SECURE-IC
THE SECURITY SCIENCE COMPANY

MANAGING NATURAL HAZARDS AND ADVERSARIAL FAULT INJECTIONS IN THE CONTEXT OF CONNECTED EMBEDDED SYSTEMS

Sylvain Guilley
Co-founder and CTO of Secure-IC

September 17th, 2021

AGENDA

1. Introduction
2. Sensors
3. Aggregation
4. Chip-to-Cloud Reporting
5. Conclusion

SECURE-IC
THE SECURITY SCIENCE COMPANY

1. INTRODUCTION

INTRODUCTION

Sylvain Guilley is the co-founder and CTO of Secure-IC.

Sylvain is also professor at “Télécom Paris”, associate research at “École Normale Supérieure” (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS). His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal / mathematical methods.

Since 2012, he organizes the **PROOFS** workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. Sylvain is also lead editor of international standards, such as **ISO/IEC 20897** (Physically Unclonable Functions), **ISO/IEC 20085** (Calibration of non-invasive testing tools) and **ISO/IEC 24485** (White-box Cryptography). He is also editor of the **TR68** part 3 (Cybersecurity of Autonomous Vehicules).

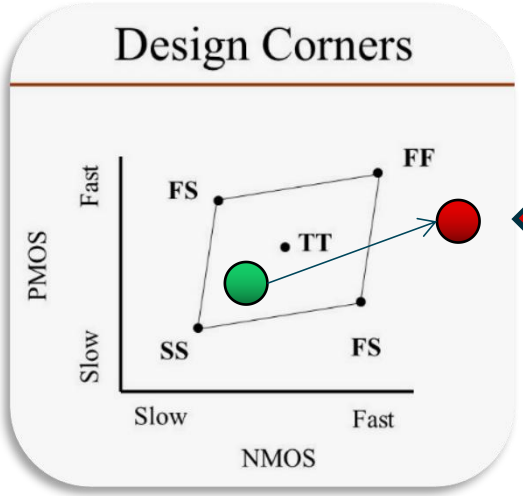
Sylvain has co-authored 250+ research papers and filed 40+ patents. He is member of the IACR, the IEEE and senior member of the CryptArchi club. He is alumni from “École Polytechnique” and “Télécom ParisTech”.

SECURE-IC
THE SECURITY SCIENCE COMPANY

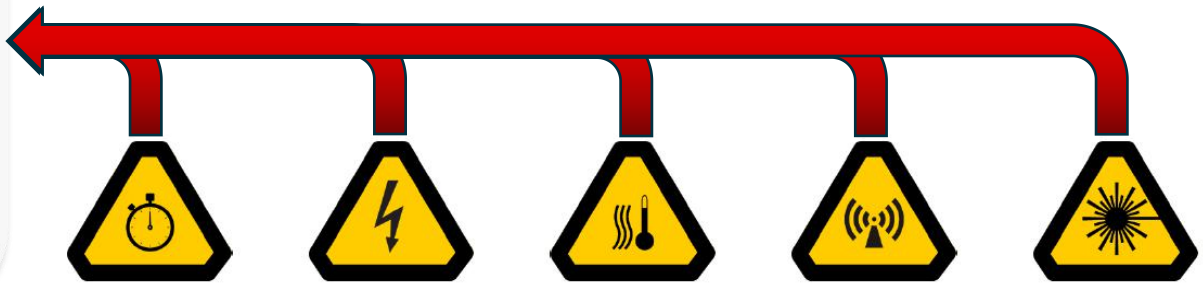
2. SENSORS

CONTEXT
(CYBER-PHYSICAL SYSTEMS, IOT, M2M, AUTOMOTIVE)

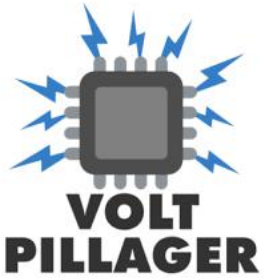
- **Attacks on chips**
  - Physical disruption
    - Clock glitch
    - EM glitch
  - DVFS abuse
    - CVE-2019-11157



- **Hazards on chips**
  - Likewise, but *natural* instead of *malevolent*



→ **Need for detection!**

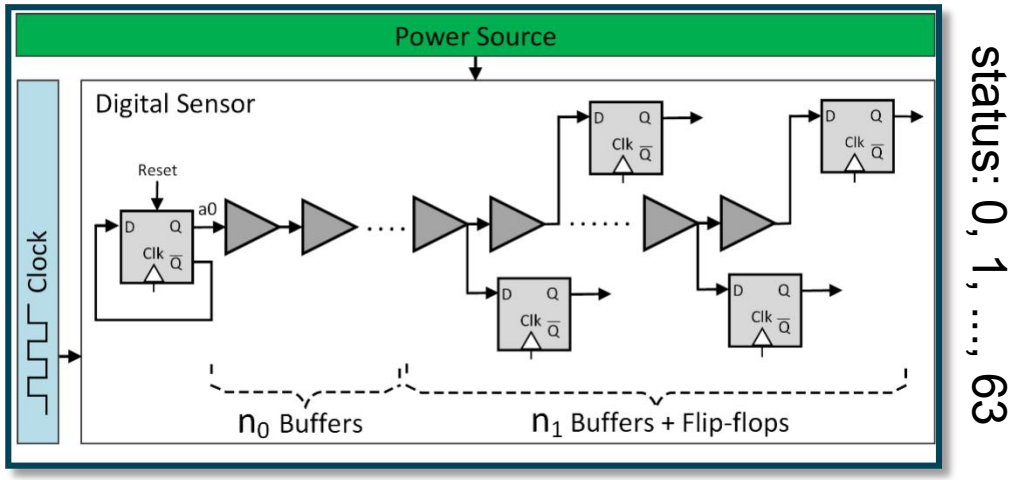


M. T. Hasan Anik, M. Ebrahimabadi, H. Pirsiavash, J. -L. Danger, S. Guilley and N. Karimi, "On-Chip Voltage and Temperature Digital Sensor for Security, Reliability, and Portability," 2020 IEEE 38th International Conference on Computer Design (ICCD), 2020, pp. 506-509.

Md Toufiq Hasan Anik, Jean-Luc Danger, Sylvain Guilley, Naghmeh Karimi: Detecting Failures and Attacks via Digital Sensors. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 40(7): 1315-1326 (2021)

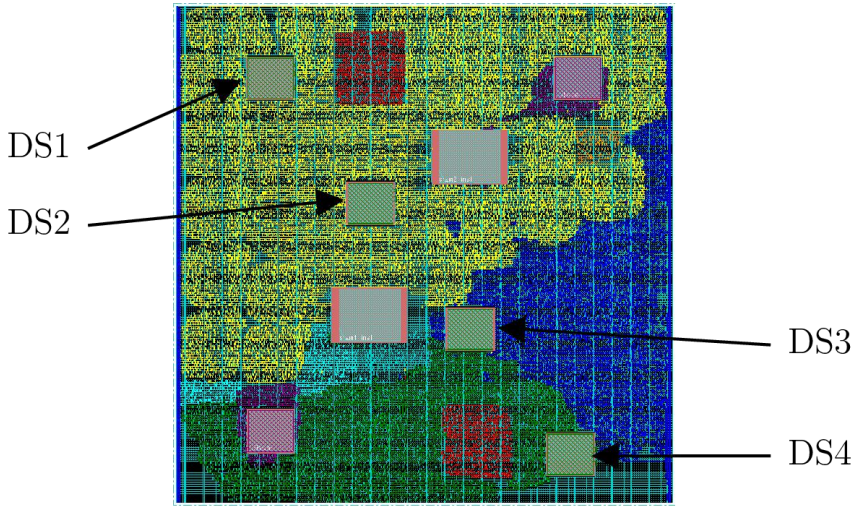
DIGITAL SENSORS (DS)

- **Are fully digital**
  = Made of standard cells
  - DS consist in artificial critical paths
    - Ease of integration
    - Furtivity
    - Aging in parallel with the logic in which it is embedded



Schematic of one digital sensor (DS)

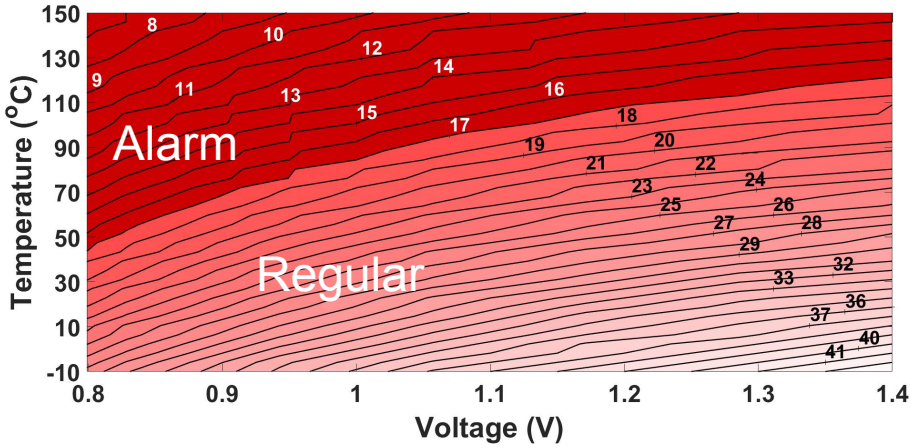
- **Compact / low power**
  - Hence can be instantiated in several instances per chip
  - Located near sensitive IPs:
    - Processor
    - Cryptographic modules



Example of 4 DS for local attacks detection

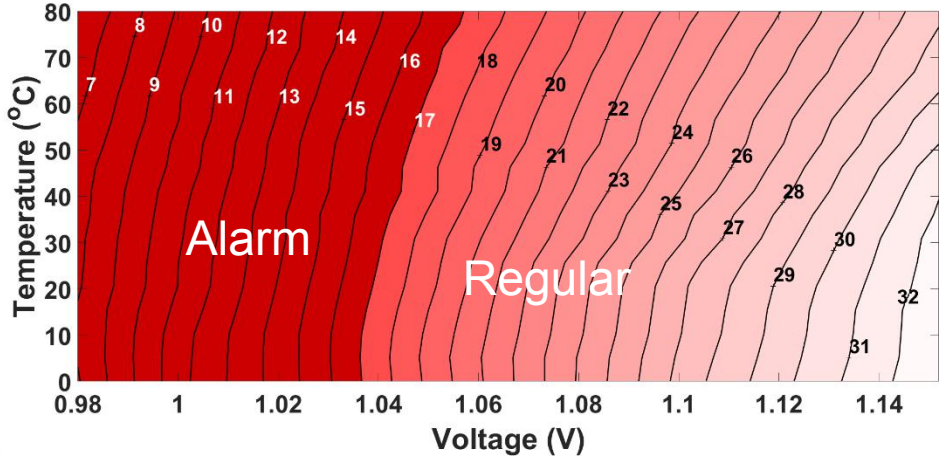
SENSING ACROSS VOLTAGE & TEMPERATURE PLANE (WITH 1 SENSOR)

- **Simulations:**
  - Monte-Carlo HSpice simulations (NANGATE 45 nm) of the sensor
  - Status threshold to raise an alarm: **17** (related to V=1.0V, 85°C - 185°F)



Using Digital Sensors to Leverage Chips' Security, Mohammad Ebrahimabadi, Md Toufiq Hasan Anik, Jean-Luc Danger, Sylvain Guilley and Naghmeh Karimi, IEEE PAINE, 2020, December 15-16.

- **Real device:**
  - FPGA implementations (low power 45 nm, 9 metal layers) of the sensor
  - Status threshold: **17** (V=1.05V, 60°C - 140°F)



- **Same qualitative behavior**
- **Calibration is post-layout**
- **AI algorithms help in this respect**

CONCLUSIONS ON DIGITAL SENSORS

- **KEY TAKEAWAYS:**
  - Devices need to be dependable
  - Digital sensor IP detects voltage & temperature
  - Multiple digital sensors can detect local attacks

(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) **EP 2 960 665 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
24.05.2017 Bulletin 2017/21

(51) Int Cl.:
G01R 31/3193 *(2006.01)* ***G01R 31/30*** *(2006.01)*

(21) Application number: **14306036.6**

(22) Date of filing: **27.06.2014**

(54) **Device and method for calibrating a digital sensor**

Vorrichtung und Verfahren zur Kalibrierung eines digitalen Sensors

Dispositif et procédé pour étalonner un capteur numérique

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(43) Date of publication of application:
30.12.2015 Bulletin 2015/53

(73) Proprietor: **Secure-IC SAS**
35510 Cesson-Sévigné (FR)

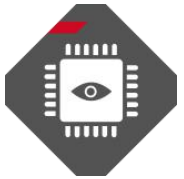
(56) References cited:
US-A1- 2013 300 463

- **NIMAY SHAH ET AL: "Built-In Proactive Tuning System for Circuit Aging Resilience", DEFECT AND FAULT TOLERANCE OF VLSI SYSTEMS, 2008. DFTVS '08. IEEE INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 1 October 2008 (2008-10-01), pages 96-104, XP031345543, ISBN: 978-0-7695-3365-0**
- **SHENG WEI ET AL: "Integrated circuit security**

- **NORMATIVE CONTEXT MOTIVATING THIS IP:**
  - FIPS 140-3 (from levels 3/4), for anti-tampering and EFT / EFP
  - ChinaDRM Enhanced Profile for fault detection
  - OSCCA, BCTC (32 requirements + site audit)
  - CC EAL 4+ with PP084 requirements:
    - Electrical Stimulation
    - Energy and Practice Exposure
    - Physical Manipulation
    - Electro-Magnetic & Electrical
  - ETSI iSIM draft standard (under development) future requirements
  - IEC 61508, ISO 26262-11

HARDWARE-ENABLED CYBER-SECURITY

SECURE-IC'S SOLUTION: CYBER ESCORT UNIT



- Real-time detection of 0-day attacks on code

BENEFITS

- Fill the security gap between SW cybersecurity and HW embedded security
- High security for nearly zero impact on performances
- Ideal for Secure Boot & protection of security-critical and crypto applications
- Forensics reporting, threat analysis → reverse the advantage
- Differentiator: High symbolic impact on the market
- Think ahead: Ahead of DARPA's SSITH program

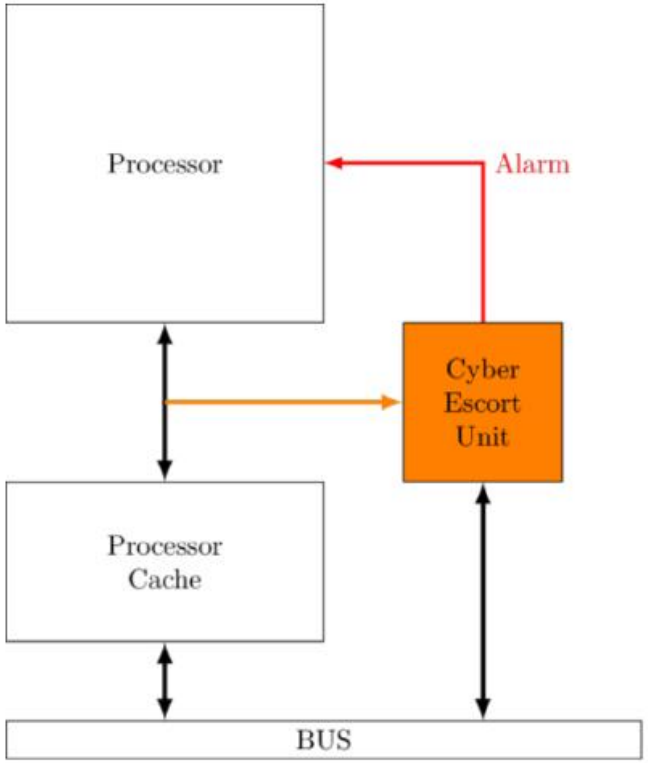
"Computer implemented method and a system for controlling dynamically the execution of a code", US10354064B2

HARDWARE LAYER AND SOFTWARE LAYER MUST COOPERATE FOR SECURITY

CYBER ESCORT UNIT

- **Real-time detection** of zero-day attacks…
  …by escorting step by step the program execution

- General security feature:
  - Protection against all cyber-attacks and physical attacks targeting the code execution or code integrity



DARPA (Defense Advanced Research Projects Agency)'s System Security Integrated Through Hardware and Firmware (SSITH) program (April, 2017)

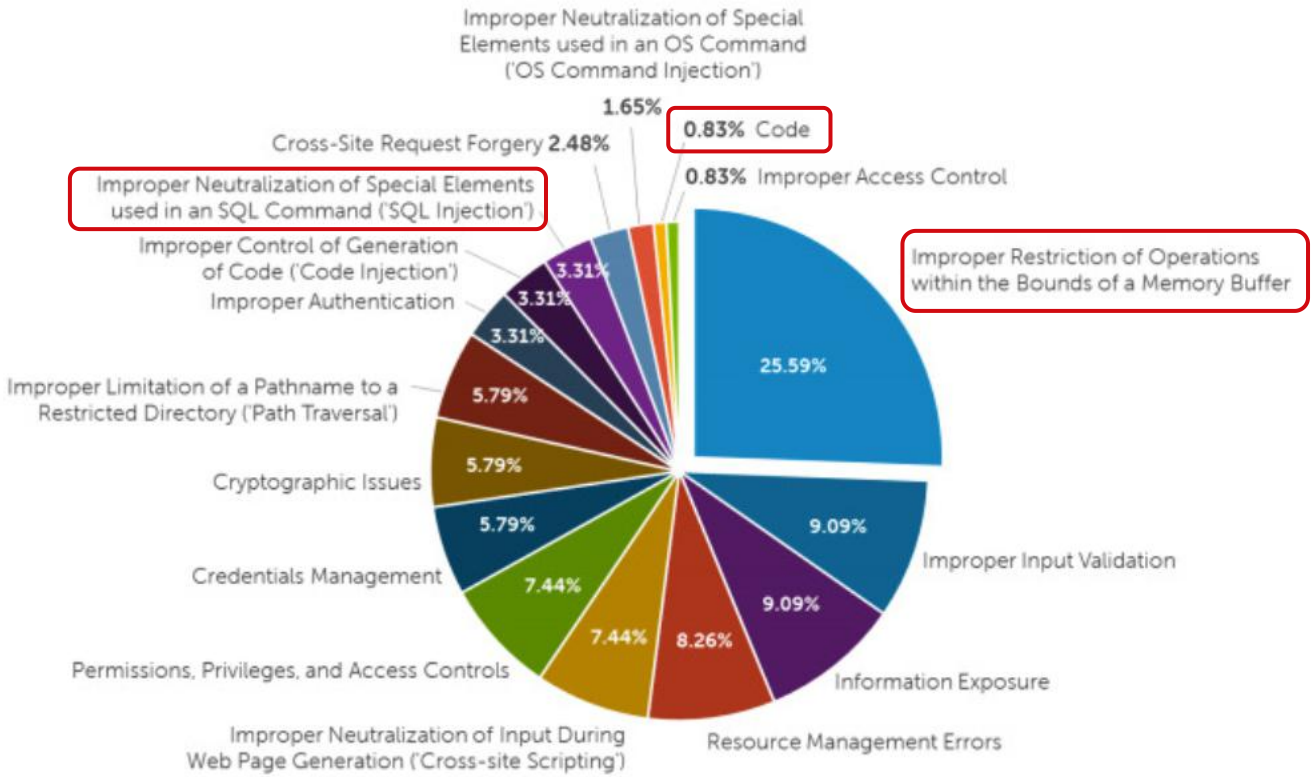
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Common Weakness Enumeration
A Community-Developed List of Software Weakness Types

HW-ENABLED CYBER-SECURITY

MOST FREQUENT CYBER ATTACK METHODS ON SCADA

Attack coverage using Cyber EU



Source: https://threatpost.com/dell-threat-report-claims-100-percent-increase-in-scada-attacks

Jean-Luc Danger, Adrien Facon, Sylvain Guilley, Karine Heydemann, Ulrich Kühne, Abdelmalek Si-Merabet, Michaël Timbert, Baptiste Pecatte: Processor Anchor to Increase the Robustness Against Fault Injection and Cyber Attacks. COSADE 2020: 254-274

A TWO-FOLD TECHNOLOGY

SECURE CALL

Anti-return address corruption

Protection perimeter:

- Stack smashing, via:
  - Buffer overrun
  - Integer underflow/overflow
  - Exploitation of signedness issue
- Return oriented Programming (ROP)

CCFI

Fine-grained code & control flow integrity

Protection perimeter:

- Same as Secure CALL, plus:
- Jump oriented Programming (JOP)
- Indirect and direct call/jump in an illicit location
- Code injection, overwriting, data/code confusion
- RowHammer
- Glitch to skip an instruction or replace an instruction by another

A TWO-FOLD TECHNOLOGY

SECURE CALL

Anti-return address corruption

Execution time impact	0%
Hardware impact	12k generic gates
Code memory fingerprint impact	0%
Need code recompilation/modification	NO

CCFI

Fine-grained code & control flow integrity

Execution time impact	~ 1%
Hardware impact	12k generic gates + ICache size
Code memory fingerprint impact	2 times code size
Need code recompilation/modification	YES

Protection	W⊕X	SOFIA [3]	Intel CET [13]	ARM PA	PICON [2]	HCODE [4]	PathArmor [14]	HCFI [15]	Our solution
a) Inter Procedural	✗	✓	✓	✓	✓	✗	✓	✓	✓
b) Intra Procedural	✗	✓	(✓)	✗	✓	✓	✗	✗	✓
c) Intra BB	✗	✓	✗	✗	✗	✓	✗	✗	✓
d) Code Integrity	✓	✓	✗	✗	✗	✓	✗	✗	✓
e) Non-intrusive	✗	✗	✗	✗	✓	✓	✓	✗	✓
f) Speculative Exec.	✓	(✓)	✓	✓	✓	✗	?	✓	✓
g) Interruption	✓	✗	✓	✓	✓	✗	?	(✓)	✓

HW-ENABLED CYBER-SECURITY

FEATURES

- **No processor modification** / **No toolchain modification**
- Agnostic for the program
- Real-time detection – no latency as for SW solutions
- Resilient to cyber-attacks because inaccessible to hackers and to advanced FIA such as EMFI

DEPLOYED ON RISC-V

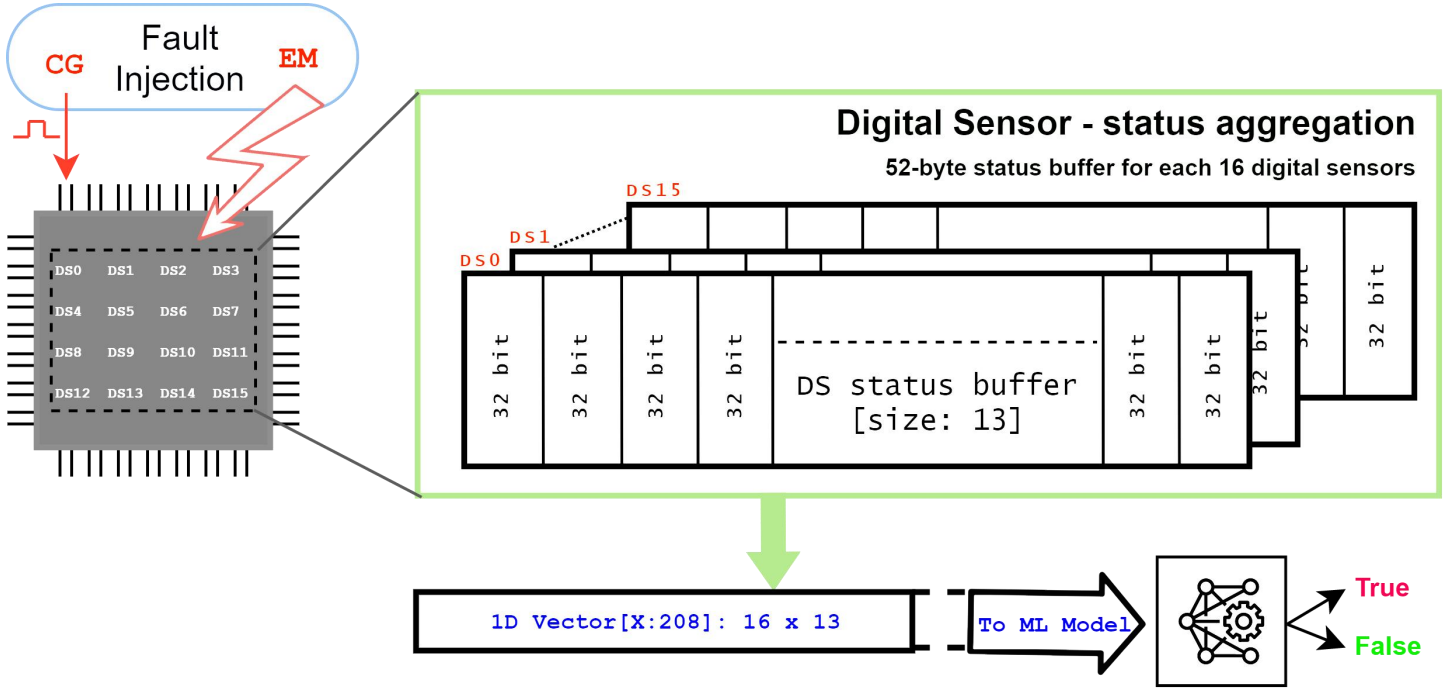
- Open ISA, clean design
- More secure by design (backward compatibility & interferences)
- Possibility to do formal verification
- Can be customized (constant-time, constant-leakage, etc.)

SECURE-IC
THE SECURITY SCIENCE COMPANY

3. AGGREGATION

SMART MONITOR (SM) FOR AGGREGATION

- Multiple Fault Sources
- Array of Digital Sensors (DS) distributed on the target chip
- Aggregating all DS status
- Experimentation to collect normal condition and fault injection condition datasets
- Using this data for training the SM before deployment

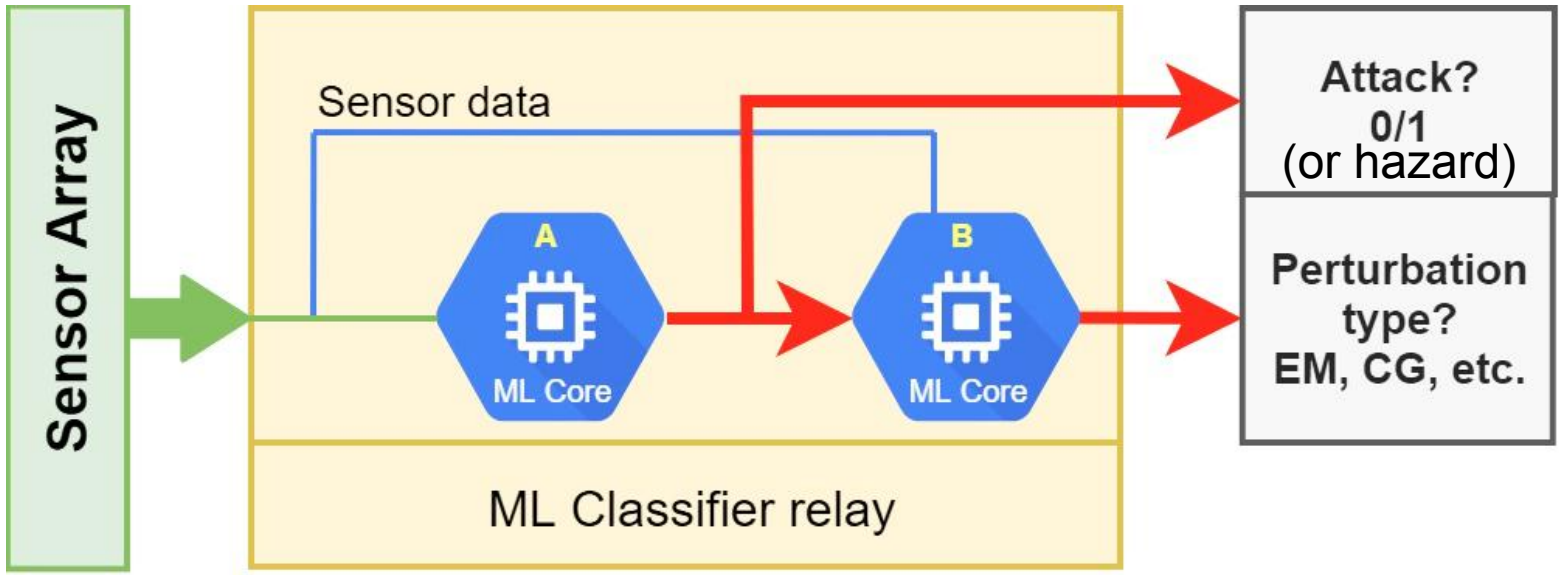


A. Facon, S. Guilley, X. Ngo and T. Perianin, "Hardware-enabled AI for Embedded Security: A New Paradigm," 2019 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), 2019, pp. 80-84, doi: 10.1109/SIGTELCOM.2019.8696136.

SMART MONITOR (SM) FOR TWO STAGES DETECTION

61508		26262	Diagnostic Metric
SIL 1	60%	ASIL A	No minimum
SIL 2	90%	ASIL B	90%
----	----	ASIL C	97%
SIL 3	99%	ASIL D	99%
SIL 4	99%	---------	------

- Increased response time (classification broken down in steps)
- Stage 1 to detect presence of attack (most important)
- Stage 2 to detect type of perturbation (for forensics / analysis purpose)



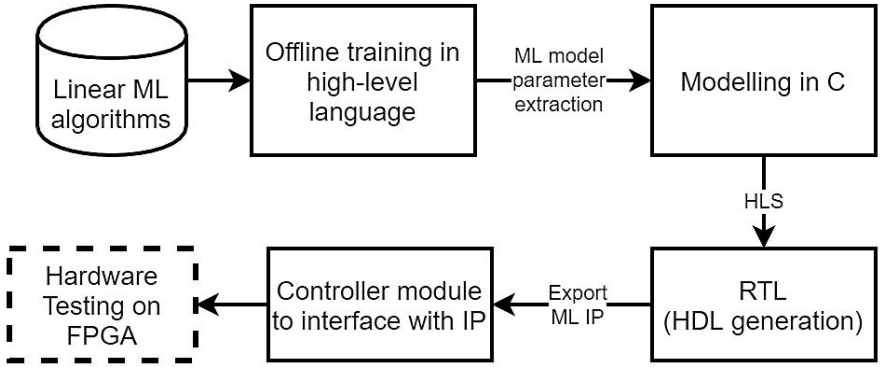
ISO/SAE 21434

Road Vehicles - Cybersecurity engineering

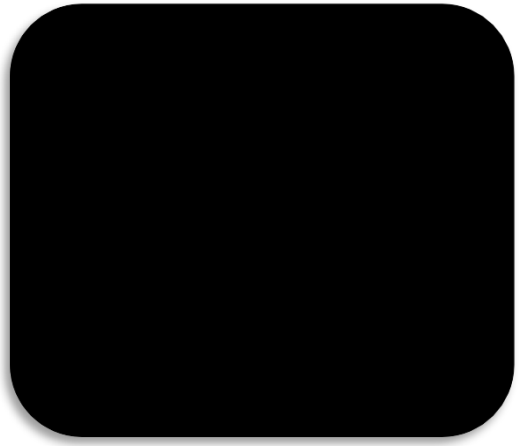
"Multi-Source Fault Injection Detection using Machine Learning and Sensor Fusion", Ritu-Ranjan Shrivastwa, Sylvain Guilley and Jean-Luc Danger.
2nd International Conference on Security & Privacy (ICSP). Jamshedpur, India. Springer. November 16-17, 2021.

HLS-BASED HARDWARE EVALUATION

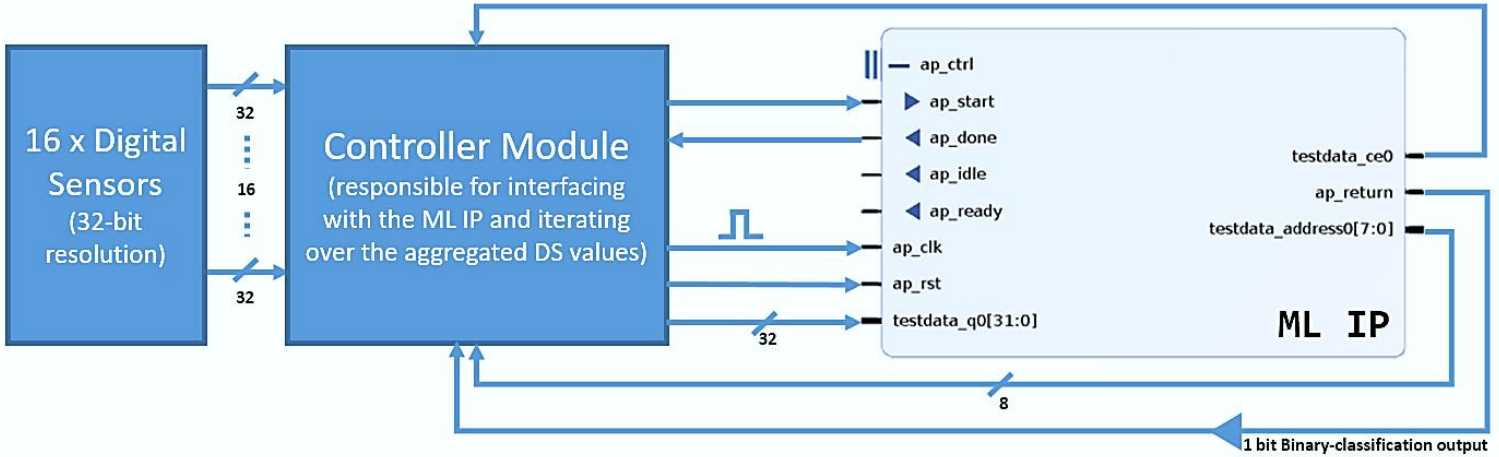
- Prototype using HLS
- Single-stage example interfaced with the controller module
- Benchmark accuracy test on hardware platform
- Standard interfacing across different ML modules
- Easy integration and controlling with a separate Aggregation and control unit



Framework flow-chart



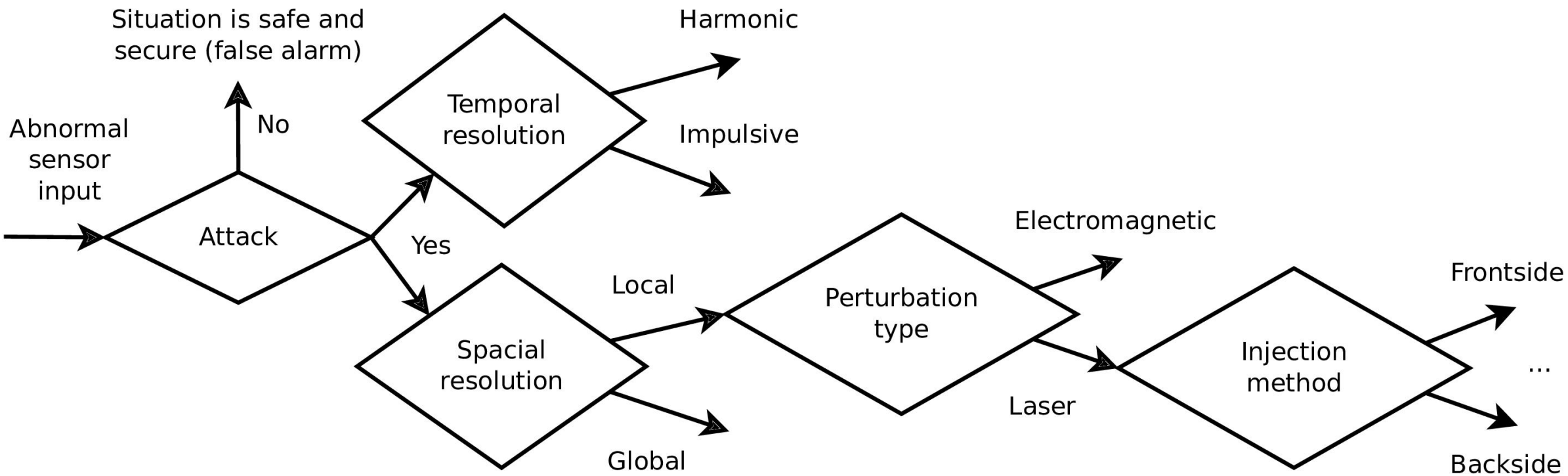
Target evaluation platform



Smart Monitor IP interfacing with Aggregation and Control Unit

SMART MONITOR

- **Refined ontologies and CC evaluation assurance levels**



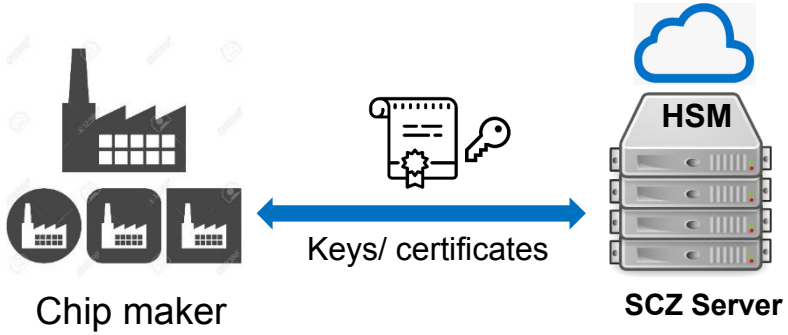
Paolucci F. et al. (2021) Industrial Cyber Security at the Network Edge: The BRAINE Project Approach. In: Colla V., Pietrosanti C. (eds) Impact and Opportunities of Artificial Intelligence Techniques in the Steel Industry. ESTEP 2020. Advances in Intelligent Systems and Computing, vol 1338. Springer, Cham. https://doi.org/10.1007/978-3-030-69367-1_10

SECURE-IC
THE SECURITY SCIENCE COMPANY

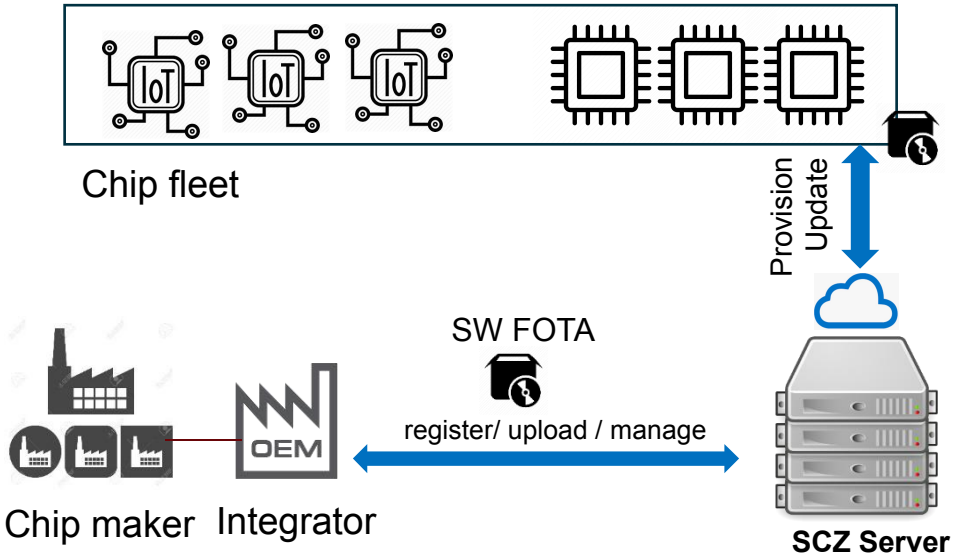
4. CHIP TO CLOUD REPORTING

SECURYZR SERVER MAIN SERVICES

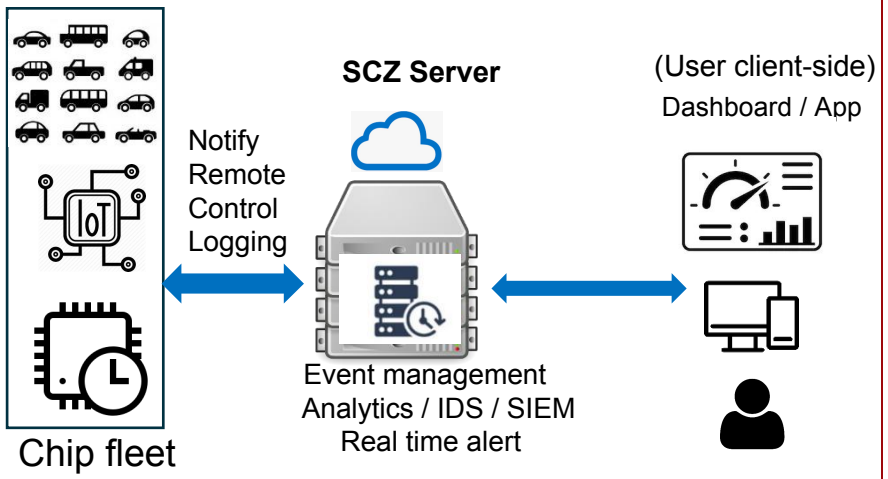
- Main Services



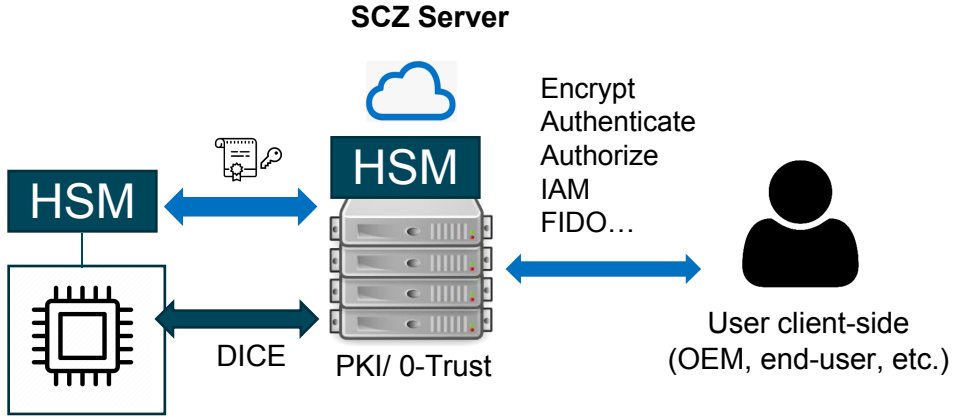
Key Provisioning



SW Management



Monitoring

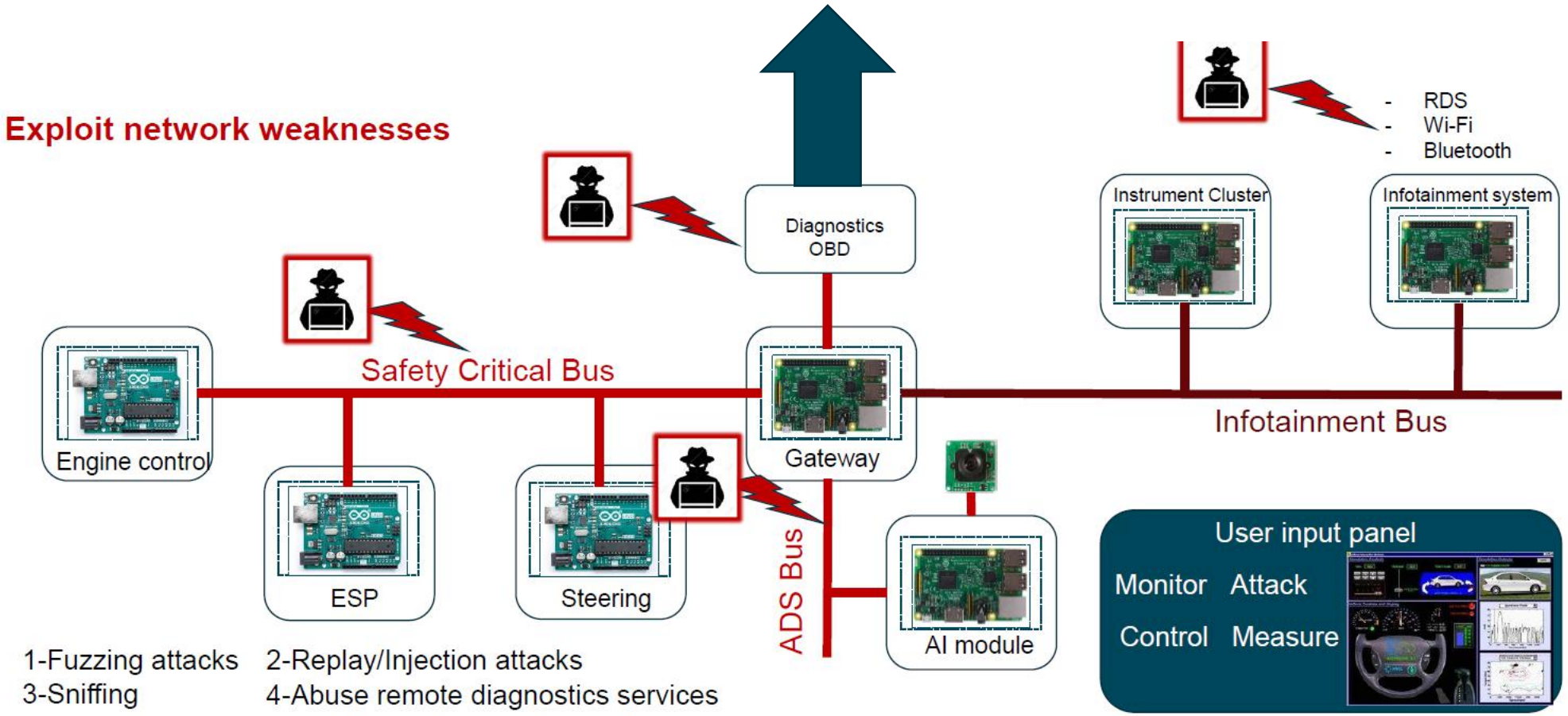


Digital Authority

ADVANCED SAAS APPLICATIONS (AUTOMOTIVE)

On-board IDS to Cloud (SCZ Server)

"Security and/or Safety as a Service"



SECURE-IC
THE SECURITY SCIENCE COMPANY

5. CONCLUSION

ATTACK DETECTION TECHNOLOGUES

ATTACK TYPE	ATTACK	SECURE-IC ATTACK DETECTION IP
ACTIVE (local)	Temperature	**DIGITAL SENSOR** **CYBER EU**
	Electromagnetic Injection (EM)	
	Clock Glitch	
	Power Glitch / Underfeeding	
	Laser Injection	
INVASIVE (local)	Focused Ion Beam	**ACTIVE SHIELD**
	Probing	
SW/CYBER (remote)	Code Injection	**CYBER EU + RISC-V**
	Buffer Overflow	
	Stack Smashing	
	Control Flow Graph Hijacking	
	0-day attacks targeting SW execution	
	Firmware tampering	**SECURE-BOOT**
	Row-Hammer Attacks	**ANTI-ROW HAMMER**
SW (local)	JTAG Violation	**SECURE DEBUG**

→ **Securyzr Server™ to report to Remote Cloud application**

SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com