# IoT Security Services

## Create Value with Security by Design and Security Lifecycle Management

**Yan-Tarō CLOCHARD, CMO & North Asia Sales VP**

SECURE-IC
THE SECURITY SCIENCE COMPANY

# SPEAKER PRESENTATION

- **Yan-Tarō CLOCHARD**
  **Chief Marketing Officer and Vice-President of Sales North Asia**

- Yan-Tarō Clochard was appointed Chief Marketing Officer at Secure-IC. He is also VP of Sales North Asia and founder of Secure-IC Japan.
- He formerly was developing bilateral Technology cooperation (cyber, 5G, AI, etc.) at the French Embassy in Japan. He previously worked in the telecommunication industry. He graduated in Electronics Engineering from ENSEA and Business from ESSEC Business School (France/Singapore)

# AGENDA

1. Secure-IC company profile
2. Security by design and security lifecycle issues
3. Security Evaluation as a Service
4. Lifecycle Security Management Services
5. Key takeaways

# 1. COMPANY PROFILE

# OUR ROOT OF TRUST

**THE ORIGINS**
15+ years of Embedded systems security research at Telecom Paris

**FOUNDED 2010**
Spin-off from Telecom Paris and HQ in Rennes (FR)

**FIRST KEY RESULTS**
- 1st certified product in 2012 (Common Criteria)
- 1st million chip deployed in 2015

**LAUNCHING OF THE SECURITY SCIENCE FACTORY**
4 research centers in France, Singapore and Japan

**COMPLETE PORTFOLIO OF SOLUTIONS**
Backed with more than 40 families of international patents

**THOUGHT LEADERSHIP IN THE SECURITY WORLD**
- ISO committees membership
- 3 world-renowned scientific advisors
- 200+ publications

**10 YEARS IN BUSINESS IN 2020**

**RISING INDUSTRY LEADER**
- 1 Billion+ IP per quarter
- 100+ customers worldwide
- Silicon Proven TSMC, GF, Samsung, SMIC, HH GRACE, ST, UMC, MAGNACHIPS
- 130nm, 65nm, 55nm, 40nm, 28nm, 16nm, 12nm, 10nm, 7nm, 5nm
- 100+ people

# THE RISING LEADER IN EMBEDDED SECURITY

**After 10 years of sustained and controlled growth on equity,**
**Secure-IC announced on January 20th, 2022, a 1st capital raise of 20 million euros**

**+€20M**

Accelerate our organic **GROWTH WORLDWIDE**

Support an ambitious **RECRUITMENT PLAN**

*"The **highest 1st fundraising** for the French cyber industry over 2021!"*

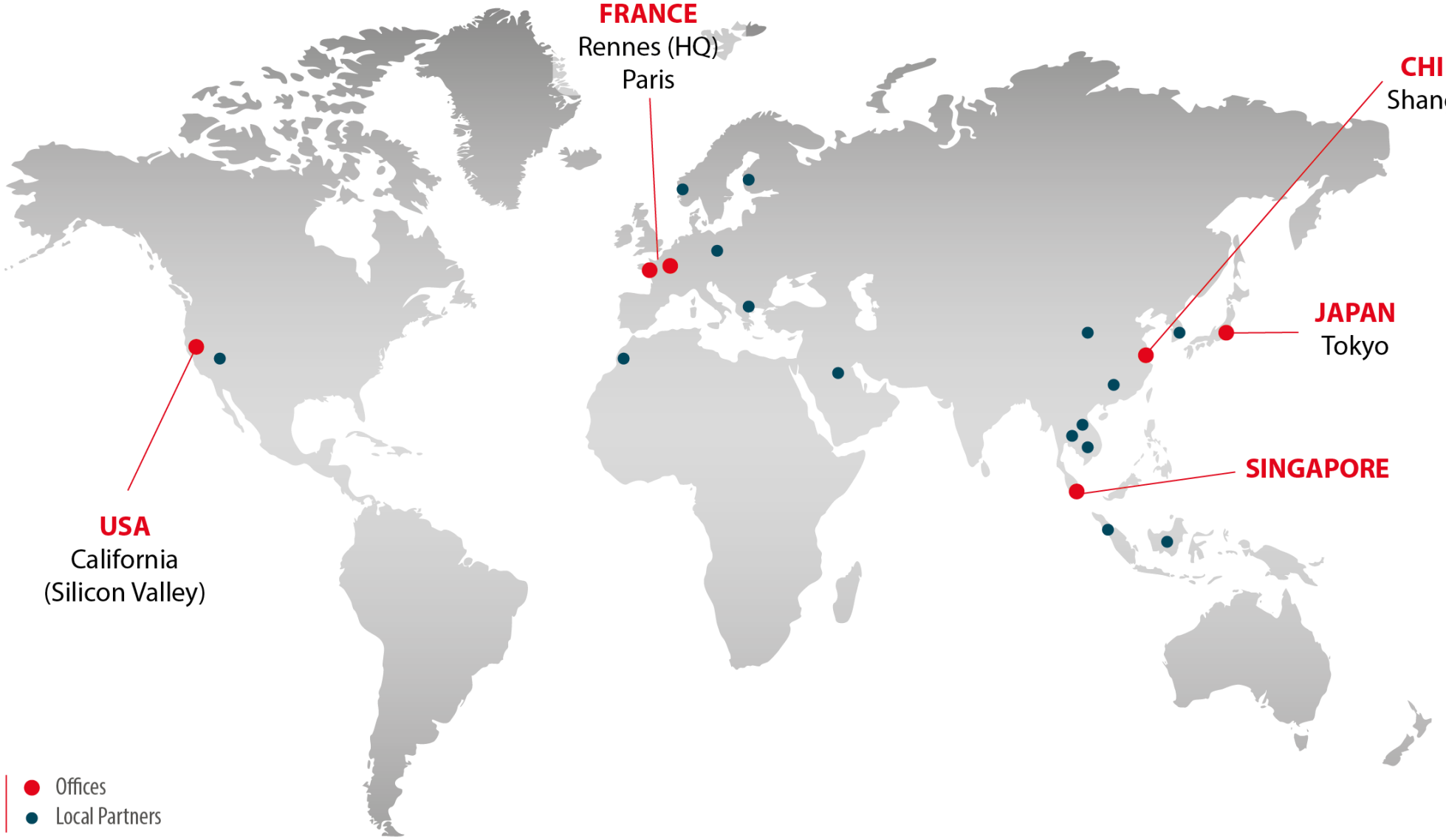
With the support of Alliance Entreprendre, GO Capital and BNP Paribas Développement

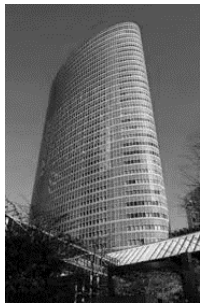
Carry out **EXTERNAL GROWTH** operations

Implement our **CHIP TO CLOUD** vision

**+50** hirings in 2022

# A GLOBAL COMPANY



6 offices worldwide

16 local partners

4 research centers

20 countries

5 continents

# SECURITY TECHNOLOGIES FOR EMBEDDED SYSTEMS

## FOR WHICH MARKETS?


## WITH WHAT PRODUCTS?

### PROTECT with SECURYZR™

- integrated Secure Element
- Security IP
- Software solutions
- integrated Security Service Platform

### EVALUATE with LABORYZR™

- End-to-end evaluation platforms for HW and SW

### SERVICE & CERTIFY with EXPERTYZR™

- Support from experts to reach security goals
- Security innovation

# OUR 3 PRODUCT LINES

## A PROGRESSIVE PATH THAT BRINGS OUR CUSTOMERS FROM SECURITY REQUIREMENTS TO CERTIFIED SOLUTIONS

**PROTECT** with SECURYZR™

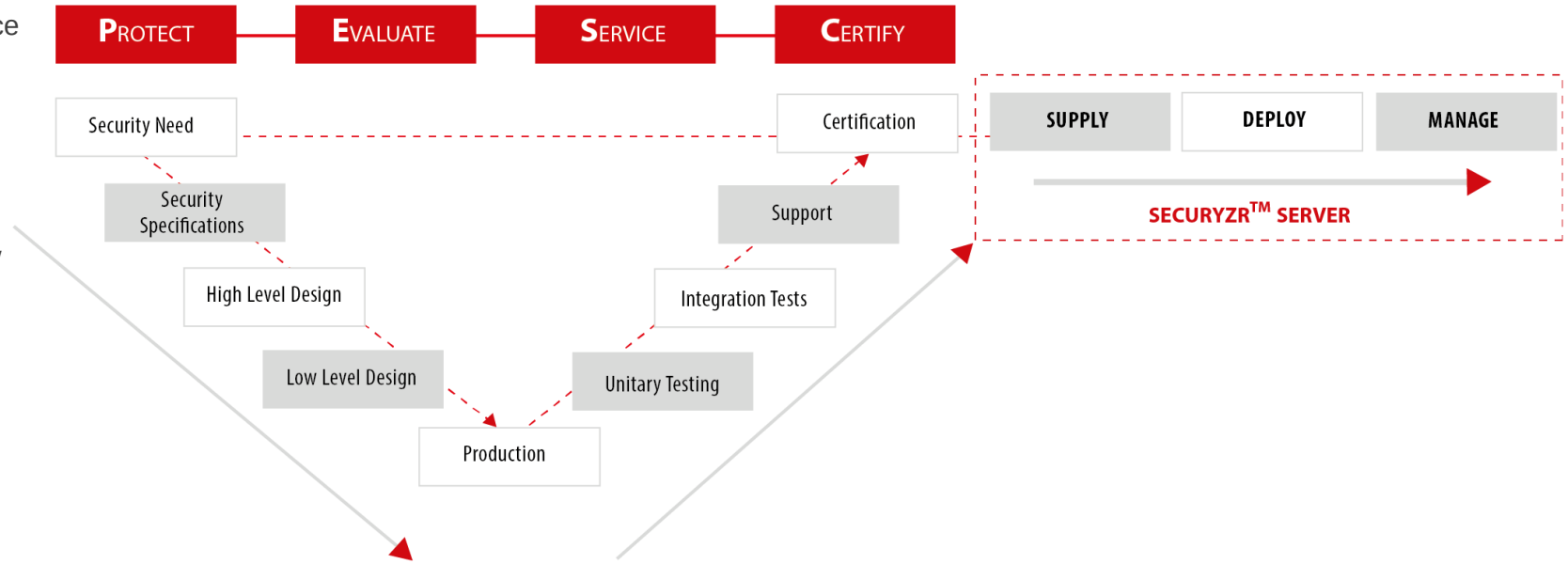
integrated Secure Element,
Security IP
Software solutions
integrated Security Service Platform

**EVALUATE** with LABORYZR™

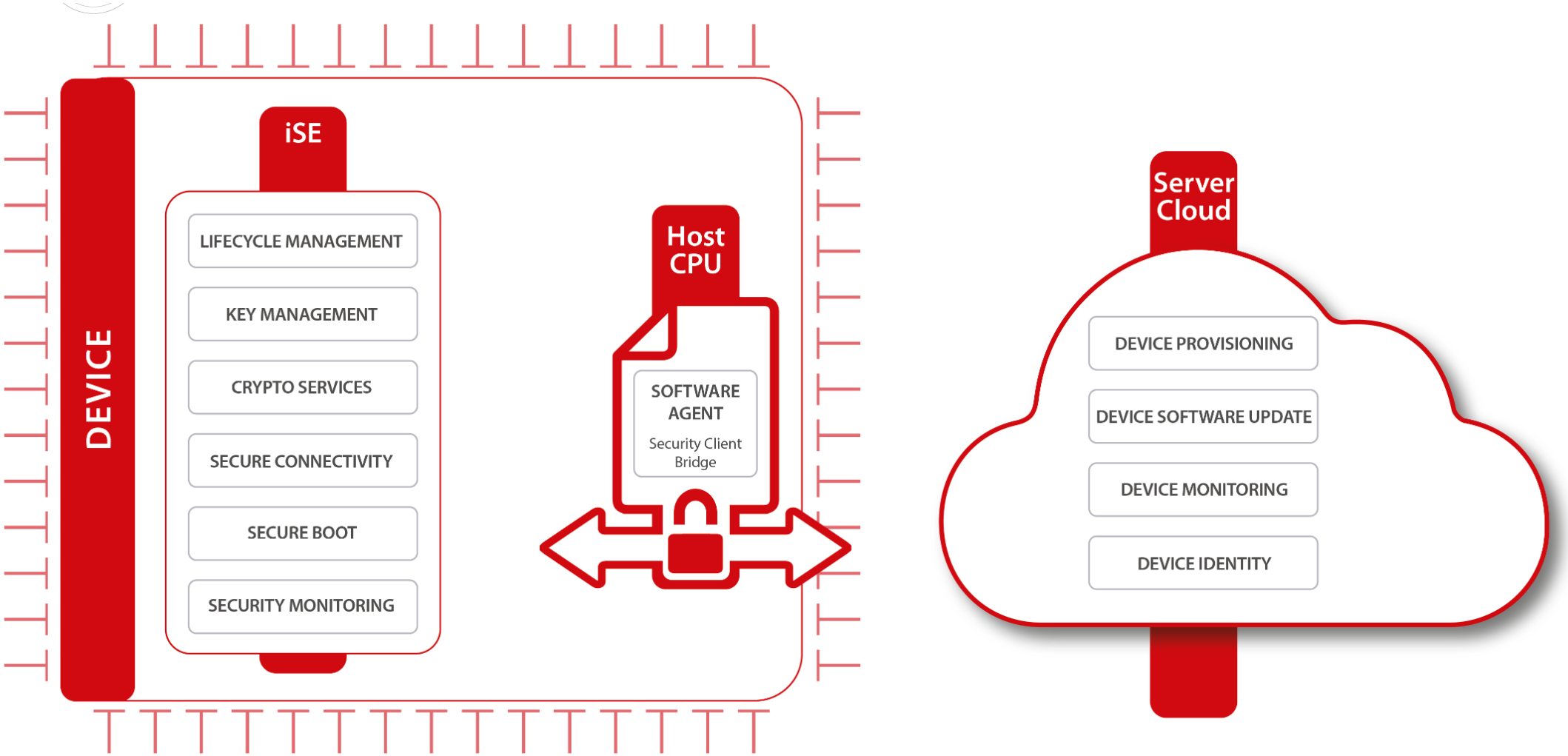
End-to-end evaluation platforms for HW and SW

**SERVICE & CERTIFY** with EXPERTYZR™

Support from experts to reach security goals
Security innovation



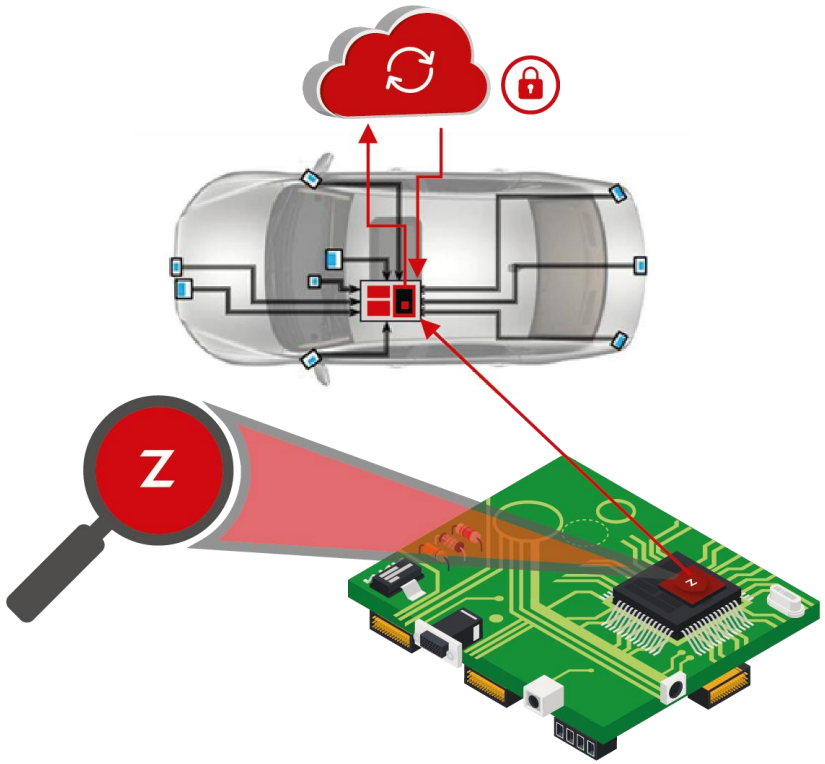
# SECURYZR iNTEGRATED SECURITY SERVICES PLAFTORM (iSSP)



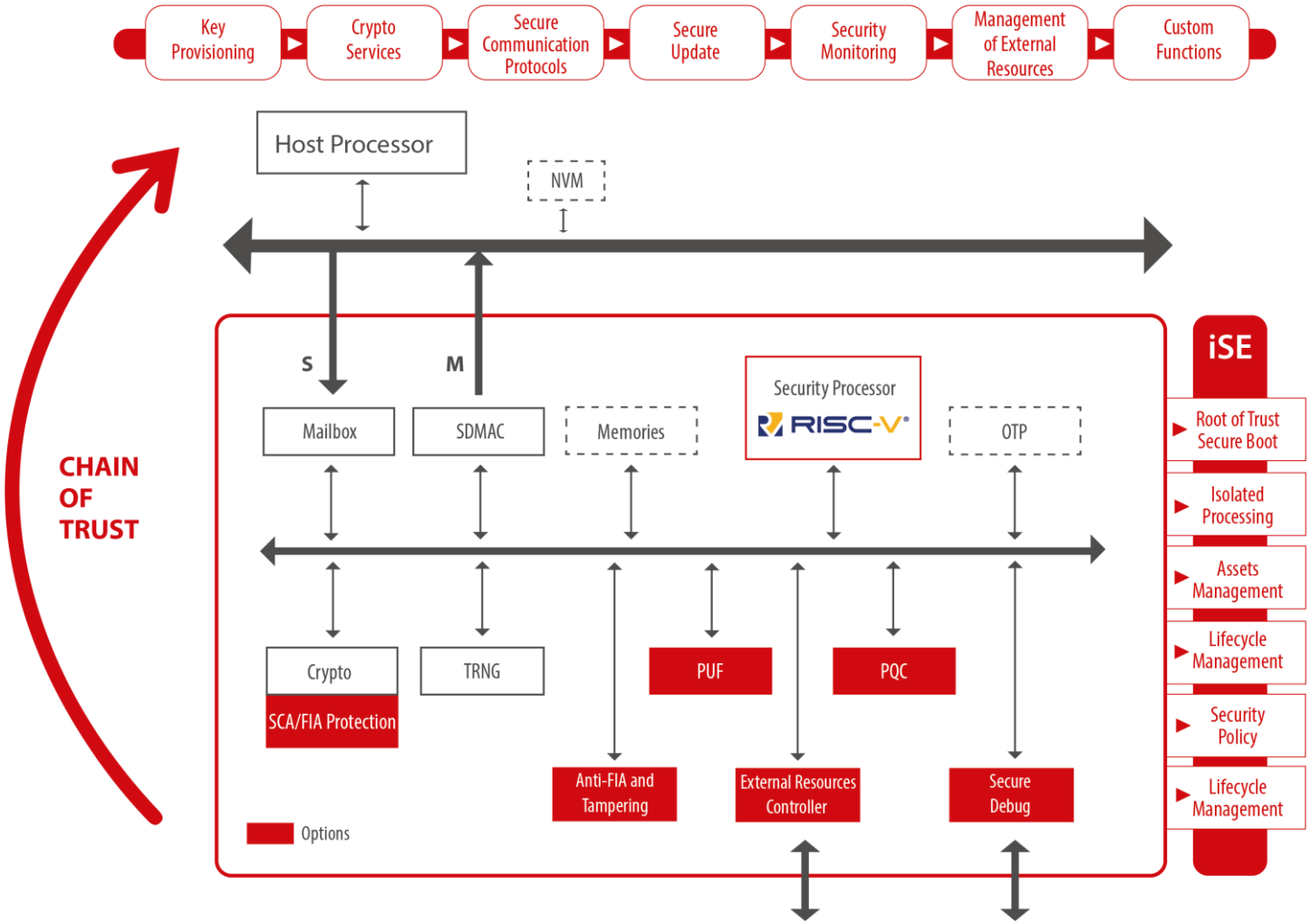
# SECURYZR iNTEGRATED SECURE ELEMENTS (iSE)

SECURYZR™

- Certification ready
- Fully digital protections
- Laboryzr proven
- Flexible architecture and interfaces
- Balancing of hardware and software part available
- Hardware based isolation
- Rich software service platform from chip to cloud
  - Securyzr firmware
  - Securyzr server



# SECURYZR iSE




| SECURYZR™ | | PERSONALIZATION |
|---|---|---|
| **Automotive** | Safety/Security: ISO 26262 up to ASIL D & Security EVITA Full, Medium, Light, CC PPV2X, etc. | |
| **IoT/OT** | Lightweight: Low area, low footprint<br>Industrial Automation: IEC 62443 | |
| **AI** | Protect your Data & Know-How | |
| **DRM** | Nagra, Verimatrix, China DRM, etc. compliant | |
| **iUICC** | iSIM, GSMA compliant | |
| **HDD** | FDE TCG Opal, Printer | |
| **High performance** | High speed operations for cloud computing, blockchain, etc. | |
| **Critical security** | Highest security certification levels: FIPS 140-2/3, Common Criteria, OSCCA, K/JCMVP, etc.),<br>protection of critical data, against reverse-engineering | |
| TAILORED SECURYZR™ | | |

SECURE-IC
THE SECURITY SCIENCE COMPANY

# IP PORTFOLIO

| | | |
|---|---|---|
| CRYPTO | SIDE-CHANNEL ATTACKS | TUNABLE CRYPTO |
| | ATTACKS ON SOFTWARE | SW CRYPTO LIBRARY |
| | HARMONIC EM ATTACKS | DIGITAL TRNG |
| ROOT OF TRUST | CLONING, COUNTERFEITING | PHYSICALLY UNCLONABLE FUNCTION (PUF) |
| | FIRMWARE TAMPERING | BOOT PROTECTION PACK |
| | REVERSE ENGINEERING | CAMOGATES |
| | JTAG VIOLATION | SECURE DEBUG |
| TAMPERING ATTACKS | FAULT INJECTION ATTACKS | DIGITAL SENSOR |
| | INVASIVE HARDWARE MODIFICATIONS | ACTIVE SHIELD |
| | EAVESDROPPING | SCRAMBLED BUS |
| | SYNCHRONIZED ATTACKS | SECURE CLOCK |
| MEMORY PROTECTION | ROWHAMMER ATTACKS | ANTI ROW-HAMMER |
| | MEMORY ATTACKS | MEMORY CIPHERING |
| AI FOR SECURITY | ADVANCED ATTACKS | SMART MONITOR |
| PROCESSOR SECURITY | CYBER ATTACKS | CYBER ESCORT UNIT |

# SECURE-IC, A PIONEER IN POST-QUANTUM CRYPTOGRAPHY

- Already existing own secure PQC implementations (SW/HW) and security analysis of NIST candidates
- Multiple projects awards and projects in PQC (France, Singapore, Japan, etc.)
- Led the French PQC ecosystem (including PQ transition: TLS, Secure boot, etc. and NIST PQC competition support – RISQ project)
- Multiple scientific papers and presentations in worldwide conferences


https://hub.secure-ic.com/pqc-issp
https://hub.secure-ic.com/pqc-webinar

- Several patent applications

RISQ

Regroupement de l'Industrie française pour la Sécurité Post – Quantique

Industry | Certification Body | Academia

+ External Partners:

BRAINE

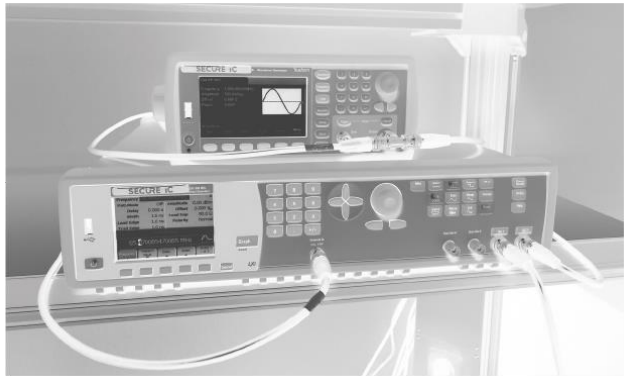
https://www.braine-project.eu/

ARCHI-SEC

https://archi-sec.telecom-paristech.fr/

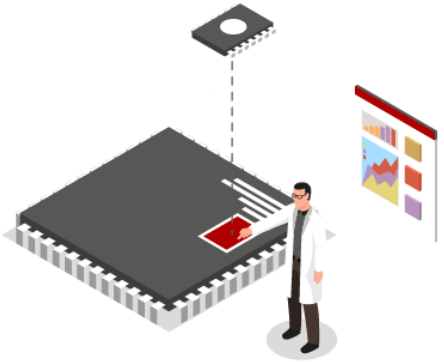
Maya project

# ADVANCED PLATFORMS FOR HW & SW SECURITY EVALUATION



## FOR DESIGNERS

- An end-to-end lifecycle security assessment: from the roots (design/code) to the certification
- Implement seamlessly a ‘Design for Security’ methodology in the design flow by testing against vulnerability and weaknesses from an early stage
- ‘In-depth Security’ testing for SW and HW
- Allows non-specialized people to assess security solutions, identify problems, and helps to improve code security



## FOR SECURITY TESTING LABORATORIES

- Build your lab to evaluate your security-based solution and be compliant to any Security certification level (FIPS, Common Criteria, etc.)
- Test your device against Hardware Trojans and Black Box analysis / Reverse Engineering

SECURE-IC
THE SECURITY SCIENCE COMPANY

# 3 TOOLS FOR LIFECYCLE SECURITY EVALUATION

LABORYZR™

DESIGN LIFE CYCLE

- **DEVICE** LAYER
- **SOFTWARE** LAYER
- **HARDWARE** LAYER

ANALYZR™

CATALYZR™


VIRTUALYZR™

- **REAL DEVICE** EVALUATION
- **SOFTWARE** VERIFICATION
- **PRE-SILICON** VERIFICATION

SECURITY LIFE CYCLE

# A WORLD OF EXPERTISE

EVALUATION AS A SERVICE

SUPPORT TO CERTIFICATION

SECURITY TRAINING

EMBEDDED SECURITY WATCH

EXPERTYZR™

## THE SECURITY SCIENCE FACTORY (SSF)

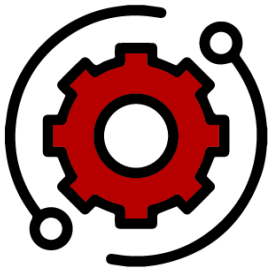
- Advanced R&D
- Advanced projects & problem solving
- Thought leadership
  - Legacy series events worldwide
  - Scientific work & publications
  - Standardization

# THE SECURITY SCIENCE FACTORY (SSF)

- **ADVANCED TECHNOLOGIES**
  - Innovating on the security technologies of future and sharing innovation with customers

- **ADVANCED RESEARCH**
  - Joint research on cutting-edge topics
  - Snapshot of research axes: Post-Quantum Cryptography, Hardware Trojan detection, AI in connected security and more

- **THOUGHT LEADERSHIP**
  - Legacy series events worldwide
  - Scientific work and publications
  - Standardization



- **SECURE-IC LEGACY SERIES**
  - Embedded Cybersecurity Forum
  - Attracting industry advocates globally

- **RESEARCH & PUBLICATIONS**
  - More than 200 publications

- **STANDARDIZATION**
  - Non-invasive attacks: ISO/IEC 20085
  - Physically Unclonable: ISO/IEC 20897
  - White-Box Crypto: SC27/WG3 N1367
  - Connected Car: ISO/SAE 21434
  - Autonomous Vehicle: AVWG 3
  - Hardware Trojan: ISO SC27/WG3 SP

# Secure-IC’s Projects References

- Securyzr for Industry

- Project application: Factory Automation
- Techno: TSMC 28nm
- Region: North Asia
- Period: 2020

- **Technical scope delivered:**
  - Secure Boot with Symmetric and Asymmetric crypto
  - Use of mask ROM
  - Both international and Chinese algorithms

# Secure-IC’s Projects References

- Securyzr for Industry

- Project application: AI sensor (vision, sound, motion)
- Techno: GF 22nm FDx
- Region: EMEA
- Period: 2020

- **Technical scope delivered:**
  - Goal: Protect the IP of the customer system
  - PUF for ID and key management
  - SCA protections for all crypto
  - Security audit of all SCZ before manufacture

# Secure-IC’s Projects References

- Securyzr for Server

- Project application: Server
- Techno: TSMC 22nm
- Region: EMEA
- Period: 2020

- **Technical scope delivered:**
  - Wide Crypto services (with Crypto IP optimized for Xilinx FPGA)
  - SCA protection (Compliant to CC EAL5+)
  - FIA protection (Digital Sensor, Active Shield)
  - PUF for key management

# Secure-IC’s Projects References

- Securyzr for 5G

- Project application: 5G/4G Communication
- Techno: TSMC 12nm
- Region: EMEA
- Period: 2021

- **Technical scope delivered:**
  - Securyzr iSE & Host Secure Boot using asymmetric cryptography
  - Cryptographic operation for TLS (1.2 and 1.3) and IPSec
  - Cryptographic engines protected against SCA
  - OpenSSL connected to the Securyzr using PKCS #11

# Secure-IC's Projects References

- Securyzr for Multi-Function Printer

- Market: MFP Cartridge
- Techno: TSMC 40nm
- Region: North Asia
- Period: 2019

- **Technical scope delivered:**
  - Anti-counterfeiting features:
    - Logic-lock
    - Camo-gates
    - PUF
    - Custom Crypto (impossible to emulate)
  - Strong one-way authentication
  - Delegate key generation and programmation by semiconductor company and/or customers
  - Ability to change architecture for each tape out
  - Maintenance after IC break

# SECURE-IC'S AUTOMOTIVE PROJECTS 20+ PROJECTS

| APPLICATION | SOLUTION | SCA PROTECTION | ANTI-TAMPER PROTECTION | PUF | CERTIFICATION | AREA |
|---|---|---|---|---|---|---|
| **V2X** | Securyzr™ | Yes | Yes | No | FIPS-140-3, OSCCA, CC, ISO26262 ASIL B | EMEA |
| **INFOTAINMENT** | Securyzr™ | Yes | Yes | Yes | FIPS-140-3, ISO21434 | North Asia |
| **ADAS (RADAR, LIDAR, ETC.)** | Securyzr™ | Yes | Yes | Yes | FIPS-140-3, OSCCA, CC, ISO21434 | USA |
| **GATEWAY** | Securyzr™ | Yes | Yes | No | FIPS-140-3, ISO21434, ISO26262 ASIL B | North Asia |
| **TELEMATICS TCU** | IPs | Yes | N/A | N/A | FIPS-140-2/140-3 | North Asia |
| **BCM** | Securyzr™ | Yes | Yes | No | OSCCA, ISO26262 ASIL D, ISO21434 | China |
| **POWERTRAIN** | Securyzr™ | Yes | Yes | Yes | ISO26262 ASIL D, FIPS-140-2/3, ISO21434 | EMEA |

# 2. SECURITY BY DESIGN AND SECURITY LIFECYCLE ISSUES

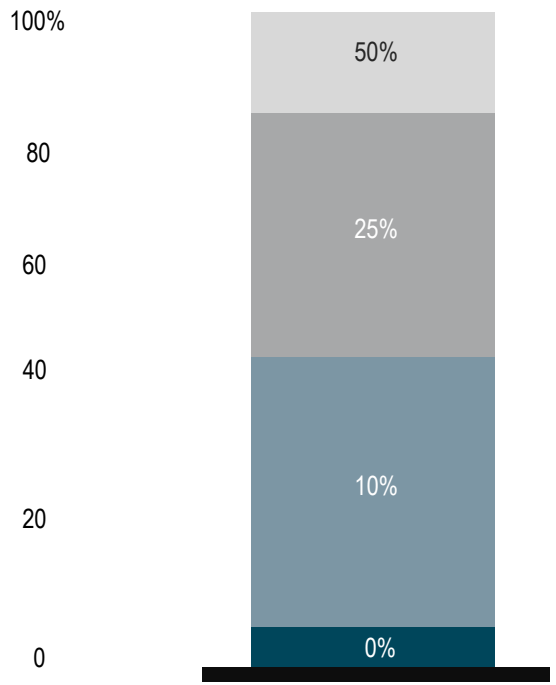
# SECURITY FROM THE FOUNDATION

## Security is the first key challenge for IoT

| | | Automotive | Industrial | Smart homes and buildings |
|---|---|---|---|---|
| Software infrastructure and apps | Applications | 2 | 2 | 2 |
| | Software infrastructure | 1 | 2 | 3 |
| Connectivity | Gateway | 1 | 3 | 2 |
| | Communications protocol | 1 | 3 | 2 |
| Hardware | End point | 1 | 1 | 1 |
| | Chip level | 2 | 2 | 1 |

Insecure | 1 | 2 | 3 | Extremely secure

## Customers would pay an average of 22% more for secure IoT devices




Sources: McKinsey/GSA Semiconductor Industry Executive Survey 2017 (table) & Bain IoT enterprise cybersecurity survey

# DESIGN FOR SECURITY

## Design for Security can be seen as Design Thinking applied to Security


Design thinking

Security

Design for Security

**BEFORE THE DESIGN**

* Identification of goods
* Threats
* Protections
* Mapping
* Development plan

**DURING THE DESIGN**

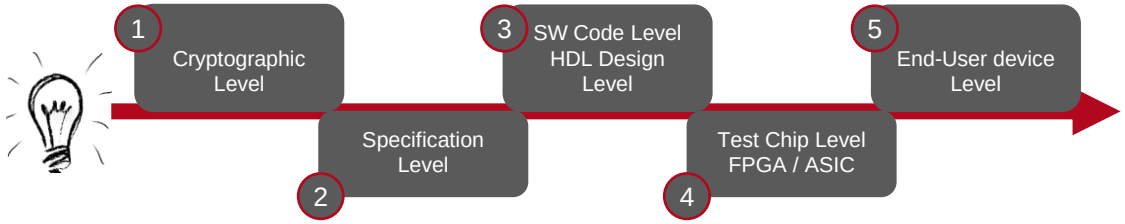
* Specifications Review
* Code Review
* Analysis of Threats
* Quotation of Attacks

**AFTER THE DESIGN**

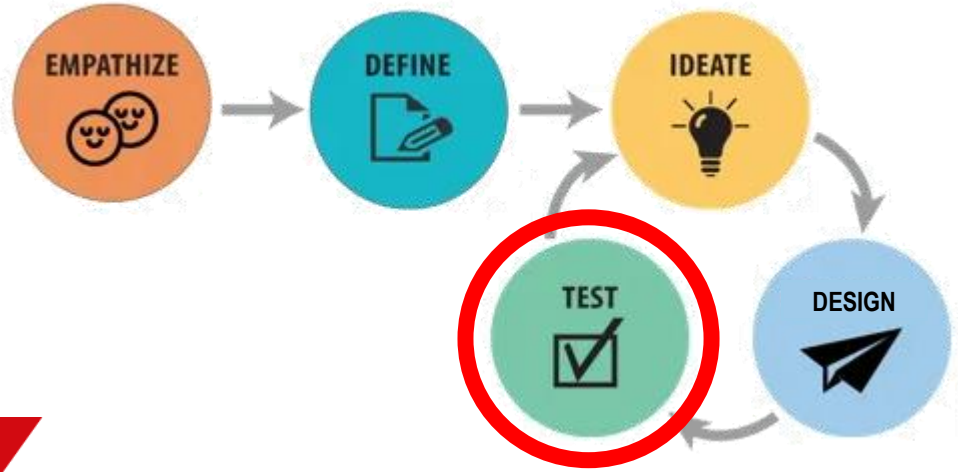
* Test Plan
* Assistance to Certification
* Help for Documentation
* Design of Patches

# SECURITY EVALUATION at every level

## Security testing throughout the development cycle

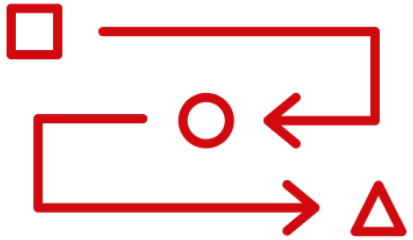


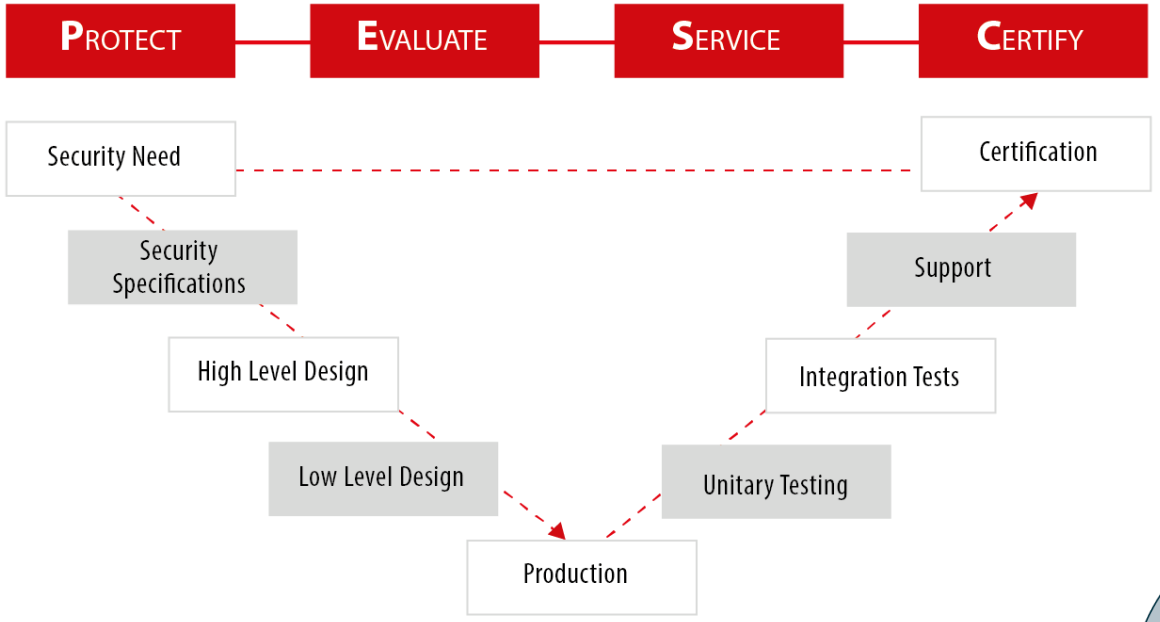

✓ Security at every development-cycle step




| EVALUATION LEVELS | SECURE-IC TEAMS & SKILLS | SECURE-IC TOOLS |
|---|---|---|
| Algorithmic level | Cryptography team | Expertyzr™ |
| Architecture level | Security architects team | Expertyzr™ |
| HDL Design Level | Pre-Silicon Evaluators | Virtualyzr™<br>Pre-Silicon Evaluation |
| SW layer level | SW Layer Evaluators | Catalyzr™<br>Software Evaluation |
| Test Chip level | White-box Evaluators | Analyzr™<br>Post-Silicon Evaluation |
| End-User device level | Black-box Evaluators | Analyzr™<br>Post-Silicon Evaluation |

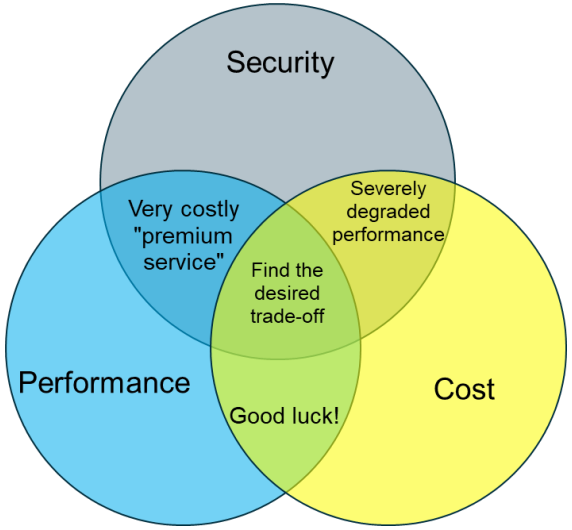
# Overview of the security development






**Methodology steps:**

- Define a sensitive asset
- Threats, weaknesses & vulnerability
- Build a secure architecture
- Populate architecture with security functions
- Perform Gap Analysis and iterate if necessary
- Verify and Evaluate the Security
- Up to certification
- Trade-off: Security vs cost vs performance



# THE PESC APPROACH

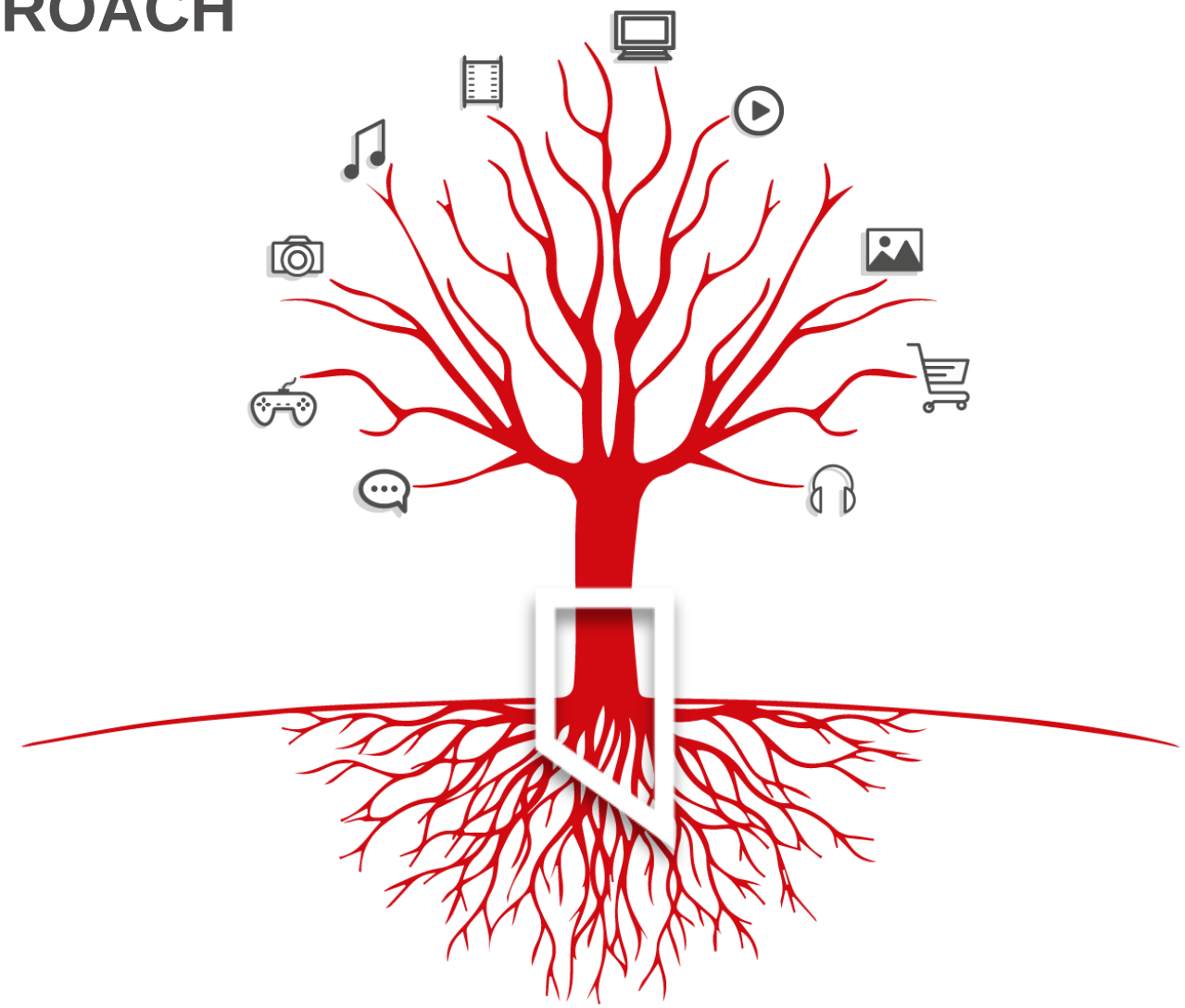
**P**ROTECT

**E**VALUATE

**S**ERVICE &

**C**ERTIFY

THE REAL PROTECTION IS WHEN SECURITY IS DESIGNED FROM THE **FOUNDATION**



**ROOT OF TRUST**

SECURITY IN DEPTH BY DESIGN

# CHALLENGES AT STAKE

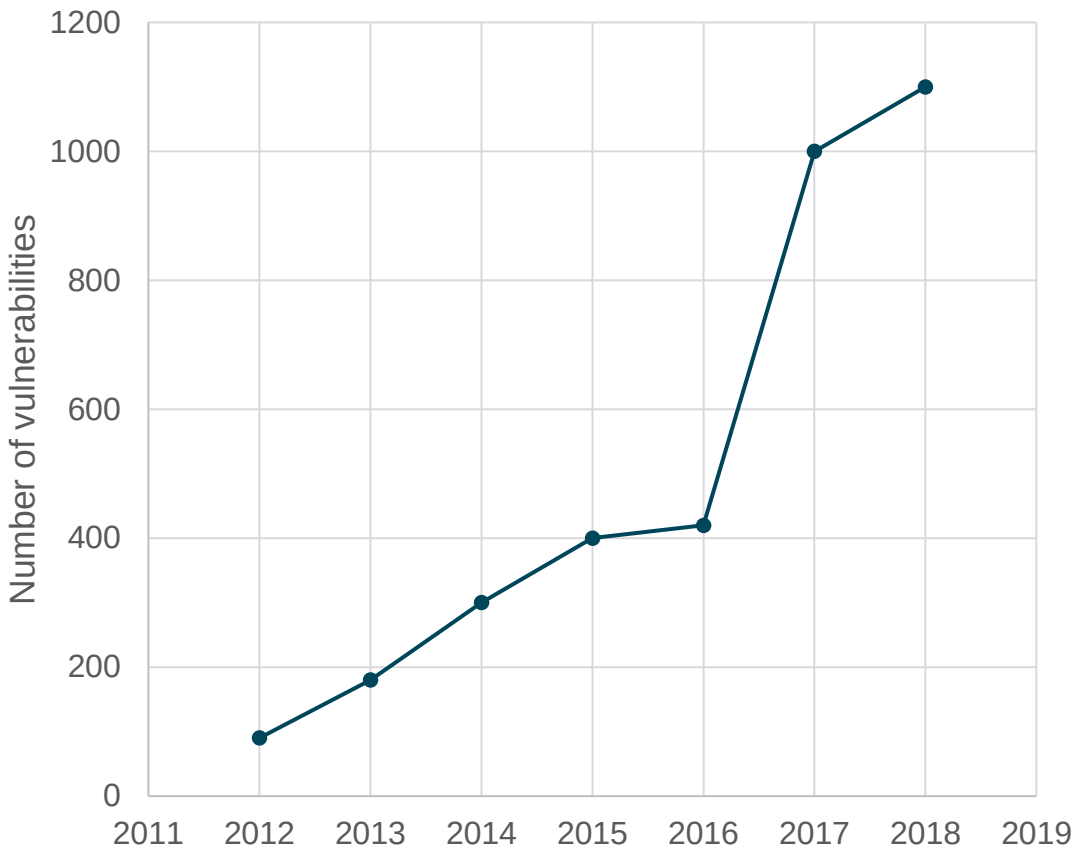
60%

of breaches are linked to a vulnerability where a patch was available, but not applied.

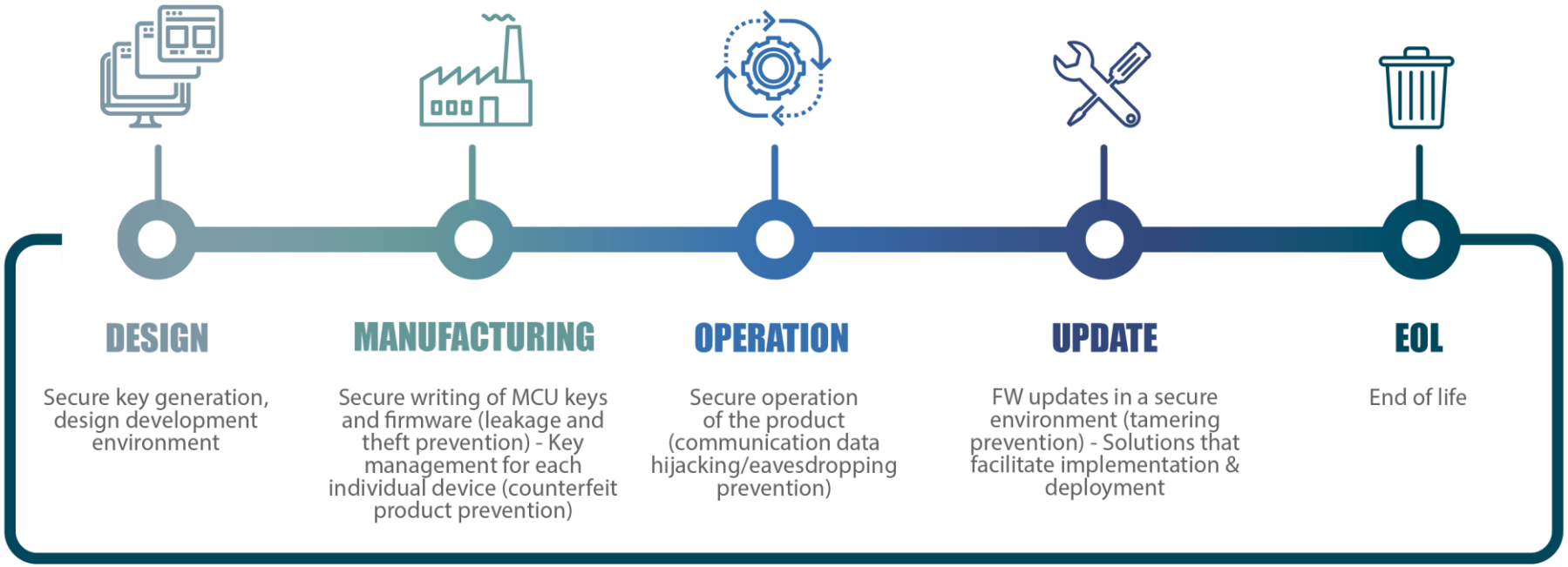
31%

of cyber attacks are due to unsecured communication protocols.

## Increasing number of device vulnerabilities over time



# TRUSTED DATA AS A SOVEREIGNTY CHALLENGE




- Considering the complexity of value chains, the **challenge is to generate and manage trust in data**.
- Secure-IC aims at answering this challenge **relying on interoperability and open standards**.

**WHAT MATTERS FOR SOVEREIGNTY IS THE TRANSPARENCY IN HOW TO EVALUATE & MAINTAIN THAT TRUST THROUGHOUT THE WHOLE PRODUCT LIFE CYCLE.**

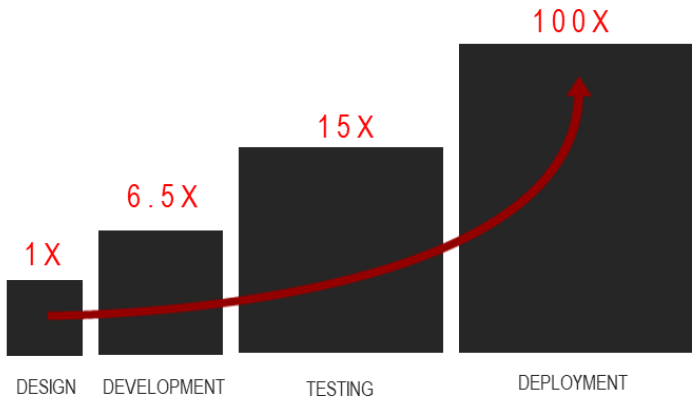
# 3. SECURITY EVALUATION AS A SERVICE

# THREAT ANALYSIS

**Because taking the right security threats into account from the beginning implies huge savings**

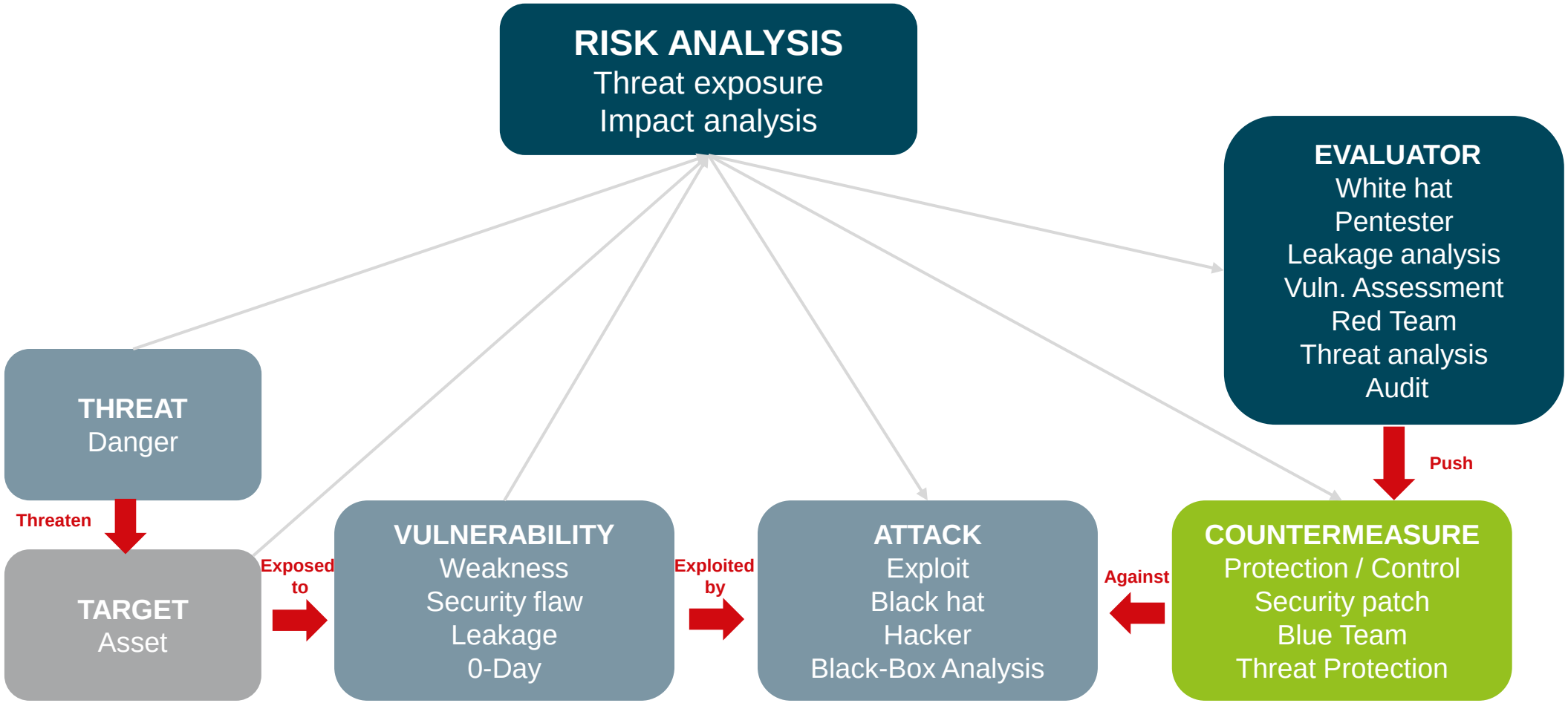
- Reduce costs by early definition of the security needs
- Perfect fit of Security configuration to your project
- We adapt to different threat analysis standard workflows

➢ Reduced development time and costs savings




Costs to fix defects when security was not embedded from the beginning

# OVERVIEW OF RISK ANALYSIS ITEMS



# THREAT ANALYSIS RISK ASSESSMENT (TARA)
# A methodic and standardized APPROACH

ISO/IEC JTC 1/SC 27/WG 3 **N1652**

REPLACES:

ISO/IEC JTC 1/SC 27/WG 3

Information technology - Security techniques - Security evaluation, testing and specification

Convenorship: AENOR, Spain, Vice-convenorship: JISC, Japan

**DOC TYPE:** working draft

**TITLE:** CD Text for ISO SAE 21434 — Road vehicles — Cybersecurity engineering

**SOURCE:** ISO TC 22/SC 32/WG 11

NIST Special Publication 800-30
Revision 1

Guide for Conducting
Risk Assessments

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

**J3061.**

The Guide For Cyberphysical Systems

**ISO/SAE 21434.**

Road vehicles — Cybersecurity engineering

# Most recurrent threats to address

**Feedback from 10 years of security projects at Secure-IC shows that some threats are most often among the top concerns in the results of the threat assessment & risk analysis.**

**Most often addressed threats:**

- Assets and private data stealing
- Firmware extraction, counterfeiting or copying
- Firmware modification and reinjection, device rooting
- Key recovery through Side-Channel Analysis
- Master key extraction for high replicability attacks
- Lifecycle alteration for privilege escalation (returning to factory mode, etc.)

- We design Securyzr™ as a baseline security to address all those recurring threats at once with a single integrated Secure Element (iSE) off-the-shelf.

# SERVICE – THE SECURITY SCIENCE EXPERTISE

EVALUATION AS A SERVICE

SUPPORT TO CERTIFICATION

SECURITY TRAINING

EMBEDDED SECURITY WATCH

EXPERTYZR

## THE SECURITY SCIENCE FACTORY (SSF)

- Advanced R&D
- Advanced projects & problem solving
- Thought leadership
  - Legacy series events worldwide
  - Scientific work & publications
  - Standardization

# SECURITY EVALUATION for audit, analysis & benchmarking

SECURE-IC
THE SECURITY SCIENCE COMPANY

EXPERTYZR™

LABORYZR

## SECURITY EVALUATION

CATALYZR
Software Evaluation

VIRTUALYZR
Pre-Silicon Evaluation

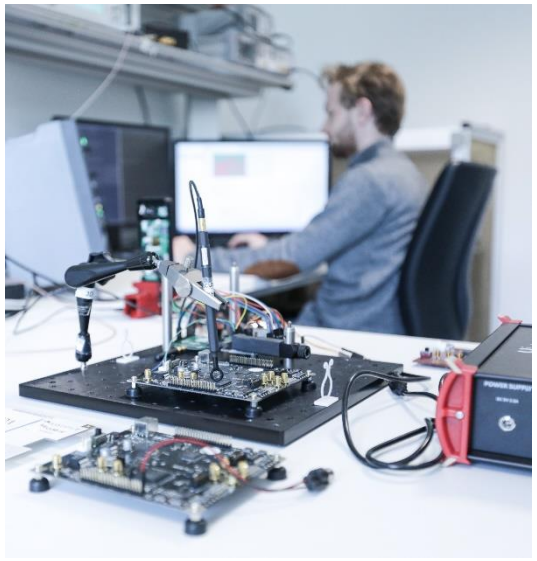
ANALYZR
Post-Silicon Evaluation

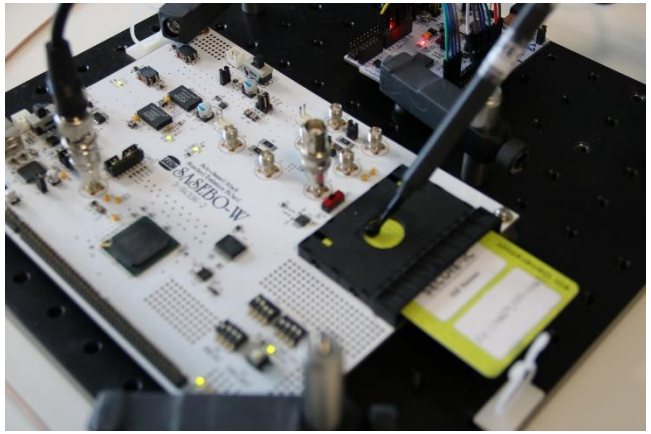
IP
Crypto / non Crypto

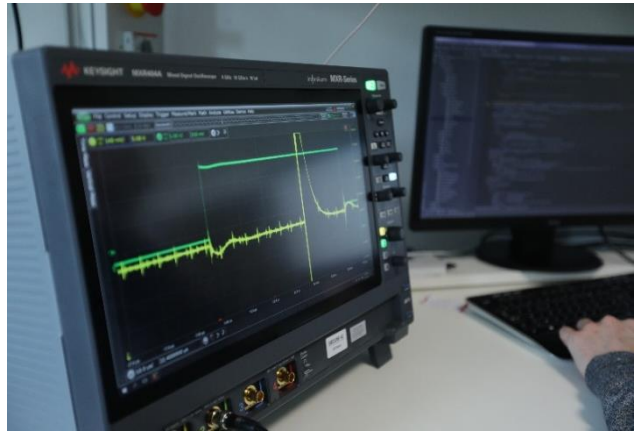
SoC

FPGA/ASIC
eFPGA

End-User device







**Compliant with:** ISO IEC

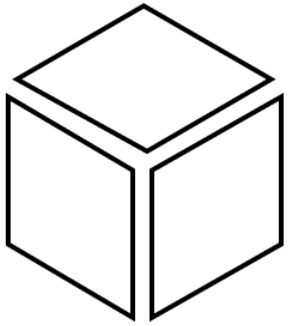
ISO/IEC JTC 1/SC 27/WG 3 **N 2132**

**ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"**
Convenorship: **UNE**
Convenor: **Bañón Miguel Mr**

**Technical Study for application of ISO 15408 evaluation framework to evaluation of ISO/SAE 21434 requirements**

# WHITE BOX & BLACK BOX ANALYSIS

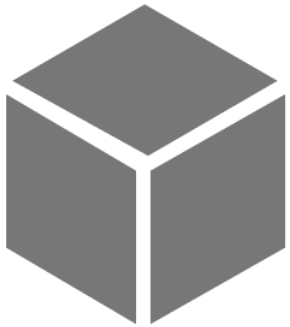
## Real ToE level: White Box / Black Box



**WHITE BOX**

**I know everything inside**

- Algorithm
- Specification
- SW and HW structures
- Full access (GPIO, etc)
- Script for communication
- Protection sensors disabled

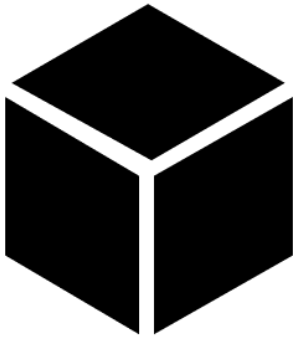


**GREY BOX**
(White-Black)

**I have a partial knowledge**

- Only Algorithm
- Or Implementation
- Partial access (deal with sensors)
- No script for communication

…

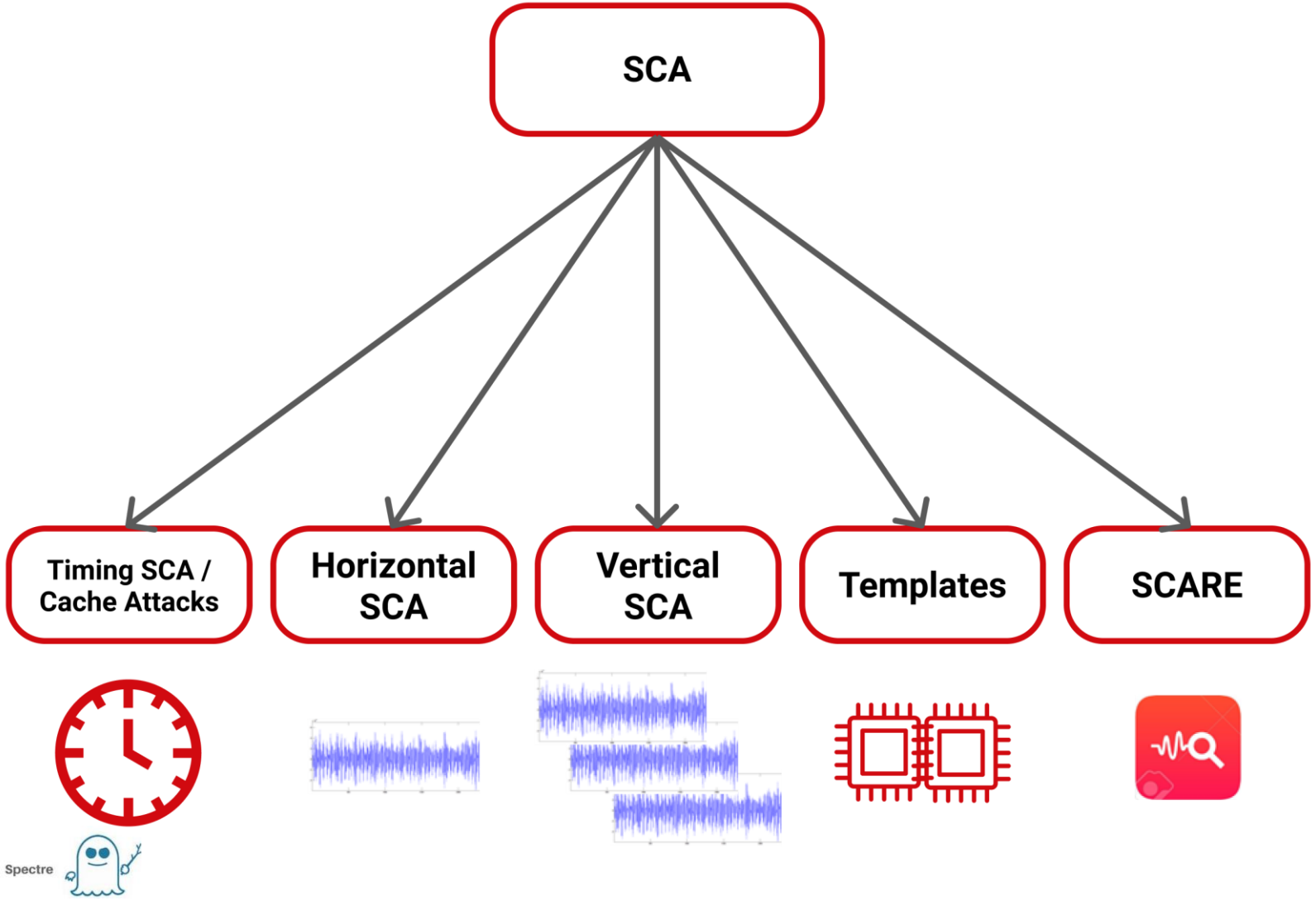


**BLACK BOX**

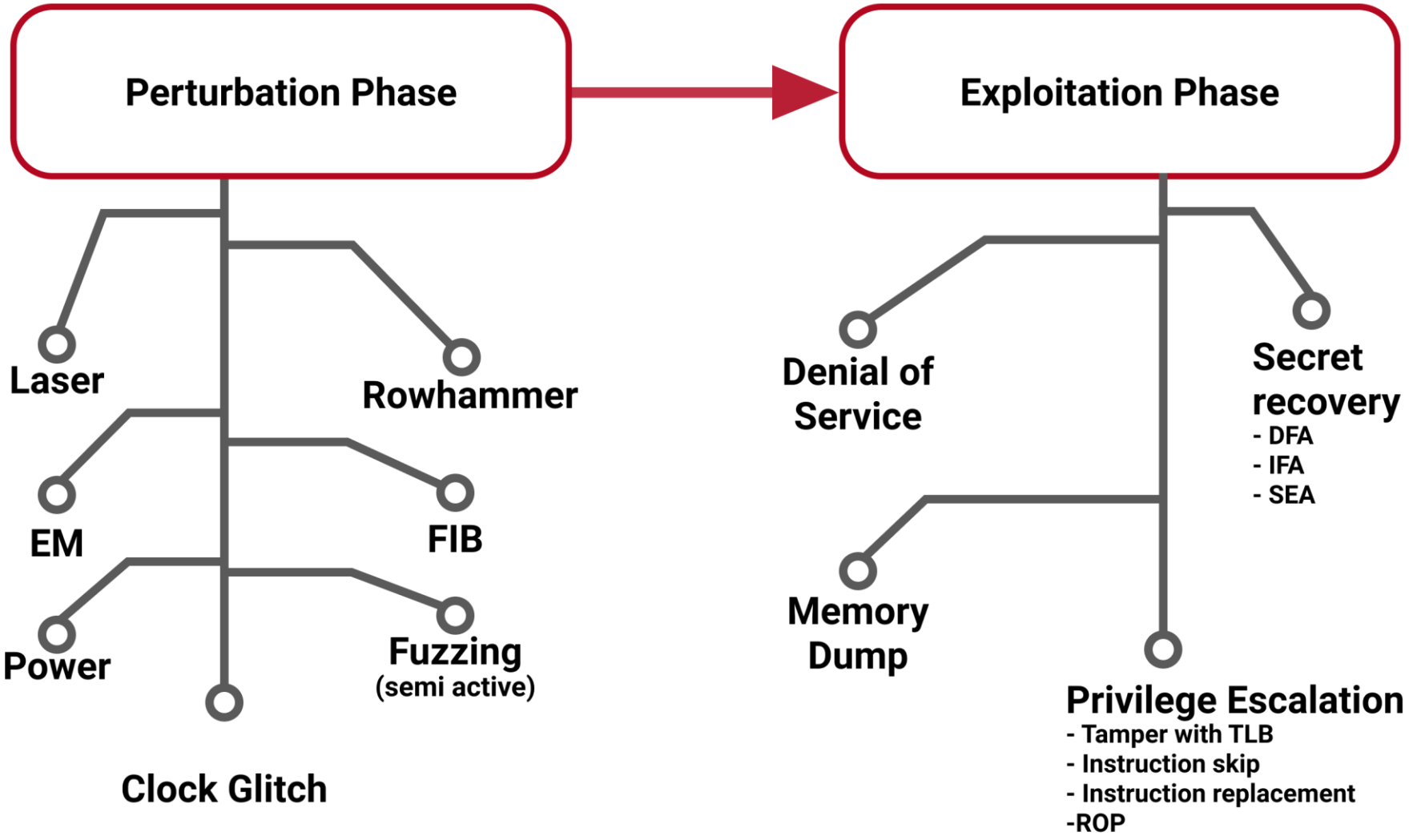
**I have zero knowledge**

- End-user product
- No provided documentation
- Hard access to the device (no GPIO, etc)
- Deal with sensors, etc

# ABOUT SECURITY THREATS PASSIVE ANALYSIS (SCA)



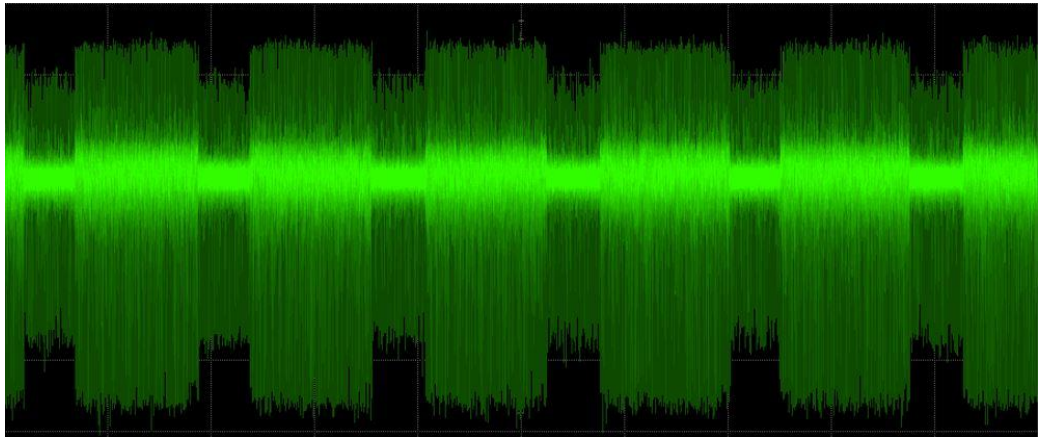
# ABOUT SECURITY THREATS ACTIVE ANALYSIS



# DEMONSTRATION: SCA on a smartphone

- Goal: Analyze a smartphone to validate its resilience against Side Channel Analysis

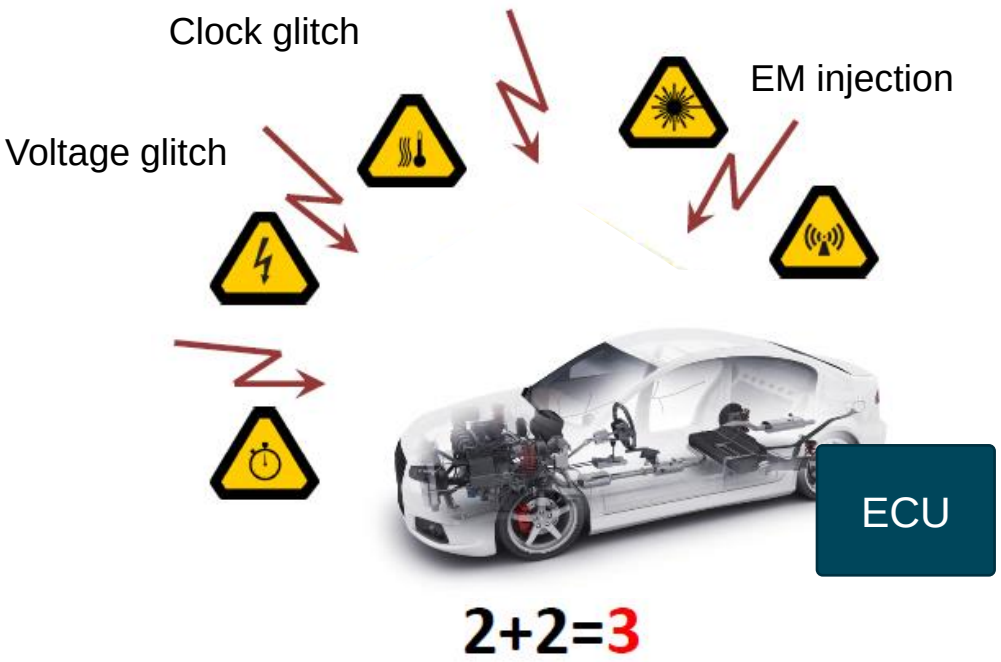
- Analysis strengths:
  - Recover the algorithm which is used to protect the data
  - Recover the secret key used to protect the data



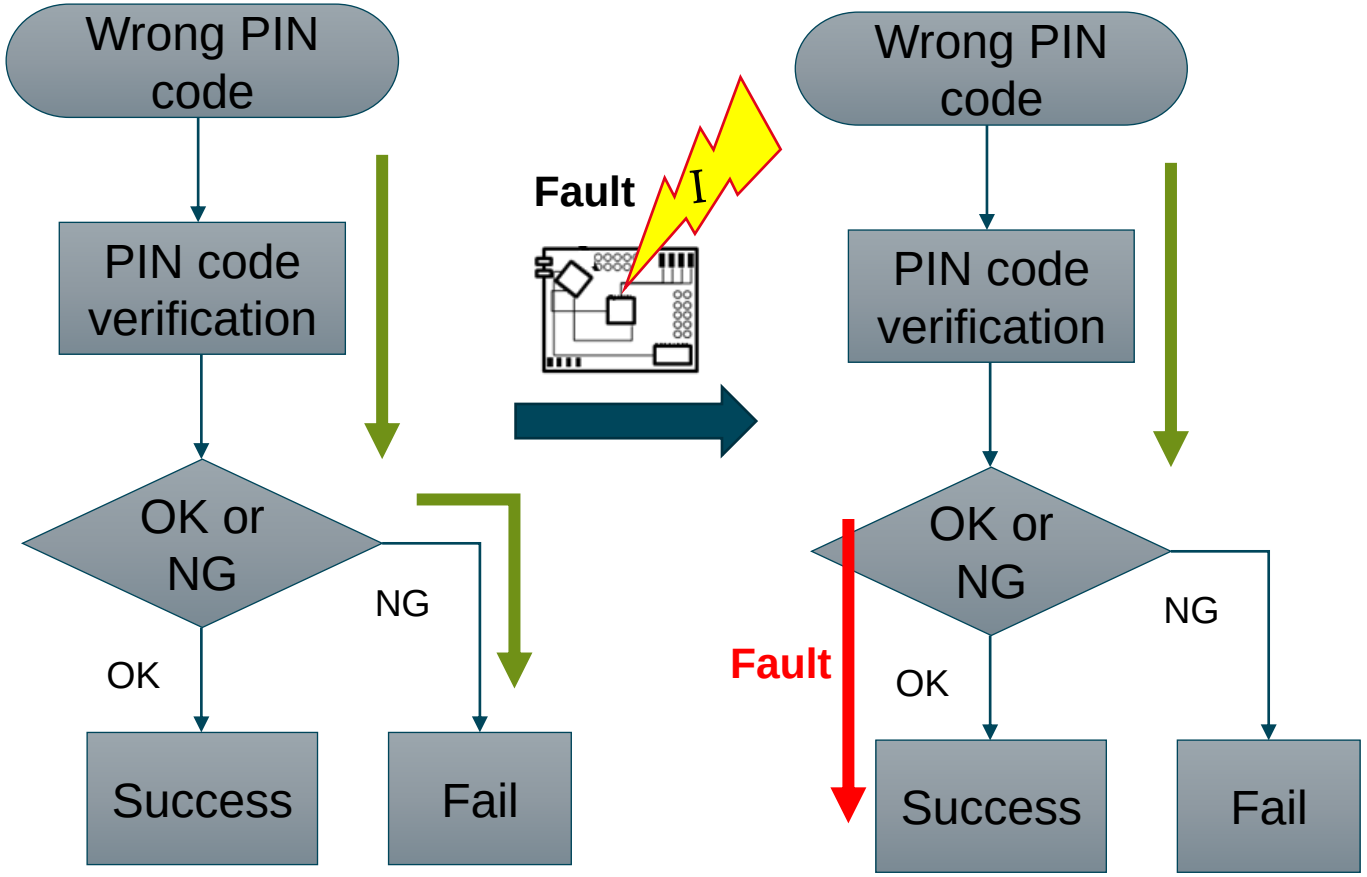
Pattern recognition

# Fault Injection attack capability

- Fault Injection can **induce miss-instruction** of ECU (e.g. skip encryption)




**Induce miss-calculation**



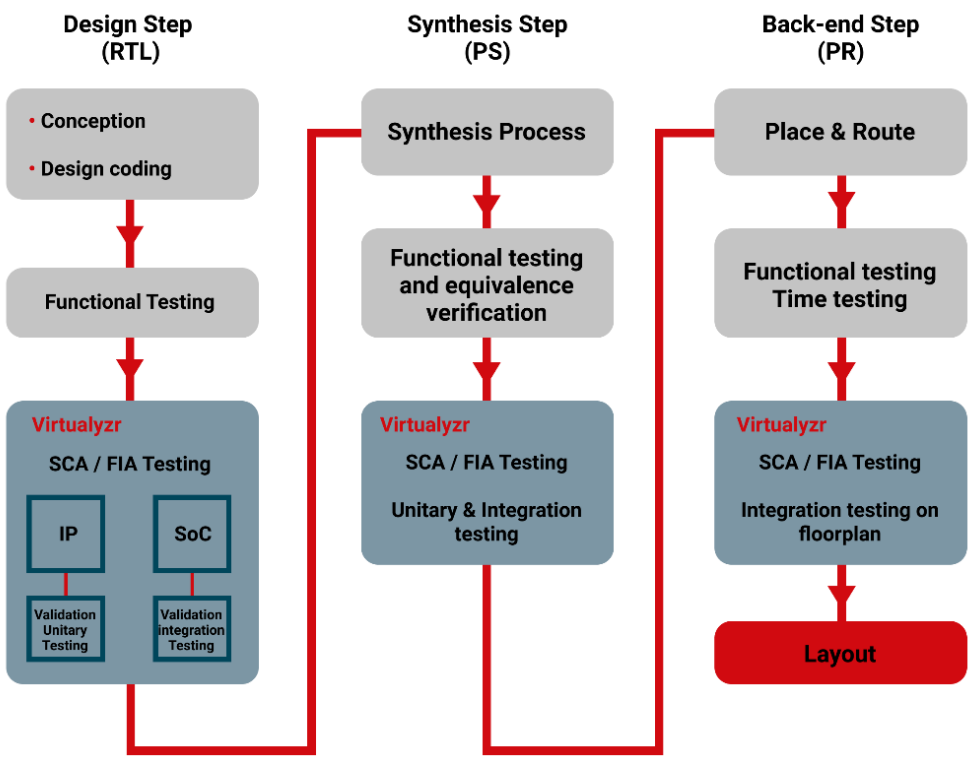

**Induce miss-instruction**

# EASY INTEGRATION TO THE DESIGN LIFE-CYCLE

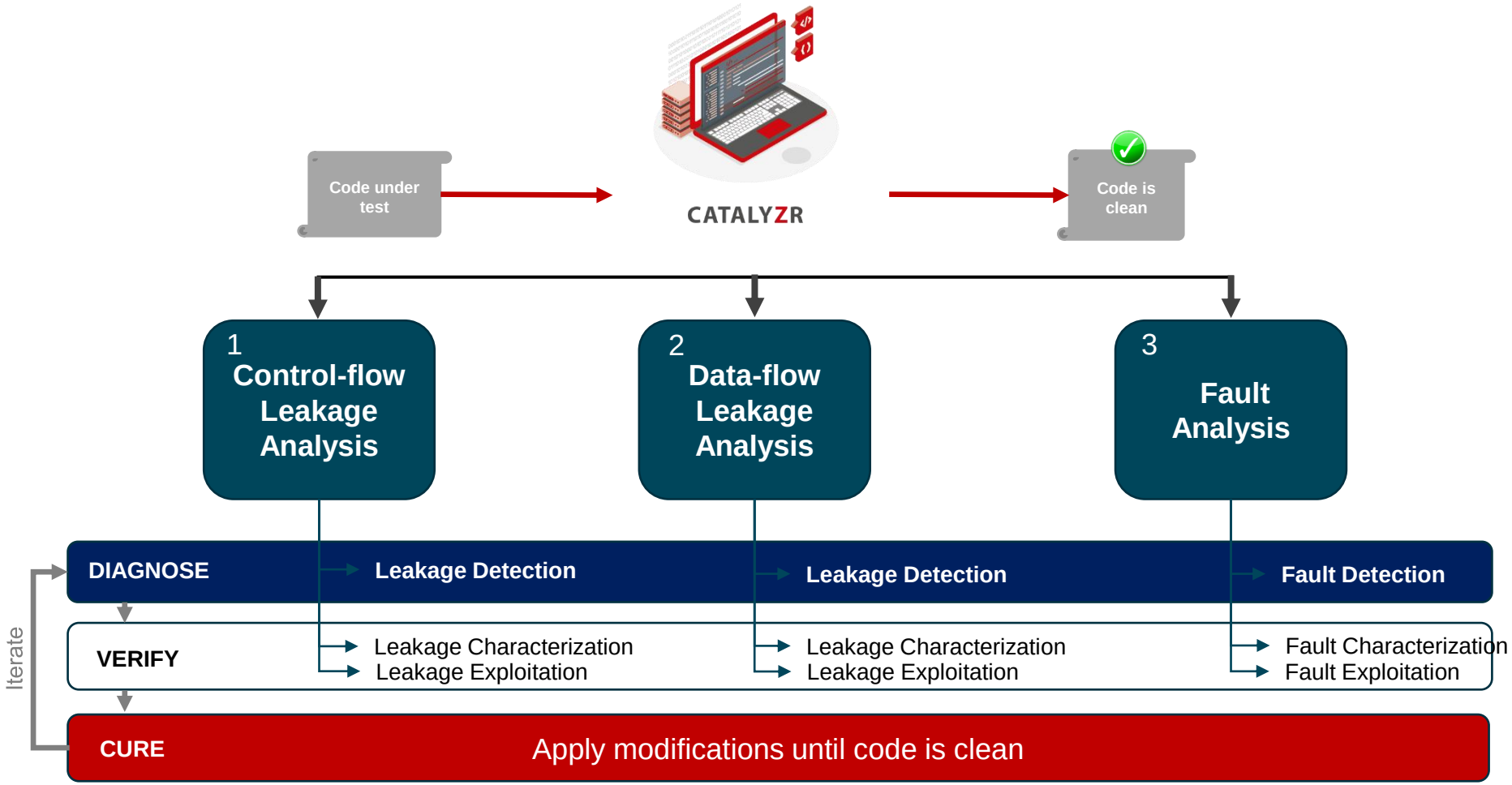
VIRTUALYZR™

**EDA Axes**

- **Design**
  - High level Synthesis
  - Logic Synthesis
  - Schematic capture
  - Layout
- **Simulation**
  - Transistor / Logic / Behavioral / HW Emulation
- **Analysis & Verification**
  - Functional verification
  - Formal verification
  - Static Timing Analysis
  - Clock Domain Crossing Verification
  - Mask Data Preparation
- **Functional Safety**
  - Analysis (compuatation failiure in time rate and diagnostic)
  - Synthesis (add reliability to structured components)
  - Verification (run a fault campaign: error detection)
- **Security Analysis**
  - RTL / PS / PR / Layout Security (SCA / FIA and more)
  - HW and SW Analysis



# CATALYZR KEY MODULES



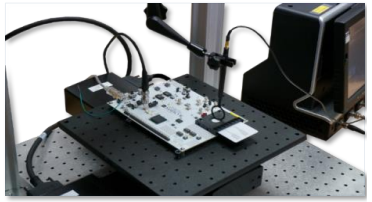
# SECURE-IC'S COMMITMENT - HARDWARE PENTEST

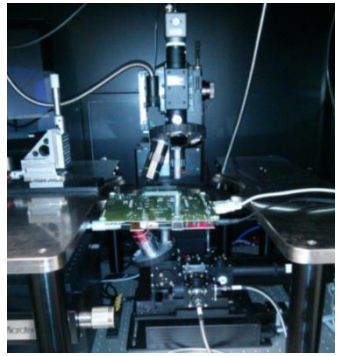
- Commitment in equipment: the best available on the market (Hardware)

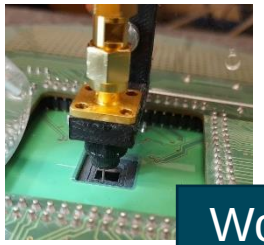
## Instrumentation: stimulate & observe



## Reverse-engineering and Bespoke Glitch and system perturbation equipment

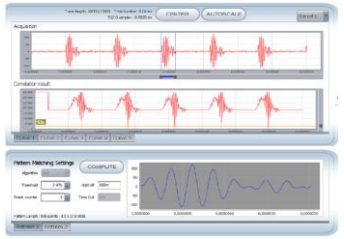


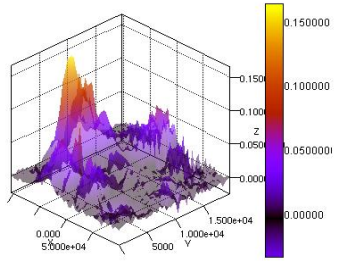


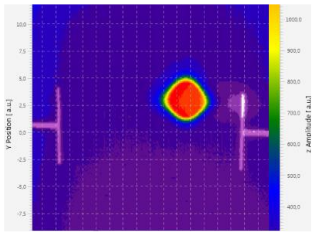



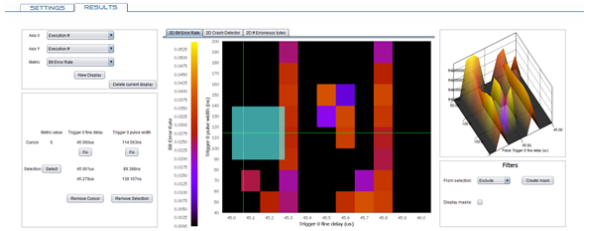
Worldwide unique BBI EM Injection

## Pilot Software Analyzr™





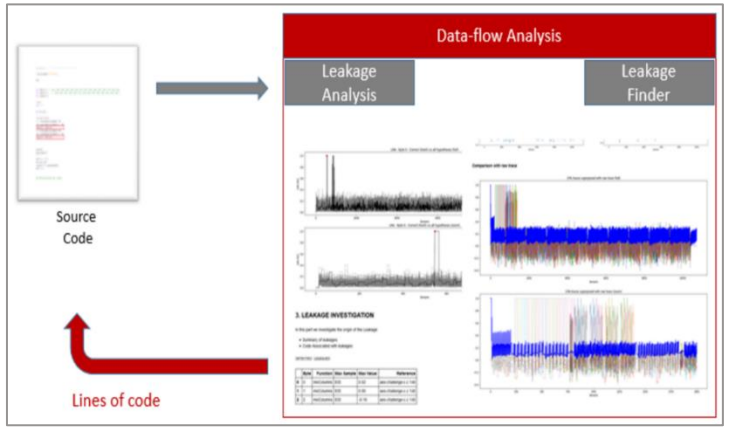



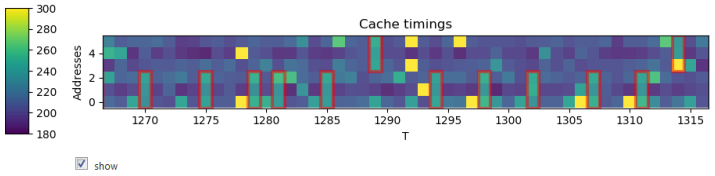


# SECURE-IC'S COMMITMENT – SOFTWARE PENTEST

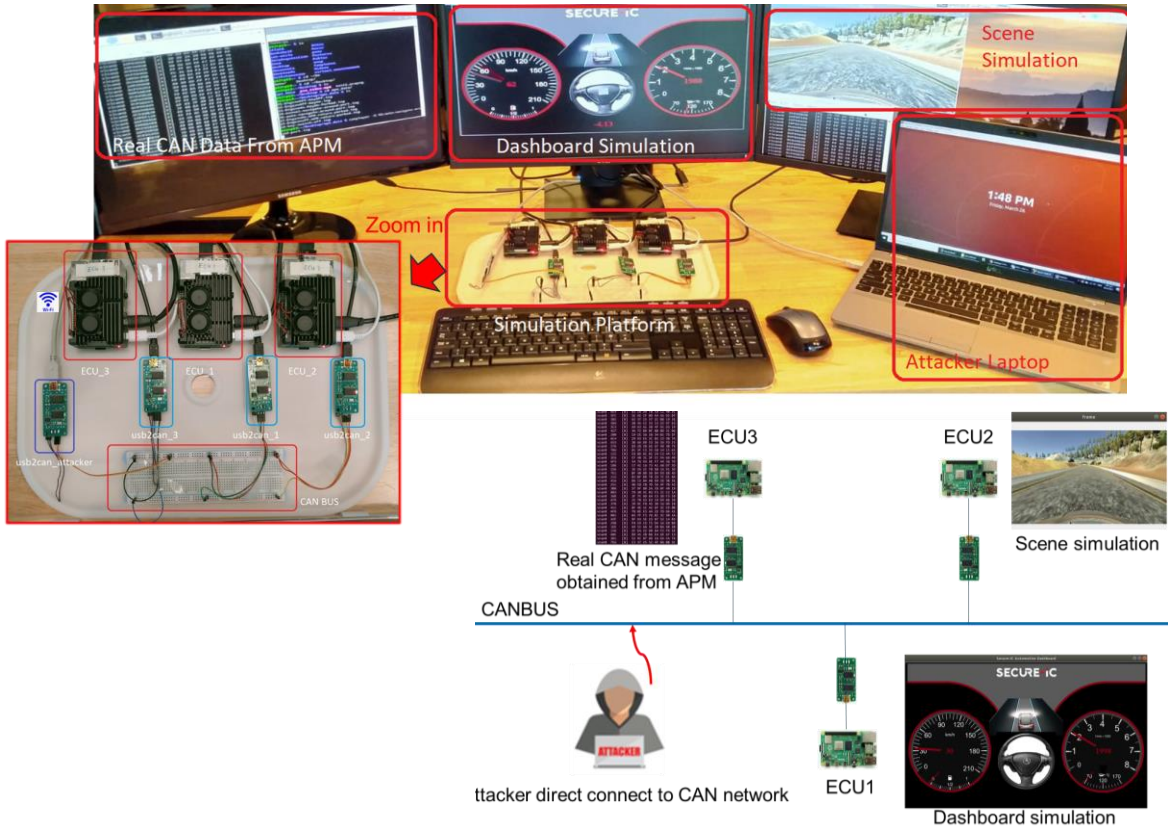
- Commitment in equipment: the best available on the market (Software)

## Cache-timing, SCA, FIA on SW: Catalyzr™



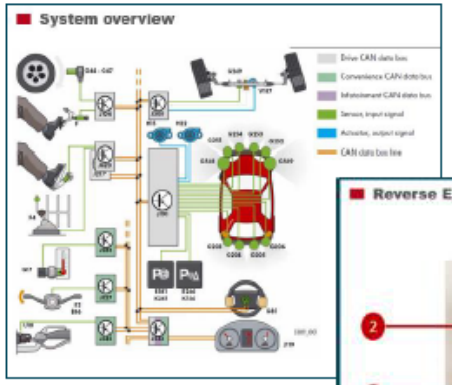

## Fuzzing & Protocol attacks

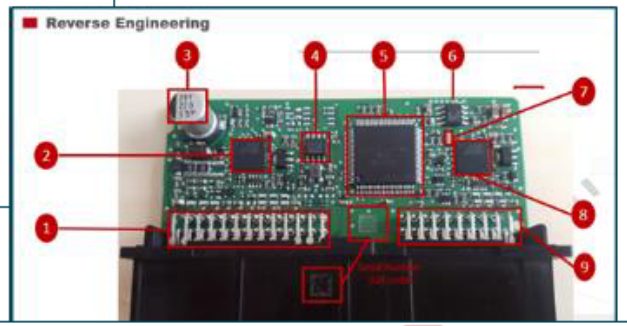


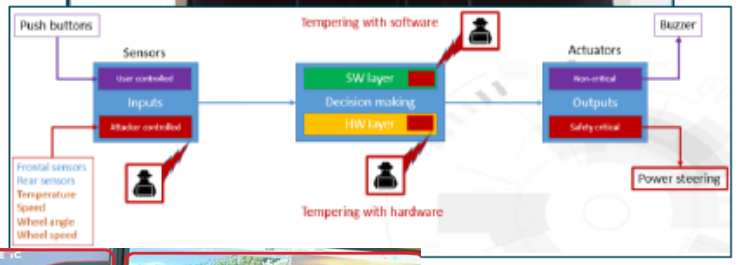
# SECURE-IC'S PROJECTS REFERENCES



- Penetration Tests for CAN / ECU Network

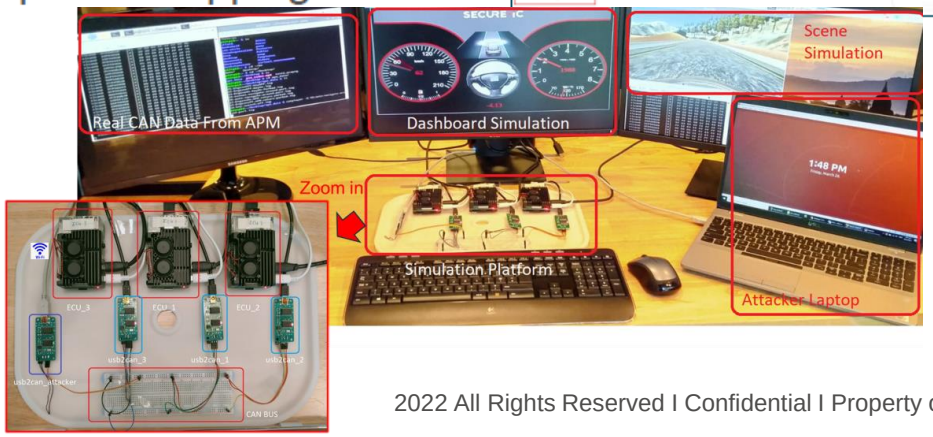



- Project application: Security Evaluation
- Region: SEA
- Period: 2020

- **Technical scope delivered:**
  - System Requirements
  - Hardware reverse engineering : component and pinout mapping
  - Automated CAN network fuzzing and tests:
    - Ability to withstand DoS attacks
    - Ability to withstand frame replay attacks
    - Ability to withstand frame injection attacks
    - Diagnostic interface testing

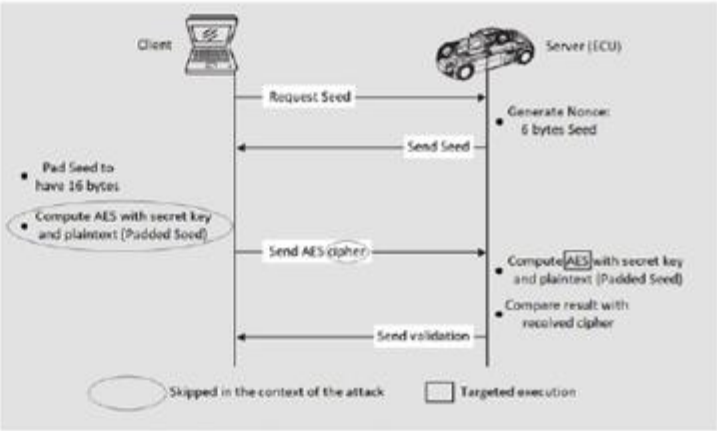


# SECURE-IC'S PROJECTS REFERENCES

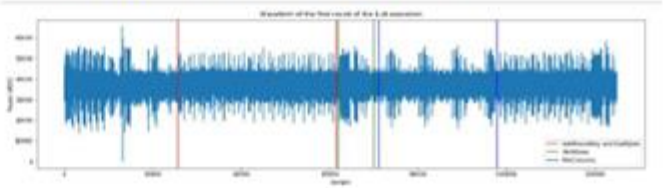


- Side Channel attacks on Diag for Automotive ECU

Analysis set-up




Unified Diagnostic Services (Security Access) protocol

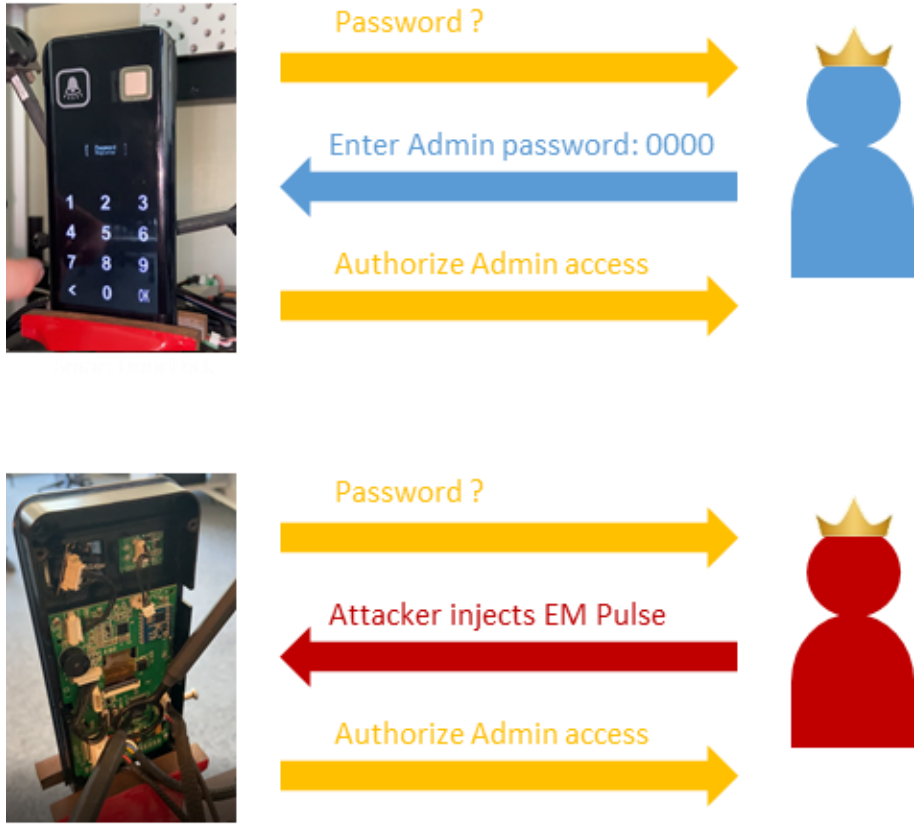


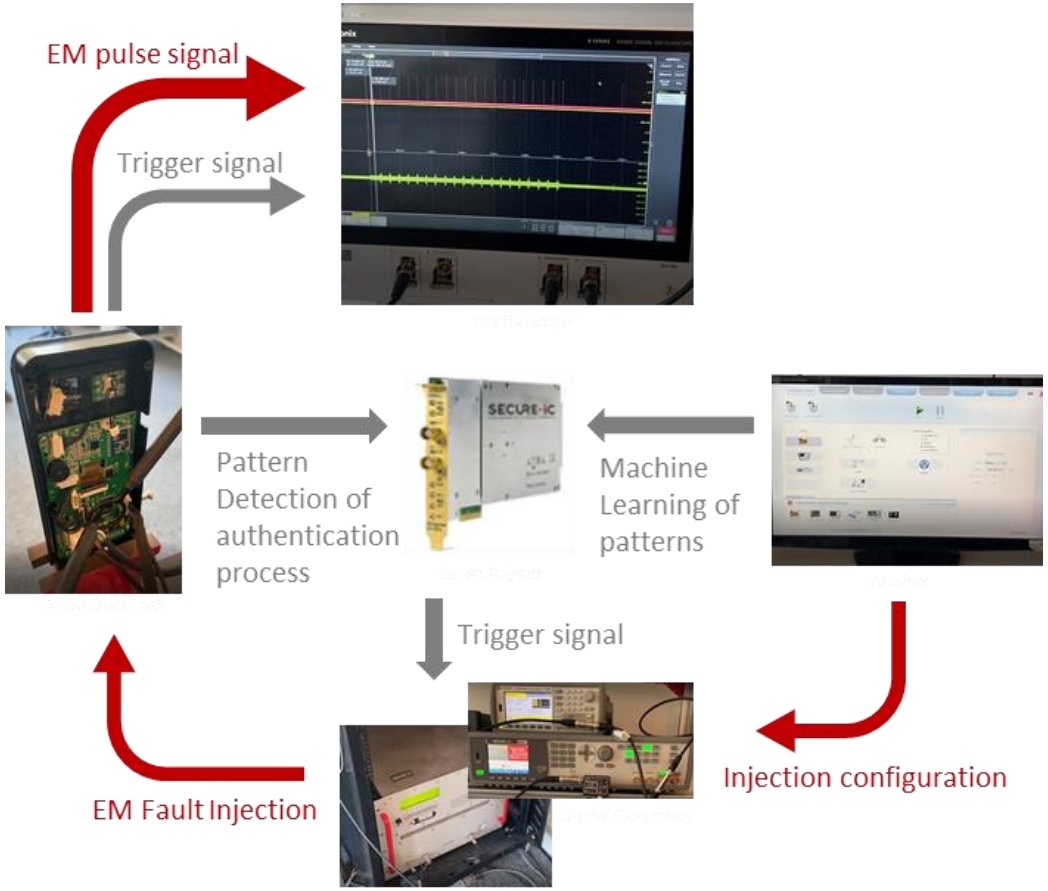
- Project application: Security Evaluation
- Region: SEA
- Period: 2020

- **Technical scope delivered:**
  - System setup for SCA attack on Security Access service (0x27) Diagnostics protocol featuring an AES-based Seed-and-key access
  - Test cycles performed to recover access and keys
  - Seed and key protocol were broken

# AUTHENTICATION BYPASS USING FAULT INJECTION: DOORLOCK EXAMPLE




- Goal:
  - Bypass authentication

# REPORT SAMPLE

SECURE-iC
THE SECURITY SCIENCE COMPANY

NUVOTON TECHNOLOGY CORPORATION

SECURITY EVALUATION REPORT

January 26th, 2022

SECURE-iC TRUSTED

WWW.SECURE-IC.COM

### 2.1. Target description

The Target Of Evaluation Nuvoton NuMicro® M2354, visible on Figure 7, is a microcontroller mostly designed for Internet of Things (IoT) devices. Its security focuses on physical attacks such as Side-Channel Attacks (SCAs) or Fault Injection Attacks (FIAs).

**Figure 7. 6 samples of the Target Of Evaluation (top), with 3 Nu-Link-Pro Adapters (bottom).**

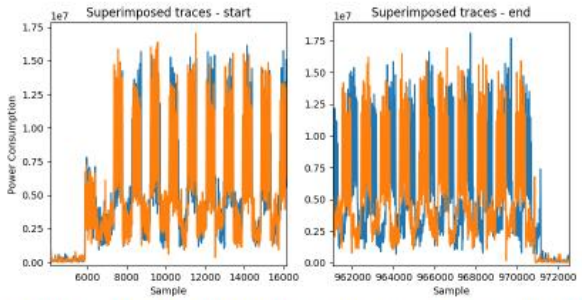



**Figure 50. Superimposed protected RSA-CRT-2048 traces: the traces are synchronized at the beginning, but not at the end of the exponentiation.**

However, a potential vulnerability has been detected on the Square & Multiply patterns. In Figure 51, one can distinguish different shapes of the couple Multiply-Square. Different bounds of frequency (FFT transformation) have been analysed.

As the randomized exponent is not accessible, one cannot efficiently check this assumption, since one should make a full advanced SPA evaluation to recover the whole exponent. Nevertheless, if the addresses are not randomized, template attacks are still possible, but need to power-off the Pseudo-Random Number Generator (PRNG) to perform the learning phase.

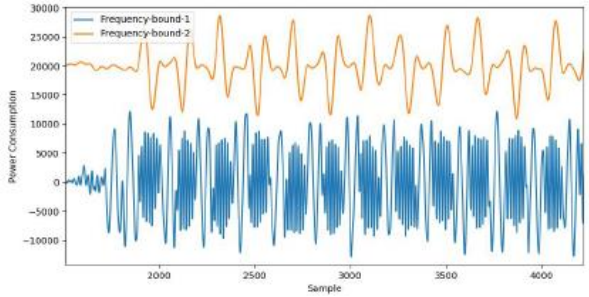



**Figure 51. FFT filter at two different bound frequencies: the blue curve characterizes the multiplication, while the orange one characterizes the square operation.**

# OTHER RECOMMENDATIONS

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
**Ambassade de France au Japon**

DGRIS

DIRECTION GENERALE DES
RELATIONS INTERNATIONALES
ET DE LA STRATEGIE
Defense Section Tokyo

Tokyo, 5th July 2020
N° 216 /ARM/DGRIS/MDD-TKO/NP

To whom it may be concern,

I hereby attest, Captain (Navy) Francois DUHOMEZ, Defense attaché at the French Embassy in Japan, that Secure-IC SAS, a company registered in France with headquarters at ZAC des Champs Blancs, 15 rue Claude Chappe Bât. B, 35510 Cesson-Sévigné, France, is a regular supplier of the French Ministry of the Armed Forces ("Ministère des Armées") and its related agencies ("DGA – Direction Generale de l'Armement).

As a world-leading provider of embedded cybersecurity solutions, Secure-IC SAS is a company of global excellence, delivering to the best technology companies in France and worldwide with solutions used in millions of products such as smartphones, laptops and computers, automotive chipsets, smart meters, passports, etc.

I insure you my sincere appreciation for the interest that ones can have for SECURE-IC and their innovative solutions,

With our deep respect,

Captain (N) Francois DUHOMEZ
Defense attaché
Embassy of France, Tokyo

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DES ARMEES

DGA

DIRECTION GÉNÉRALE
DE L'ARMEMENT
*DIRECTION DES OPERATIONS*
*Service des Achats d'Armement*
*Division Achats Bruz*
*DGA/DO/S2A/PROD/DA-BZ*

**CERTIFICAT**
**DE BONNE EXÉCUTION DE MARCHE**
**délivré au titre du marché n°2012 81 0305**

Je soussigné Ingénieur en chef des études et techniques de l'Armement (ICETA) Eric Alamo, autorité signataire des marchés au Service des achats d'armement site de Bruz de la Direction des Opérations (DO) de la direction générale de l'armement (DGA), certifie, par la présente, que le marché n° 2012-81-0305, notifié le 5 février 2013, à la société SECURE IC, relatif au développement d'un système logiciel de simulation de la consommation de composants électroniques pour l'analyse par canaux auxiliaires pour la DGA a été exécuté dans les règles de l'art et mené régulièrement à bonne fin.

Le présent certificat est délivré pour servir et valoir ce que de droit.

Fait à Bruz, le 22 mars 2019

L'ingénieur en chef des études et techniques d'armement
Eric Alamo
Autorité signataire de marchés

*Le présent certificat est délivré au regard de la bonne exécution d'un contrat particulier et ne préfuge pas de la capacité du titulaire à exécuter toute prestations.*
*Le ministère des Armées ne saurait ainsi être tenu responsable des éventuelles difficultés d'exécution par le titulaire de contrats futurs.*

Direction générale de l'armement
Direction des Opérations / Service des achats d'armement
Production / Division achats site de Bruz
BP 7 – 35998 Rennes Cedex 9
Téléphone : 02 99 42 91 60 - Télécopie : 02 99 42 98 59

フランス共和国
軍事省

装備総局
作戦局　装備品購入課

契約履行証明

契約番号 2012 81 0305

下記に署名する、装備総局作戦局において装備品購入課の契約締結権限を有する防衛装備技術研究チーフエンジニア、エリック・アラモはここに、2013 年 2 月 5 日付の SECURE IC との「サイドチャンネル解析のための電子部品の消費電力シミュレーションのソフト開発に係る契約（契約番号 2012-81-0305）」が規定に則り、首尾よく履行されたことを証明する。

2019 年 3 月 22 日ブリュにおいて作成

防衛装備技術研究チーフエンジニア
エリック・アラモ

*本書は特定の契約において上記企業が首尾よく履行したことを証明するもので、あらゆる業務における同企業の履行能力を証明するものではない。今後、仮に同企業が請け負う契約において、同企業による履行が難しくなった場合、軍事省はその責任を問われない。*

装備総局
作戦局 装備品購入課
BP7 – 35998 Rennes Cedex 9
Tel : 02 99 42 91 60 / Fax : 02 99 42 98 59

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

**Partnership with U.S. DARPA to foster security technology innovation**
https://www.secure-ic.com/news/darpa-partnership/

# 4. LIFECYCLE SECURITY MANAGEMENT SERVICES

# SECURITY SERVICE FOR EACH STAGE OF LIFE

| STAGE OF LIFE | SECURITY SERVICE | DESCRIPTION |
|---|---|---|
| Fab / manufacturer premises | **Key management** | Initial (root) key injection (or enrollment if PUF is used). All subsequent accesses and credentials are managed by this key |
| In the wild, at each power-up | **Secure-boot** | Verification of the platform physical and logical integrity, configuration of the defense mechanisms, and logging of the device health |
| While connected to the network | **Cryptographic services** | Authentication and confidentiality of the incoming/outcoming data |
| While being powered-up | **Security monitoring** | Check whether no physical nor cyber attack is perpetrated on data / code at rest |
| While being powered-up | **Data protection** | Check whether no physical nor cyber attack is perpetrated on data / code in transit |
| While being powered-up | **Secure management of specialized resources** | Check whether no physical nor cyber attack is perpetrated on data / code in special operators |
| While being powered-up, when functional or security upgrade is needed | **Secure-boot** | New firmware image is loaded, and system is rebooted |
| While being powered-up, when new users are needed | **Key management** | New keys are derived (e.g., by injection, or by KDF from PUF), and locked |
| Key compromised | **Key management** | Certificates of revocation are sent, and new keys + certificates are installed |
| Device decommissioning | **Key management** | Keys are revoked and state is locked in suicide mode |

# SECURYZR™ SERVER: iSSP Fleet Management Security Services

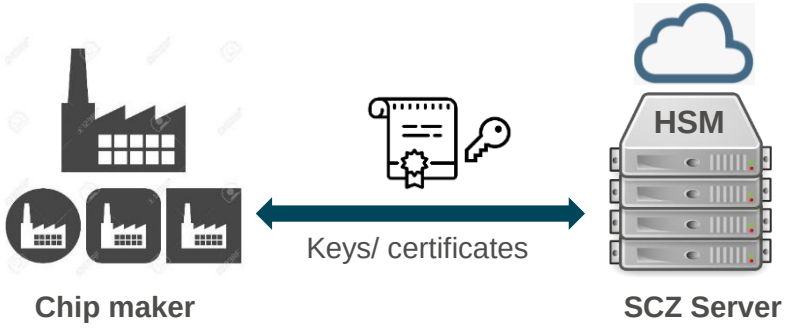
**iSSP IS YOUR TRUSTED iNTEGRATED SECURITY SERVICES PLATFORM FROM CHIP-TO-CLOUD**

| | |
|---|---|
| **KEY PROVISIONING** | • Provision and manage securely your devices' assets: keys and certificates |
| **FIRMWARE UPDATE** | • Update and manage securely your devices' software: Firmware and applications |
| **MONITORING** | • Monitor securely your devices' status against intrusions and anomalies |
| **DEVICE IDENTITY** | • Trust from the chip to the cloud your devices, users and data |

# Key Provisioning Service

**PROVISION AND MANAGE SECURELY YOUR DEVICES' ASSETS: KEYS AND CERTIFICATES.**

- 8 key action services



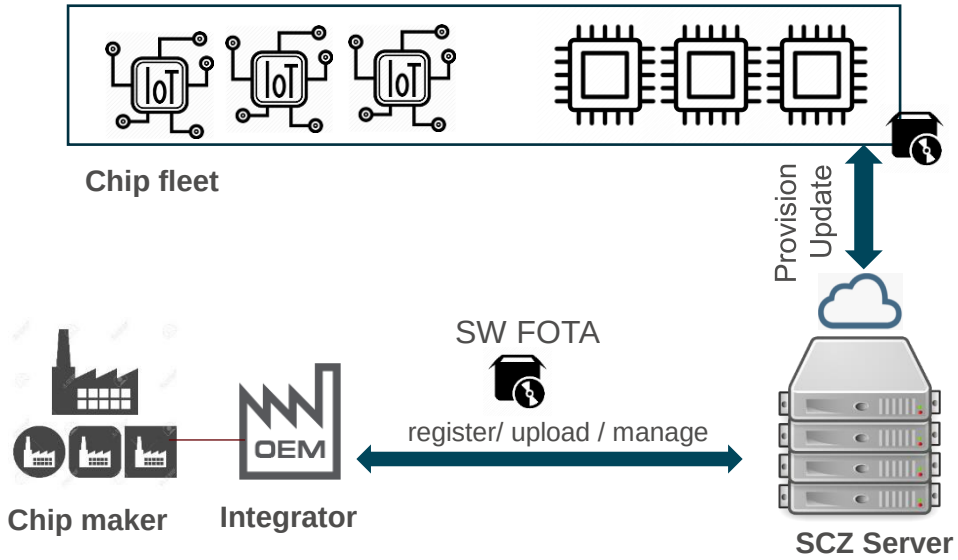

Key Provisioning

1. Assets Generate
2. Assets Store
3. Assets Transport
4. Assets Inject/Install
5. Assets Update
6. Assets Revoke
7. Assets Import/Export
8. Assets Fleet Lifecycle

# Firmware Update Service

**UPDATE AND MANAGE SECURELY YOUR DEVICES' SOFTWARE: FIRMWARE AND APPLICATIONS.**

- 8 key action services



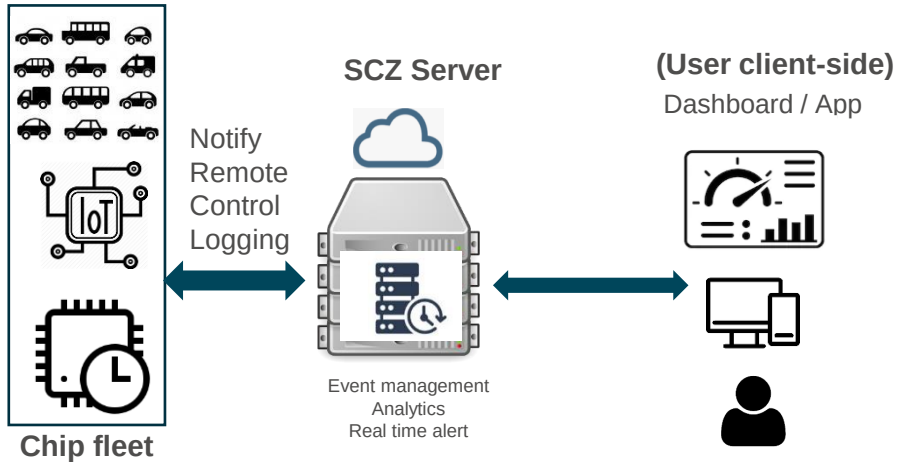

Firmware Update

1. SW Import
2. SW Store
3. SW Analyze
4. SW Sign Verify
5. SW Rollback
6. SW Transport
7. SW Update
8. SW Fleet Lifecycle

# Device Monitoring Service

**MONITOR SECURELY YOUR DEVICES' STATUS AGAINST INTRUSIONS AND ANOMALIES.**

- 4 key action services




Device Monitoring

1 Status Monitoring

Event Monitoring

2 Anomaly Handling

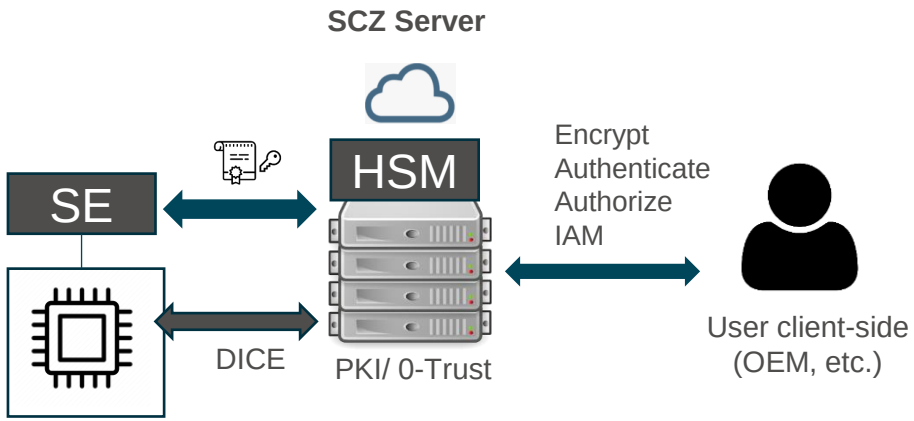
3 Intrusion Detection

4 Fleet Monitoring

# Device Identity Service

**TRUST FROM THE CHIP TO THE CLOUD**
**YOUR DEVICES, USERS AND DATA.**

- 5 key action services




Device Identity

1. Device Authentication
2. Device Credential Mgmt.
3. Device Remote Attestation
4. User IAM
5. Fleet Identity Lifecycle

# 5. KEY TAKEAWAYS

# SERVICE TO CERTIFICATION READINESS

## Pedagogical certification scheme analysis

- Certification overview – scope
- Review of certification levels and associate requirements
- Analysis of Laboratory offer
- Detailed Explanations of certification process

## Target Evaluation and Environment definition

- Specification and Product documentation review
- Architecture review

## Security target

- Compliancy with targeted assurance level
- Test of the implemented protection and pre-quotation using Analyzr tool
- Gap Analysis

# FULL SUPPORT TO REACH CERTIFICATION

Multiple benefits with Secure-IC as a partner to pass Certification:

A. Faster Go-to-market:
- Lot of time can be saved on the certification process by producing a high end and well focused documentation

B. Save Workload:
- A large amount of complex technical work in terms of documentation can be handled for
  - HW part
  - SW part

C. Save Money:
- Reduce time and HR workload in the certification process down the line

D. Higher Confidence:
- Secure-IC's employees have high experience in certification and support to certification

# GUARANTEE SECURITY ALL ALONG THE LIFECYCLE

**SECURE-IC SUPPORTS THE ECOSYSTEM AT EVERY STEP OF THE PRODUCT LIFECYCLE STARTING FROM SPECIFICATIONS UP TO THE HIGHEST CERTIFICATION LEVELS**

- It is the role of the **integrated Secure Element** to safeguard the product at the silicon level.
- Security certifications in any industry must be clearly known and applied all along the value chain
- Security should be evaluated all along the steps of its lifecycle and in depth
- To ensure the integrity of the data, the whole system must be secured and managed. **Trusted devices enable trusted data** through a secure **Chip to Cloud** method.

Joy of innovation

nuvoTon

SECURE-iC

THE SECURITY SCIENCE COMPANY

谢谢

謝謝

Děkuji

Bedankt

Thank you

Kiitos

Merci

Danke

Grazie

ありがとう

감사합니다

Dziękujemy

Obrigado

Спасибо

Gracias

Teşekkür ederim

Cảm ơn