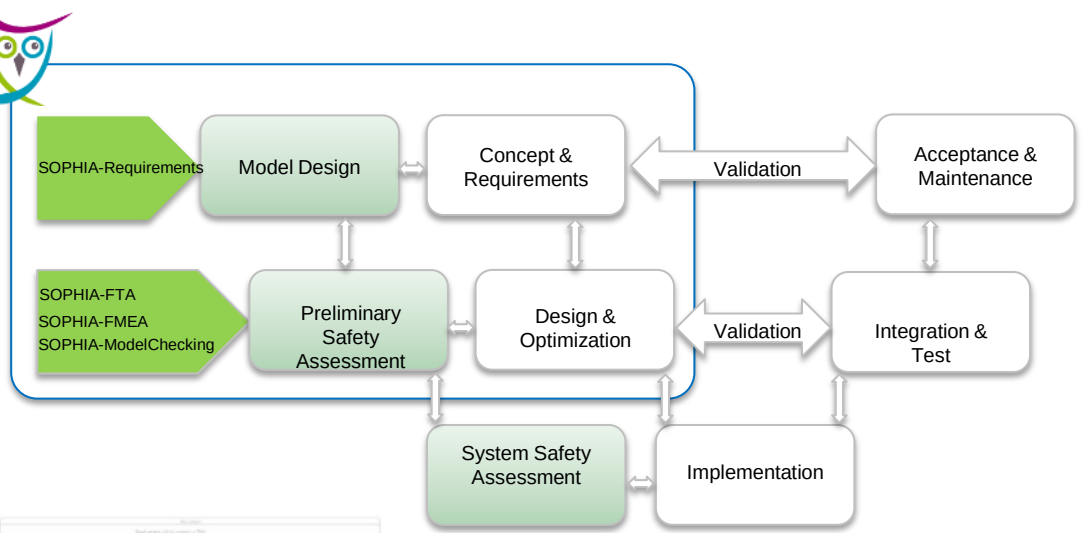
AUTOMATED RISK ANALYSIS

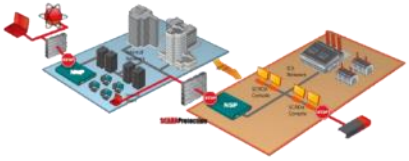
EBIOS Risk Analysis

Sophia

System Development





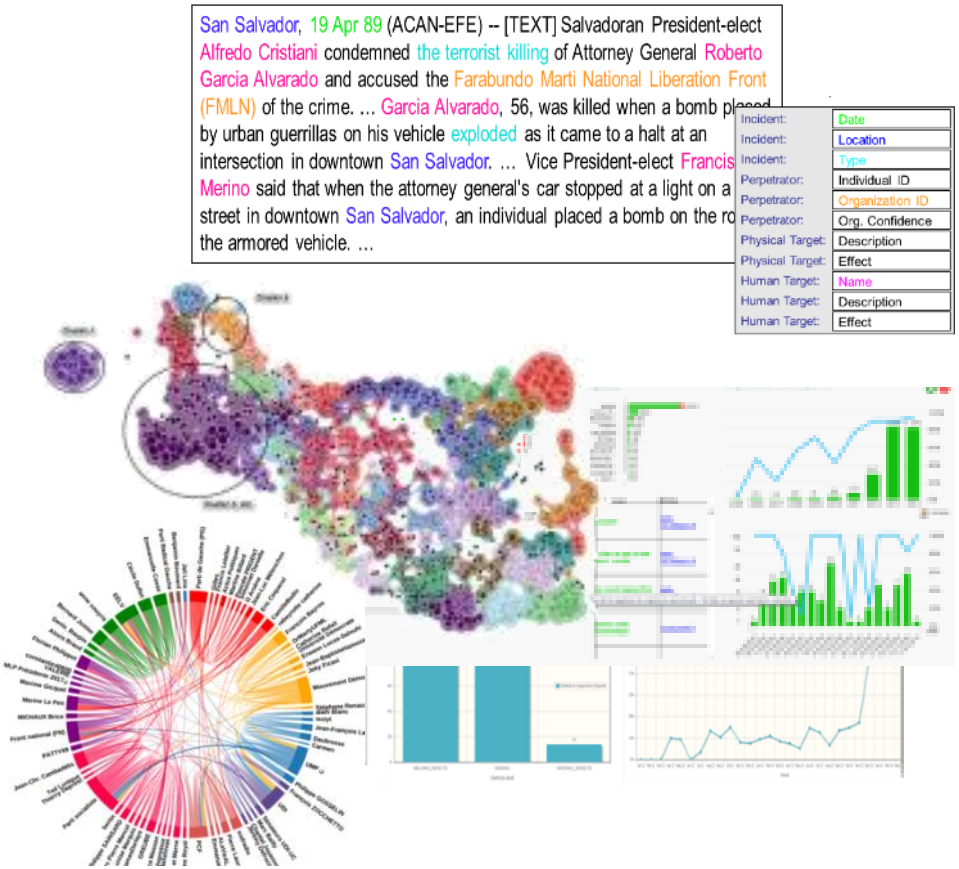


- Users
- System
- Software
- Data
- Hardware

THREAT INTELLIGENCE

Making sense of artefacts, communications, and interactions.

- **Data analysis**
  - Pattern identification
  - Traffic analysis
  - Text and picture analysis
- **Information search**
  - Multimedia, multilingual
- **Visual analytics**

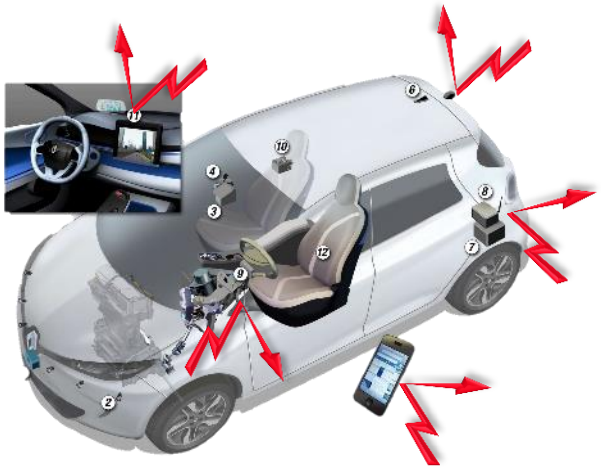


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FROM ANALYSIS TO SOLUTIONS

Users
System
Software
Data
Hardware

➢ Characterization of the Threats



➢ Evaluation / Certification

Common Criteria

MasterCard

VISA

EMVCo

ANSSI-CC-2009/25

Microcontrôleurs RISC 32-bits SAMSUNG S3FS91J / S3FS91H / S3FS91V / S3FS93I, avec SWP, Rév. 7

BSI-PP-0035

Security IC Platform Protection Profile Version 1.0 June 2007

Critères Communs version 3.1 (R3)

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Samsung Electronics Co. Ltd

Samsung Electronics Co. Ltd

CEA - LETI

CCRA

SOG-IS

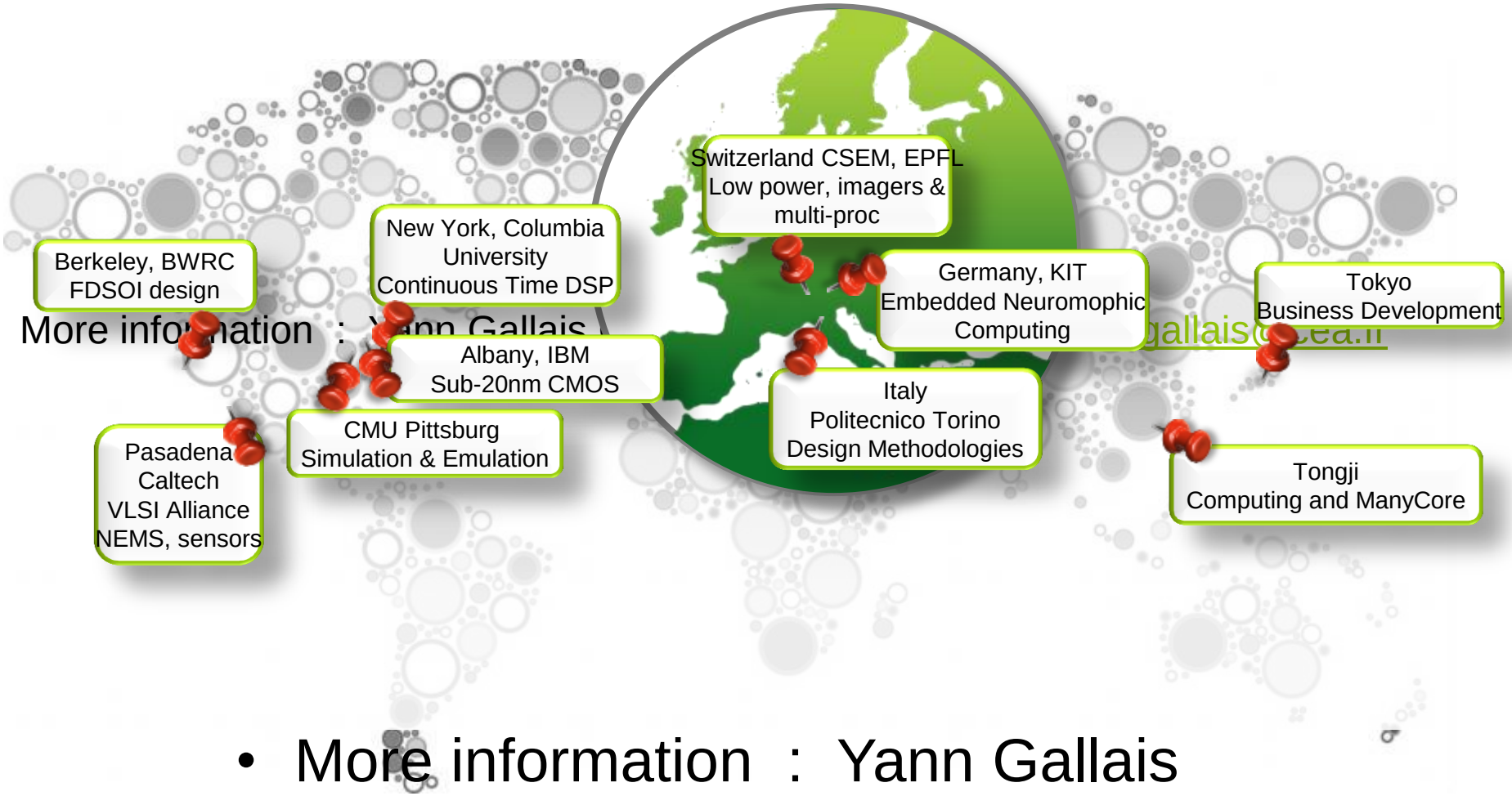
Le produit est reconnu au niveau EAL4.

➢ Improvement of security

- **At CEA Tech (LIST, LETI, DPACA), we provide tools for analysing the security issues pertaining cyber systems, whether at**
  - System's level
  - Device level
  - Component level

- **The difficulty & challenge is to build a security-coherent approach through those different tools to ensure a coherent security chain.**

WORLDWIDE RESEARCH RELATIONSHIPS



- More information : Yann Gallais
  - CEA-TECH Japan Office
    - Yann.gallais@cea.fr


Thank for your attention