HUAWEI

GLOBAL SOFTWARE TECHNOLOGY SUMMIT 2024

Model-based Design and Verification and CyberSecurity Solutions for Automotive and Digital Power

Sergio Saponara, Gianluca Dini

Dipartimento Ingegneria della Informazione (DII), Università di Pisa

3rd July 2024

SPEAKER'S BIO: SERGIO SAPONARA

sergio.saponara@unipi.it, +39 3468790937, https://www.linkedin.com/in/sergio-saponara-3031431/

- **Director elected of Dipartimento Ingegneria Informazione** https://www.dii.unipi.it/
- **Full Professor** at UniPI for *HW and Embedded Security, Vehicular Electronics, Electronic Systems for Robotics, Design of IoT Systems*
- **Spoke leader** *Multiscale Modeling&Engineering,* **Italian Center for Super Computing** https://www.supercomputing-icsc.it/
- **President** BSc and MS degrees in Electronic Engineering
- **Advisor** of the Italian Government (MUR) for the Chips Act
- **Director** Summer School "Enabling Technologies for IoT"
- **Director** Specialization Course "Automotive Electronics and Powertrain Electrification"
- **Delegate** for technology transfer of DII (Dipartimento Ingegneria della Informazione)
- **Delegate** for UniPI in EERA (European Energy Research Alliance
- **Director** of UCAR (interUniversity Center for Automotive Research)
- **Steering committee** member of **European Processor Initiative (EPI),** Movet (Motor, Vehicles, Tec.)
- Associate member of INFN, CNIT, CINI; of European Institute for Science, Media, Democracy and FWO (Flanders Science Foundation)
- PI for UniPI in EU projects AERO*, EUTRAINS, Textarossa, The European Pilot*, *EPI SGA1*, *EPI SGA2*, *Athenis3D, Hiefficient, Cost PED,…*
- ***IEEE distinguished lecturer*** *and co-founder of IoT SIG of IEEE SP and CAS societies*
- *400 publications indexed in Scopus/WoS, Hindex 34 and 5000 + 24 patents with UNIPI and CNR, INFN, Marelli, Ericsson, ST*
- ***Marie Curie Research Fellow*** *in IMEC, Leuven in 2002*
- *MS in Electronic Engineering in 1999 and PhD in Information Engineering in 2003 (STM PhD grant)*

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

Department of Excellence

Pisa-via Caruso

https://www.dii.unipi.it/
https://crosslab.dii.unipi.it/
https://forelab.unipi.it/

DII DEPARTMENT OF EXCELLENCE BY MUR

X RESEARCH, HIGHER EDUCATION & TECH TRANSFER

(20 M€ EXTRA BUDGET AWARD, 2018-2022 AND 2023-2027)

3 SITES: PISA-VIA CARUSO, PISA- VIA DIOTISALVI, NAVACCHIO-POLO TECNOLOGICO

DII EXPERTISE

- AI & HPC
- ELECTRONICS & IC
- TELECOMMUNICATION & REMOTE SENSING
- CYBERSECURITY & COMPUTER ENGINEERING
- ROBOTICS
- BIOENGINEERING
- ELECTROMAGNETICS

SOME PROJECTS

- EPI1, EPI2
- TEXTAROSSA
- EUPEX
- EUPILOT
- ADMIRE
- AERO
- HIEFFICIENT
- PNRR HPC 6 MOBILITY

HW AND SW SOLUTIONS FOR VEHICULAR CYBERSECURITY

1) Secure FOTA (Firmware Over The air) update with Post-Quantum Cryptography (PQC) signature (on RISC-V plus SHAKE accelerator)

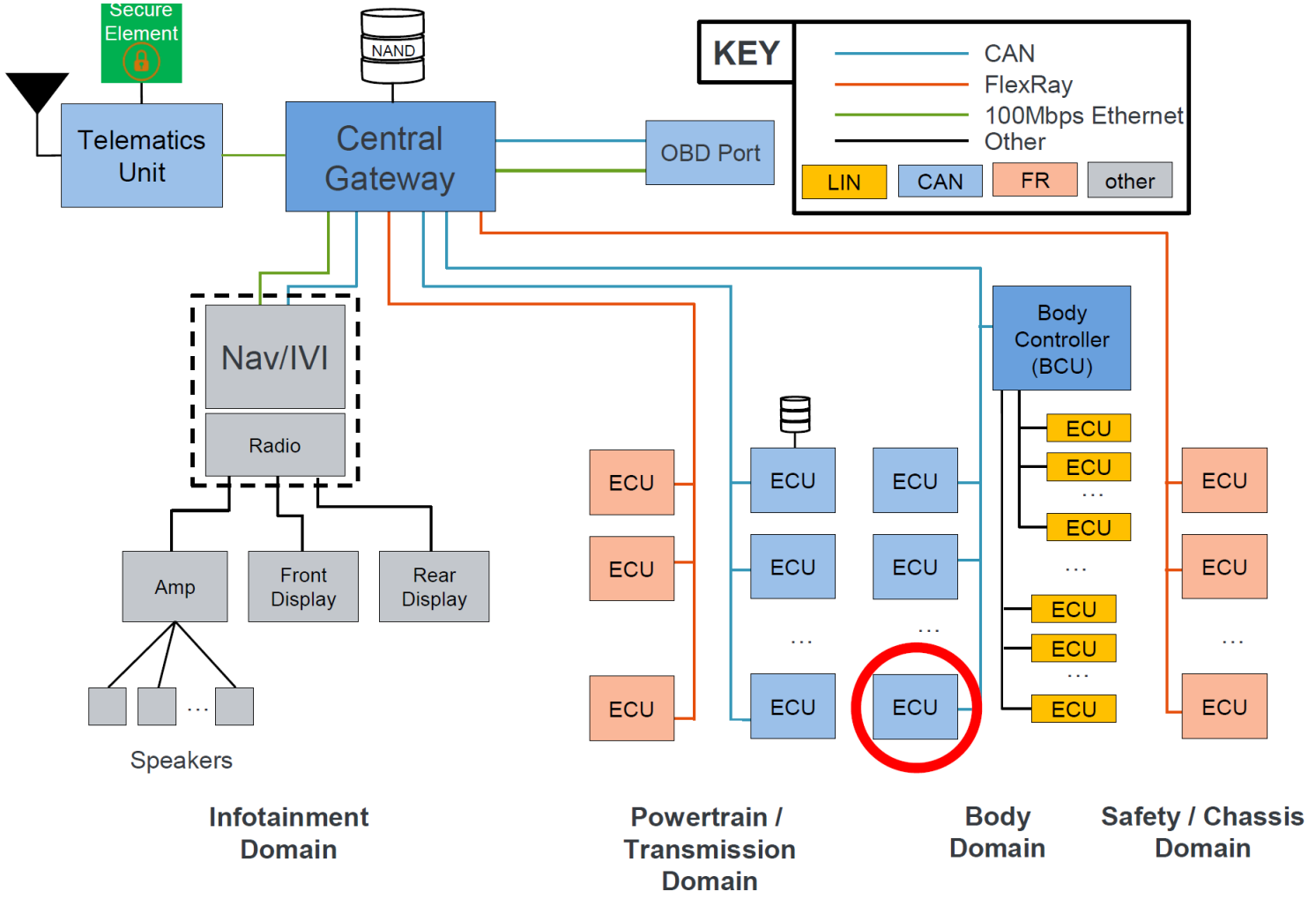
2) Anomaly, Intrusion Detection & Fingerprint

3) SEAL-Embedded Homomorphic Encryption library for user's privacy

4) HSM (HW Security Module) for the European Processor Initiative

5) Hacking Keyless Entry System

VEHICULAR CONNECTIVITY CYBERSECURITY ISSUES

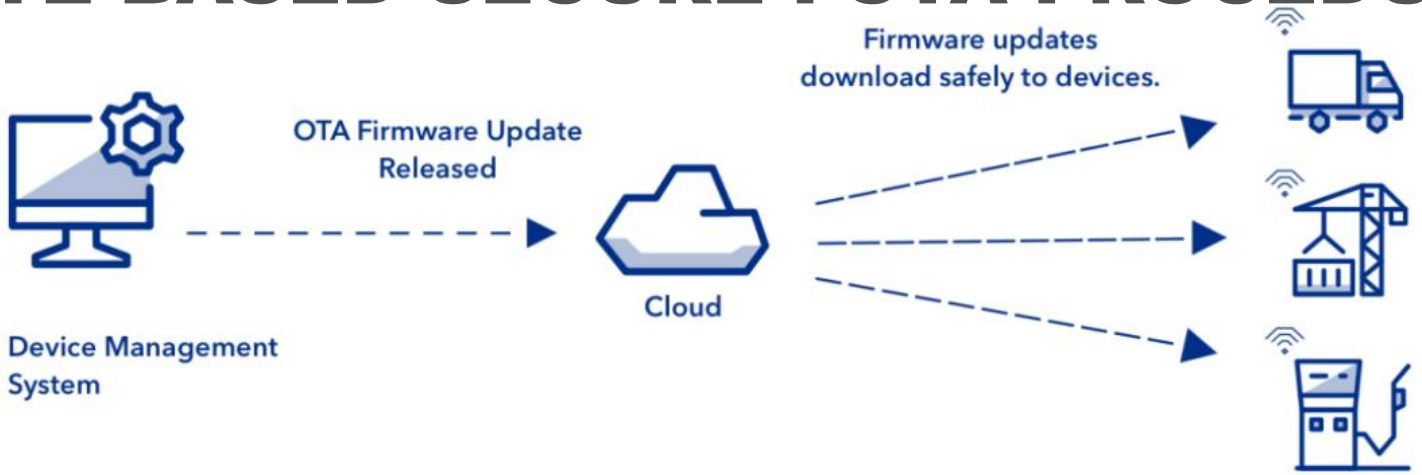


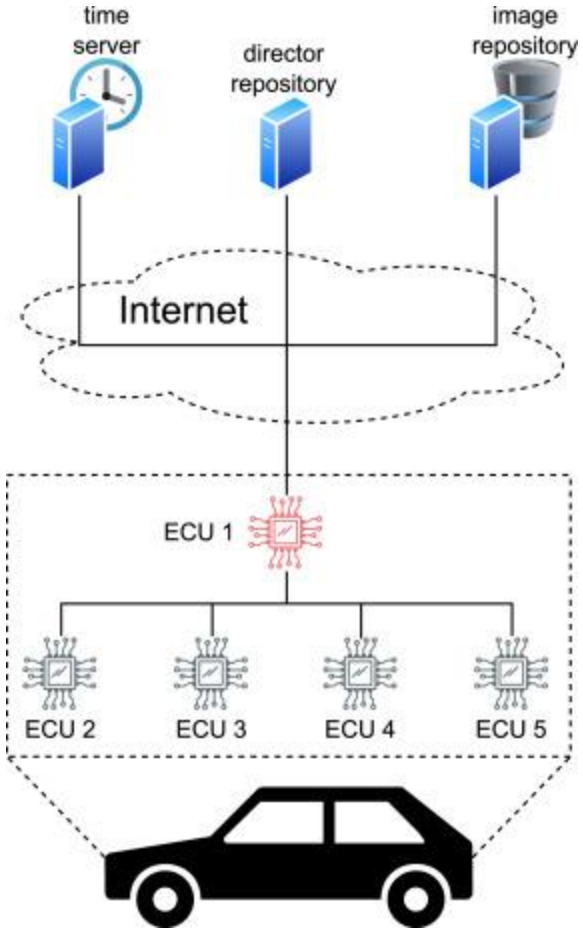
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

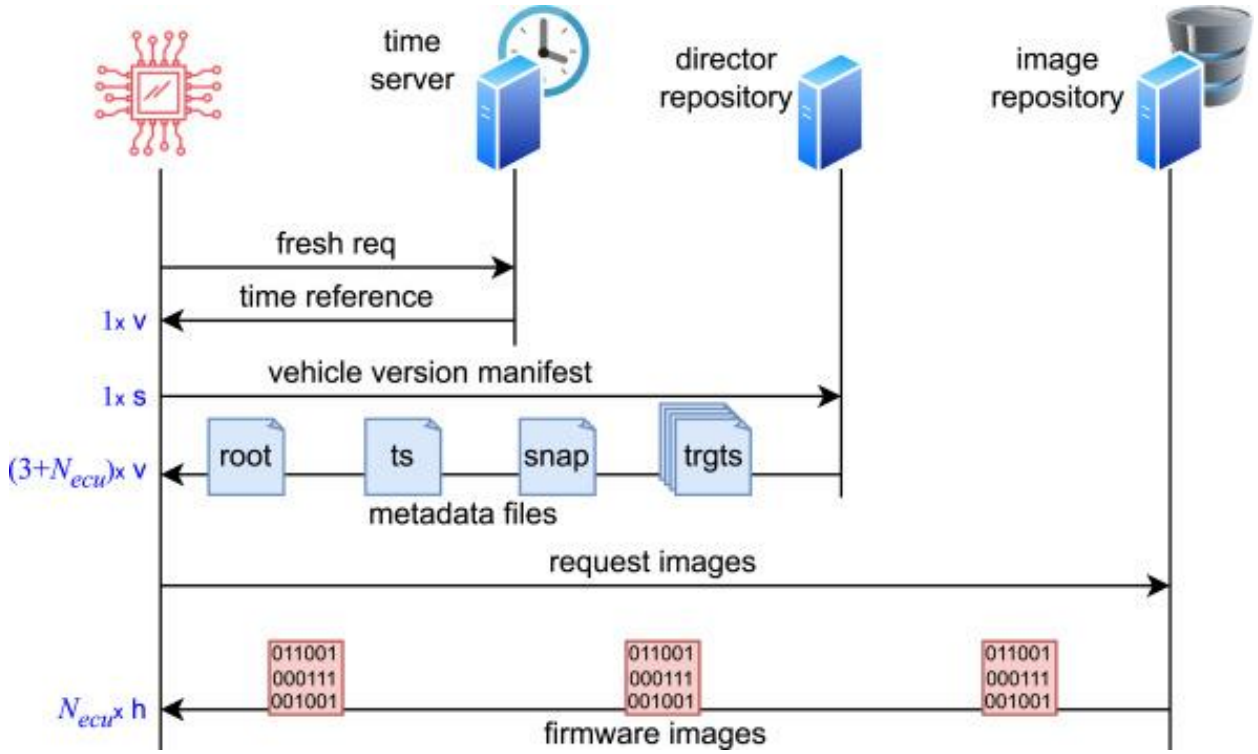
https://www.youtube.com/watch?v=krSj81thN0w

CANSECWEST 2021: Tbone Drone vs Tesla - Ralf-Philippe Weinmann & Benedikt Schmotzle, Comsecuris

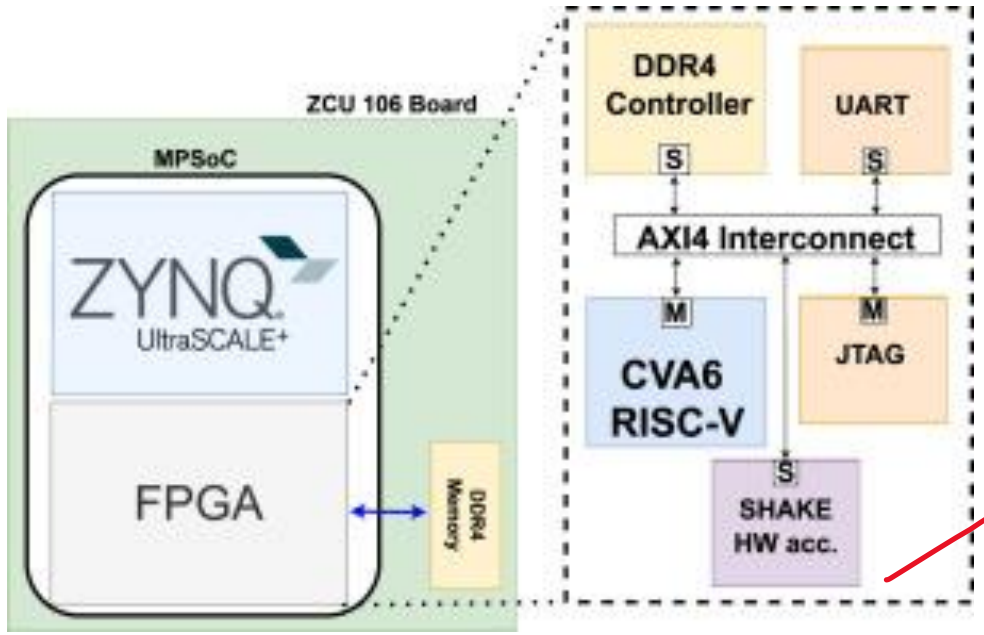
ATTRIBUTE-BASED SECURE FOTA PROCEDURE

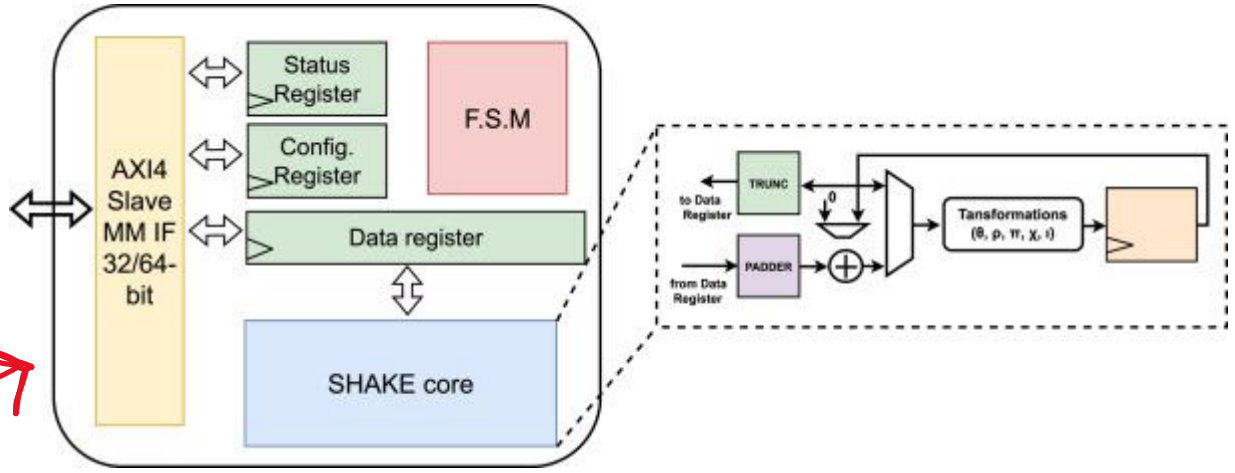


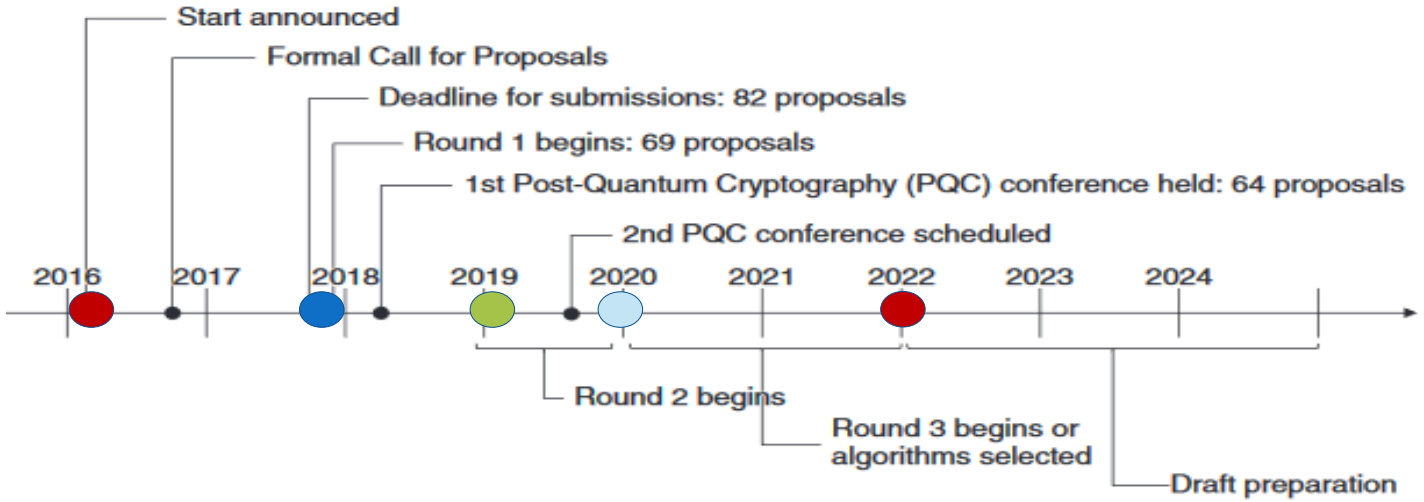




SECURE FOTA WITH POST-QUANTUM-CRYPTO







NIST standardized Crystals-Kyber and Dilithium for PQC for hash and public-private key crypto

HW acceleration → x10 speed-up

Crystals-Dilithium 5 with SHAKE	RISC-V 64b CVA6 [ms]	
	SW-only	SW/HW
100 KiB	86.47	8.12
500 KiB	432.13	40.49
1 MiB	884.96	82.92
5 MiB	4142.50	414.28
10 MiB	8848.53	828.56
100 MiB	88,483.49	8289.25

HW AND SW SOLUTIONS FOR VEHICULAR CYBERSECURITY

1) Secure FOTA (Firmware Over The air) update with Post-Quantum Cryptography (PQC) signature

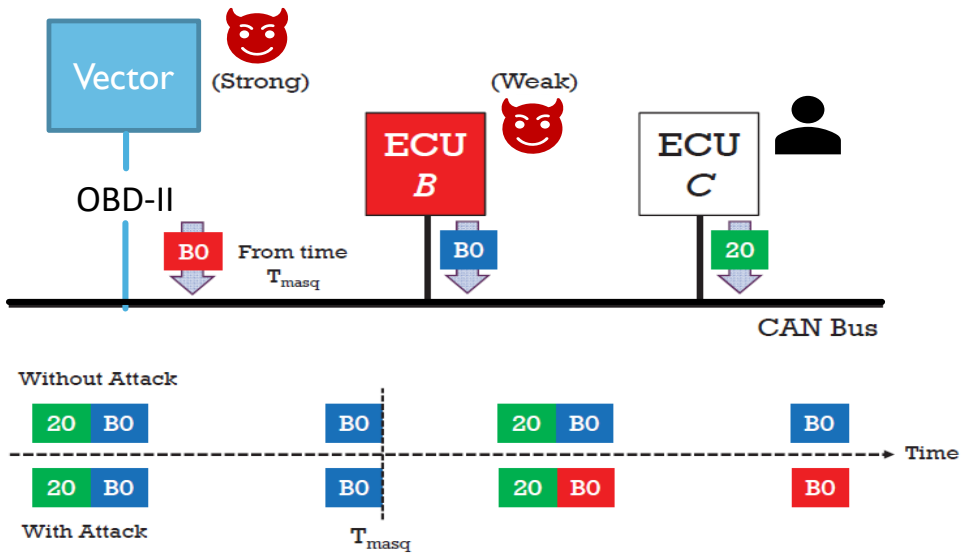
2) Anomaly, Intrusion Detection & Fingerprint

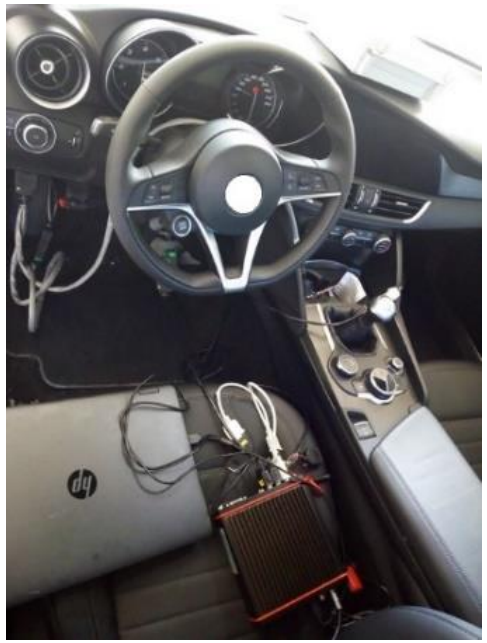
3) SEAL-Embedded Homomorphic Encryption library for user's privacy

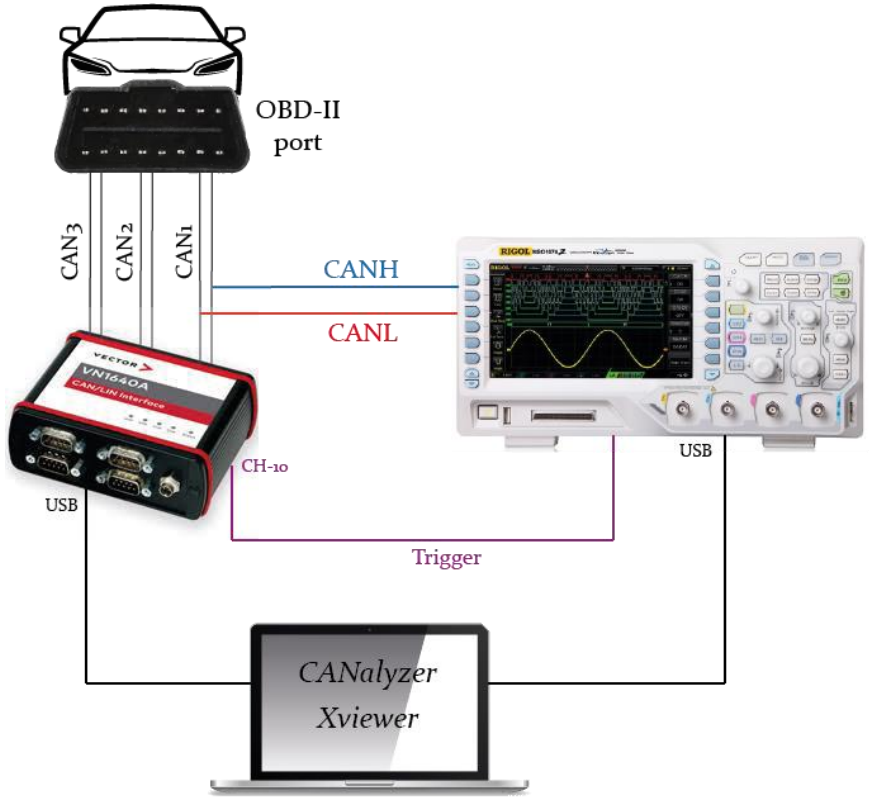
4) HSM (HW Security Module) for the European Processor Initiative

5) Hacking Keyless Entry System

INTRUSION DETECTION & FINGERPRINTING







UNIVERSITÀ DI PISA

MARELLI

3 SW techniques developed and ported on embedded platform- Collaboration with Marelli

- Voltage and time physical features on CAN/CAN-FD extracted and analysed with AI (CNN) and statistical algorithms
- Ported on NXP S32K1xx and Infineon TC39xx, experiments with Giulia Alfa Romeo car

INTRUSION DETECTION & FINGERPRINTING

Fusion in a multi-feature IDS: message-based IDS + time and voltage fingerprinting

4 patents Marelli-UniPI (2 also US-EU-China patents)

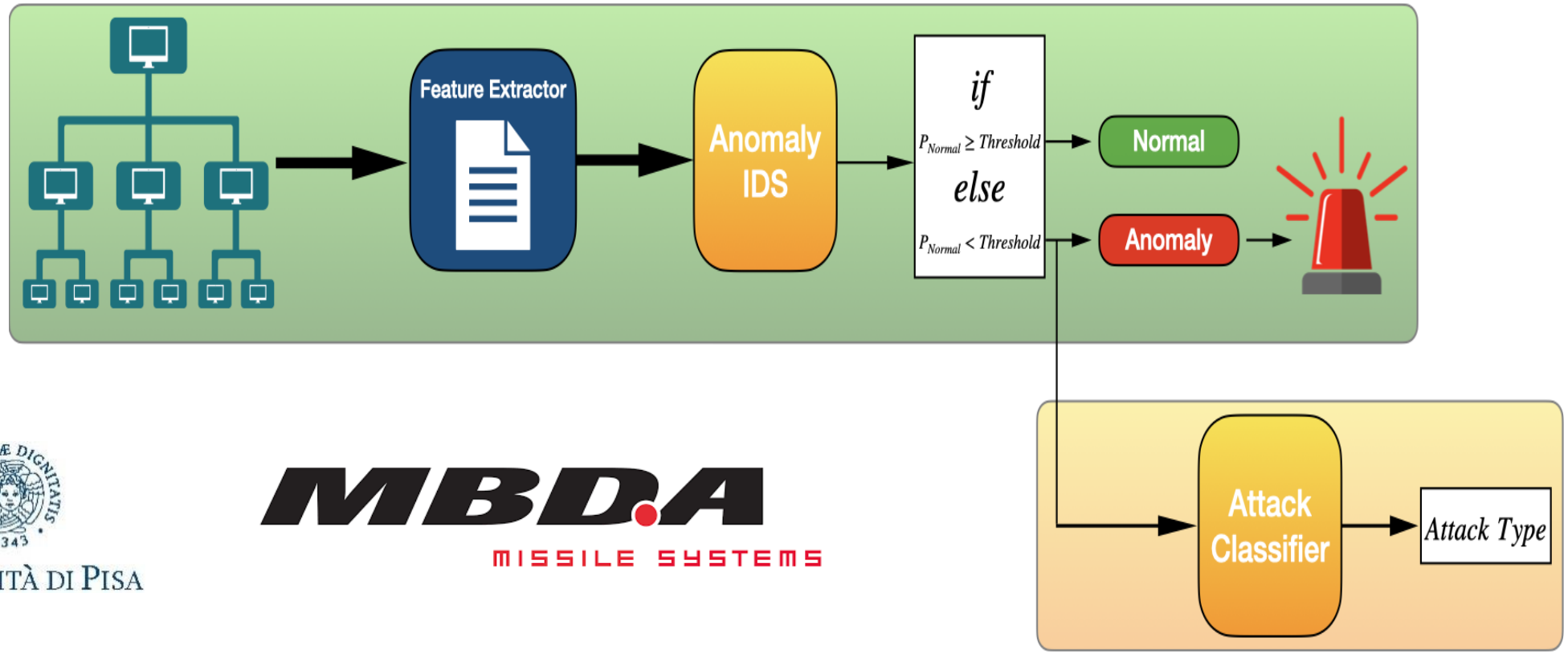
https://patents.google.com/patent/EP4096168A1/en
https://patents.google.com/patent/CN115412278A/en
https://patents.google.com/patent/US20220394045A1/en
C. ROSADINI, A. CORNELIO, S. CHIARELLI, W. NESCI, S. SAPONARA, E. DE PINTO

https://patents.google.com/patent/EP4096169A1
https://patents.google.com/patent/US20220407880A1/en
https://patents.google.com/patent/CN115412279A/en
C. ROSADINI, A. CORNELIO, W. NESCI, S. SAPONARA, A. GAGLIARDI, P. DE CESARE

UNIVERSITÀ DI PISA

MARELLI

ANOMALY & INTRUSION DETECTION



UNIVERSITÀ DI PISA

MBDA MISSILE SYSTEMS

1 technique: Network traffic features on TCP/IP networks extracted and analysed with AI (Autoencoder + decision tree classifier) and tested vs SNORT for defense applications (MBDA). To be used in parallel to rule-based IDS like SNORT

HW AND SW SOLUTIONS FOR VEHICULAR CYBERSECURITY

1) Secure FOTA (Firmware Over The air) update with Post-Quantum Cryptography (PQC) signature

2) Anomaly, Intrusion Detection & Fingerprint

3) SEAL-Embedded Homomorphic Encryption library for user's privacy

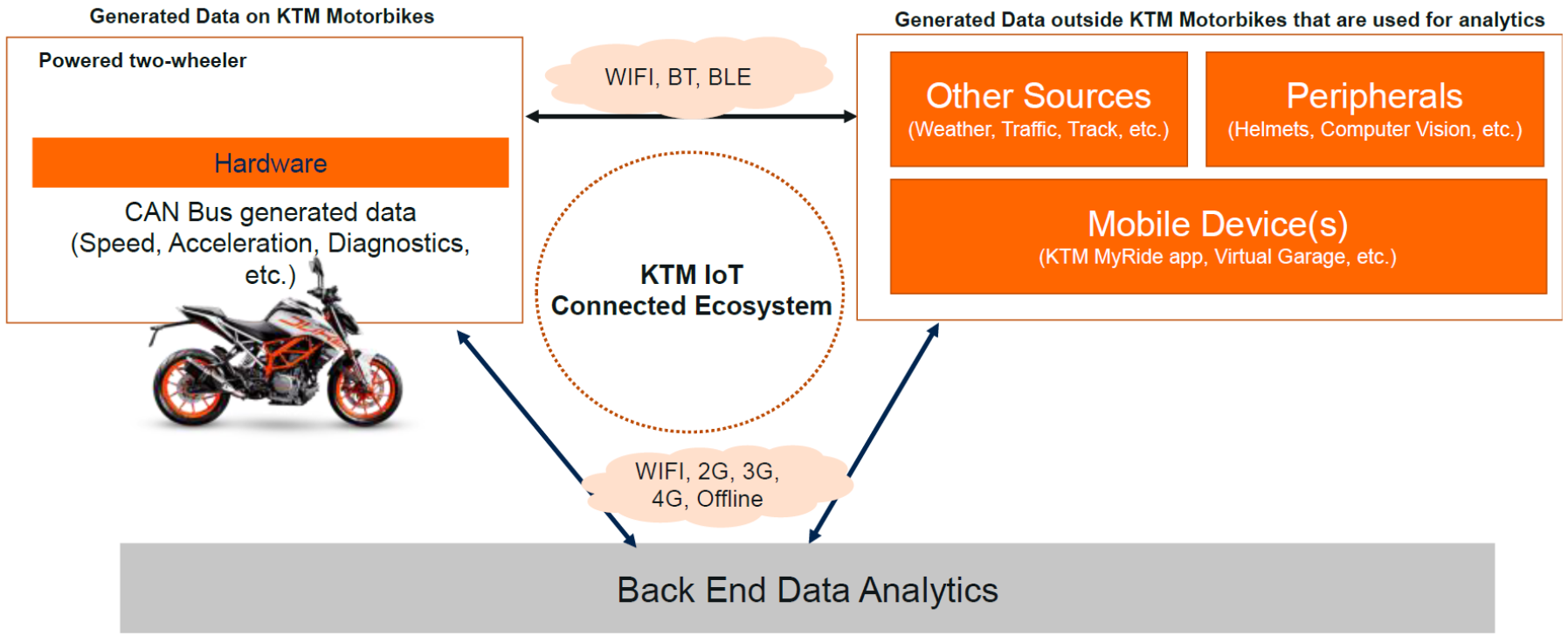
4) HSM (HW Security Module) for the European Processor Initiative

5) Hacking Keyless Entry System

HOMOMORPHIC ENCRYPTION

- Useful to guarantee privacy of users' data in Cloud services

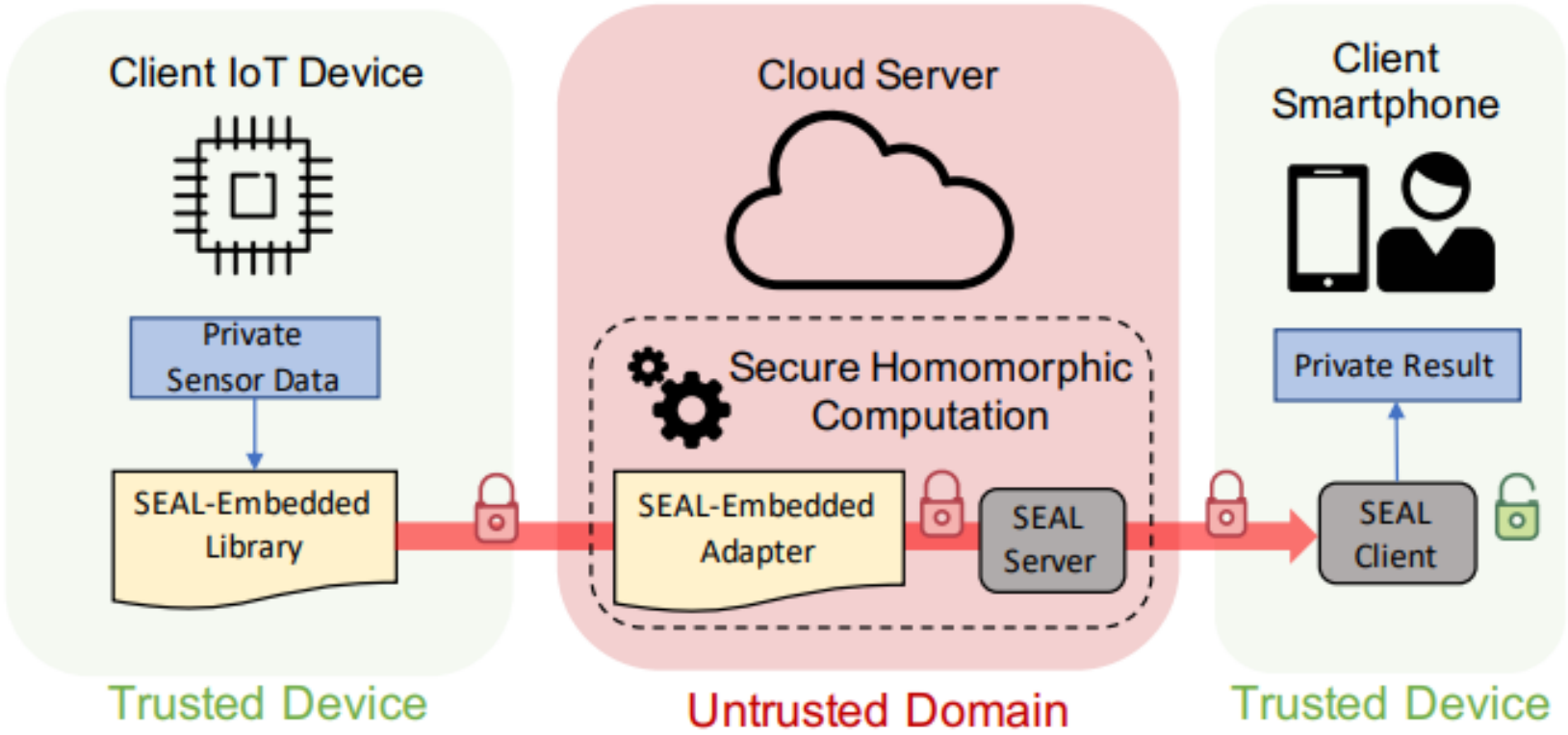
- Computations (data sorting, ranking, thresholding, add, mul…) on data kept encrypted at cloud side with the same results of classic decrypted data → Third-party cloud services can be used while keeping secrets of edge customers/users



HOMOMORPHIC ENCRYPTION

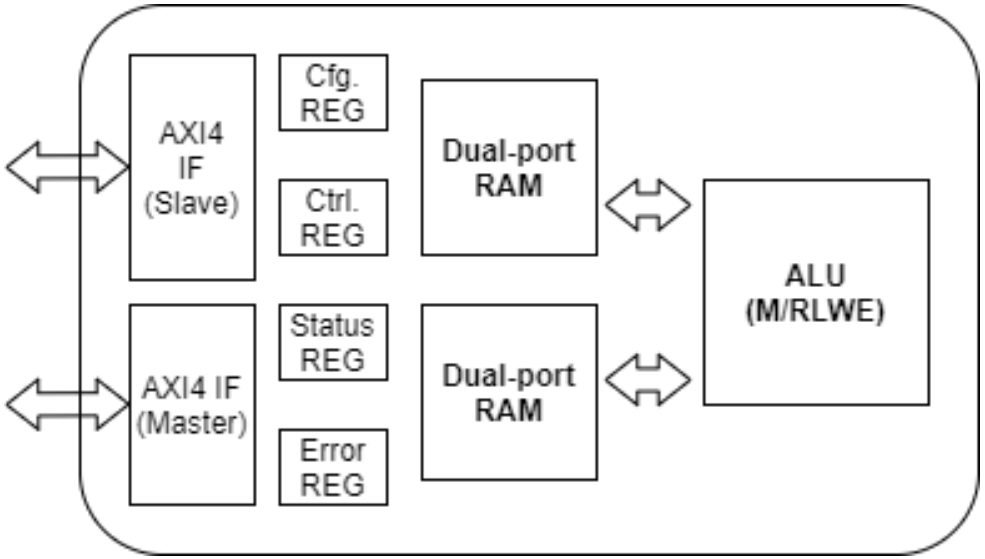
- UNIPI developed a mixed HW-SW implementation of the Microsfot SEAL Full-Homorphic-Encryption (FHE) library both at Edge (SEAL embedded) and cloud side

- Idea is extending the Crypto-tile IP to support in HW the computing intensive primitive of the SEAL FHE library



FPGA USE CASE: SEAL-EMBEDDED HOMOMORPHIC ENCRYPTION LIBRARY

- Microsoft SEAL-Embedded library: Spin-off of the Microsoft SEAL library
- Homomorphic Encryption library for Edge devices (based on RLWE Lattice code)
- Only encryption fucntions: encrypted data are sent to the server that computes Homomorphic operations using the SEAL library
- Encryption on edge devices is slow: benchmark campaign on 64-bit RISC-V and 32-bit RISC-V CPUs



Polynomial Degree	Msg Size	SW (ms)	HW (ms)	HW DMA (ms)
1024	2048 B	168.35	7.84	0.142
2048	4096 B	364.53	15.68	0.297
4096	8192 B	2352.74	93.72	1.866
8192	16384 B	10032.13	374.83	7.79
16384	32768 B	45856.85	1624.12	35.19

HW AND SW SOLUTIONS FOR VEHICULAR CYBERSECURITY

1) Secure FOTA (Firmware Over The air) update with Post-Quantum Cryptography (PQC) signature

2) Anomaly, Intrusion Detection & Fingerprint

3) SEAL-Embedded Homomorphic Encryption library for user's privacy

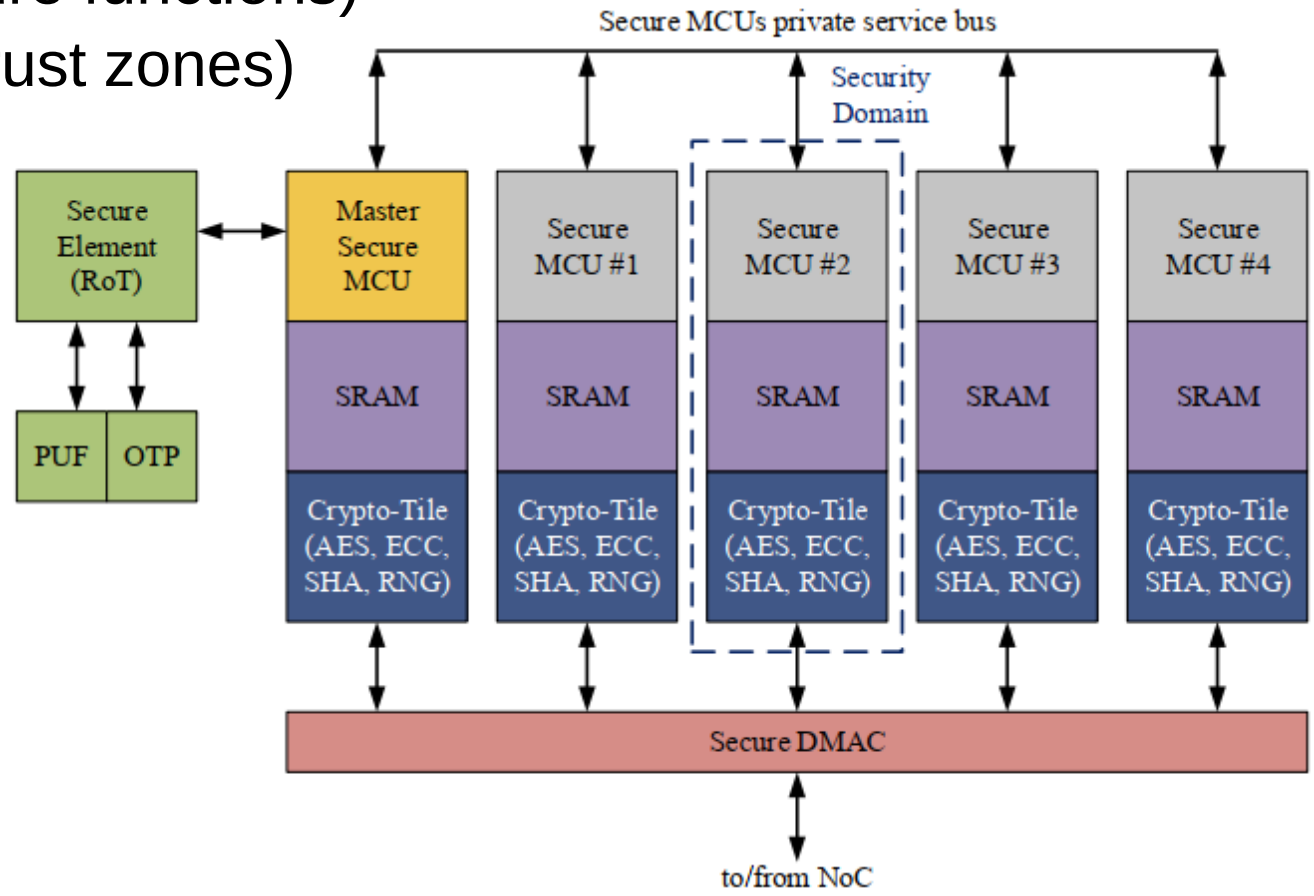
4) HSM (HW Security Module) for the European Processor Initiative

5) Hacking Keyless Entry System

HSM IN EUROPEAN PROCESSOR INITIATIVE

Multiple Security Domain

- MCU running secure SW (Linux-kernel)
- Dedicated RAM (key storage)
- Crypto-Tile (HW-accelerated secure functions)
- Independent Security Domains (trust zones)



DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

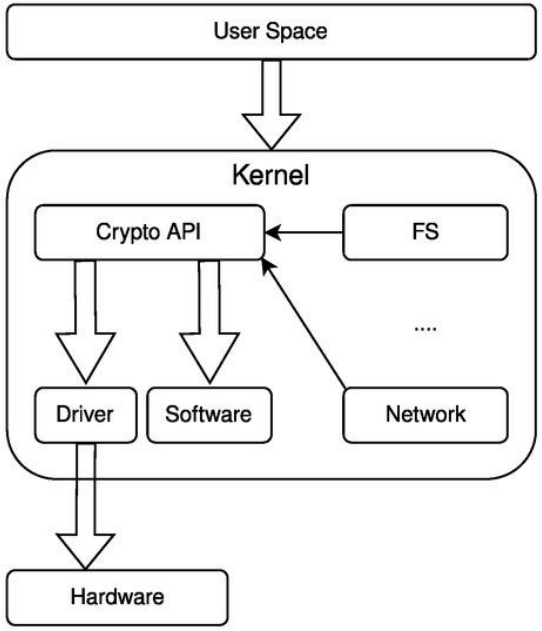
IN SUPREMÆ DIGNITATIS 1343

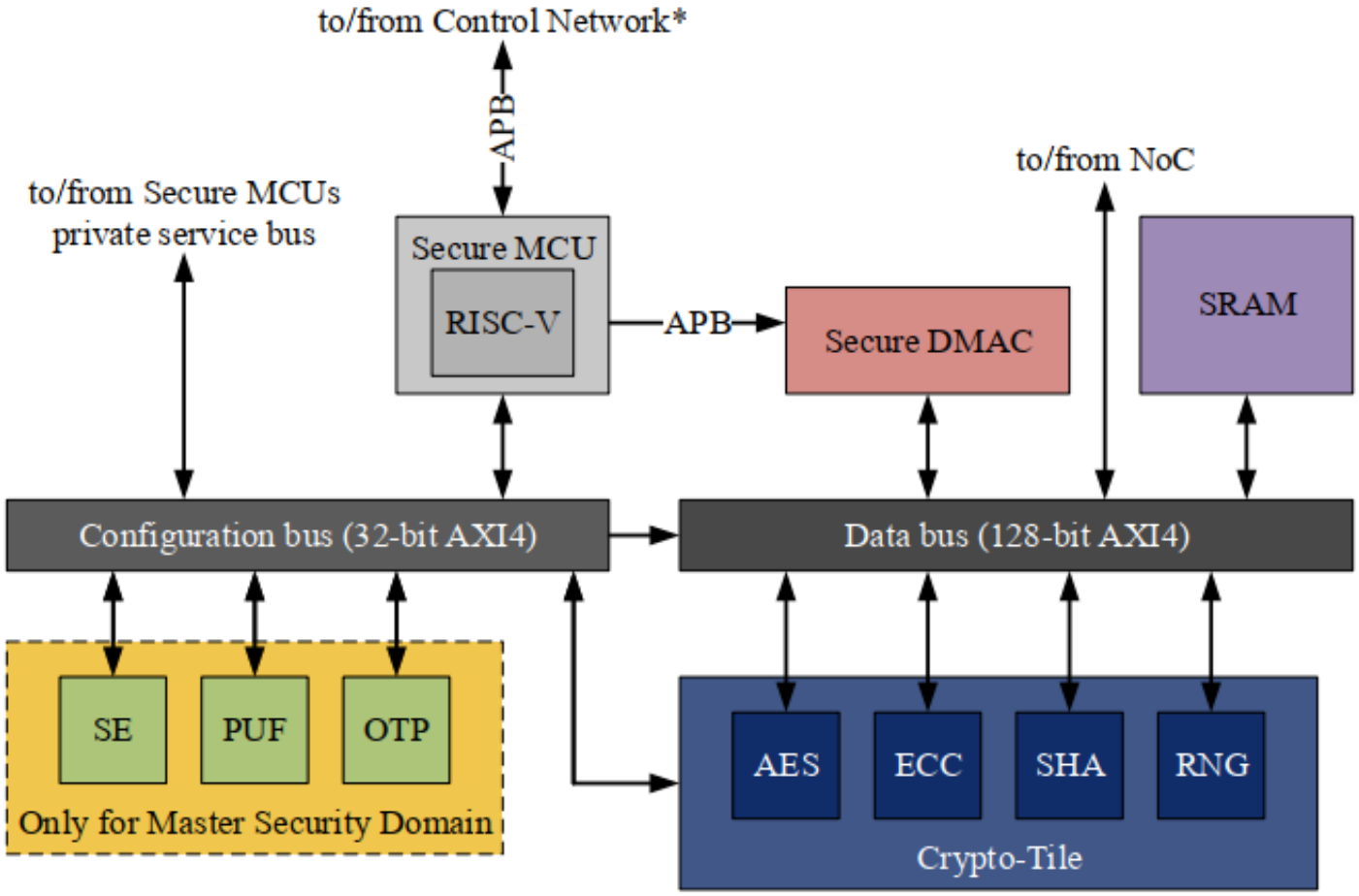
SIPEARL The Silicon Pearl

PROGRAMMABLE SECURE TILE

Bare-metal SW functions +

Linux Kernel running on RISC-V core with specific driver for HW accelerated crypto





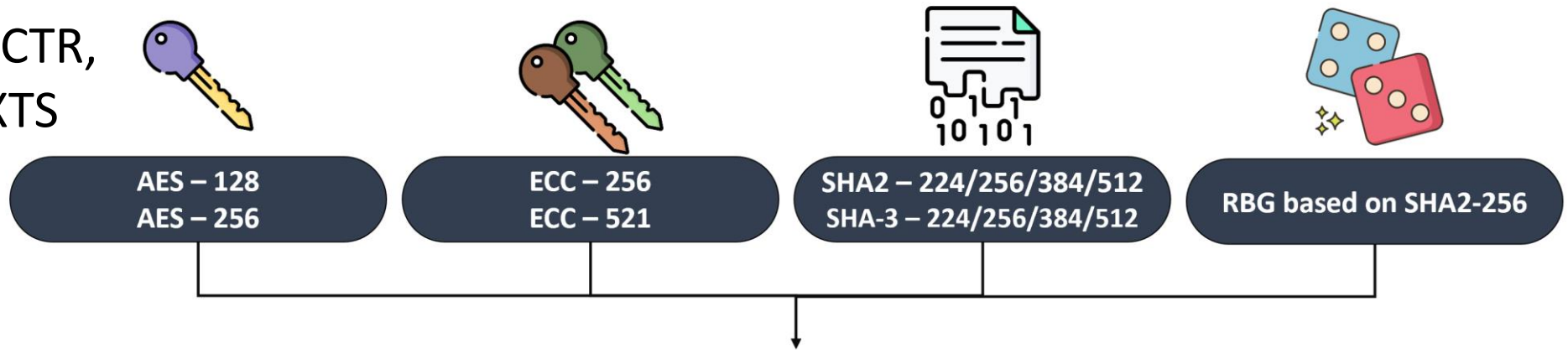
64b RISC-V IP (secure diversity vs Rhea ARM application processor) + Crypto-Tile suite of many HW-accelerated secure IPs

UNIPI prototypes: Secure tile in VCU128 FPGA, Cryptotile IP with ARM CortxA-53 in ZCU106

CRYPTOTILE HW SECURE PERFORMANCE

9 AES modes:

ECB, CBC, CFB, OFB, CTR,
CMAC, CCM, GCM, XTS



Accesses restrictions

- Seal/Unseal mechanisms
- Restriction on key material
- Privilege Levels: Supervisor/User
- Debug access can be fully disabled
- Report of unauthorized accesses (error flags)

Panic mechanism

FSM to regulate usage of Cryptographic Operations

- Strict rules to move among the states
- Restriction on data access basing on state

“**Halt & Resume” mechanism**

Multi-layer secure boot strategy

SCA countermeasures

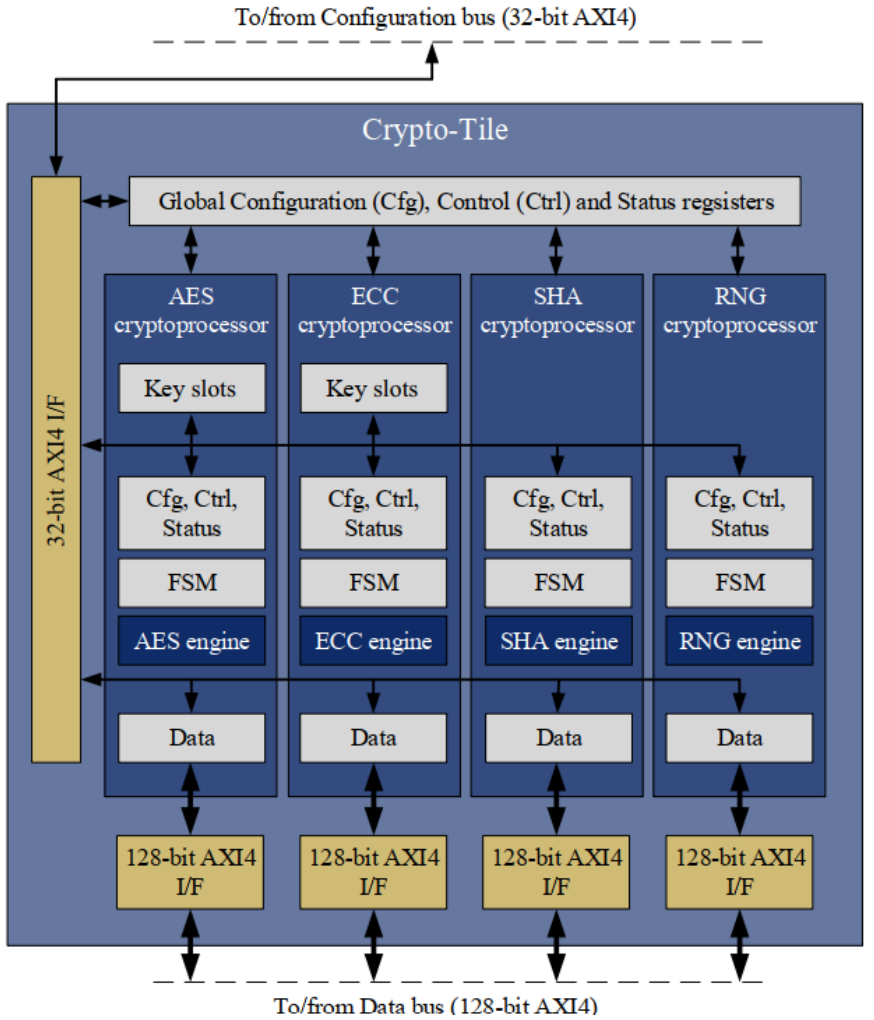
- Clock randomization: increase post-processing timing and power analysis because traces require to be aligned
- Power Analysis resistance

TRNG (FiRo/Garo-based) assessed vs NIST EA & STS suite and BSI AIS 31 suite

CRYPTOTILE HW SECURE PERFORMANCE (ASIC)

Entity	Max. Frequency [GHz]	Area	
		Absolute [kGE]	Percent [%]
Crypto-Tile (top-level)	3.7	1325.16	100.0
AES engine	2.425	56.01	4.2
ECC engine	1.525	658.90	49.7
SHA engine	3.725	128.32	9.7
RNG engine	4.325	127.16	9.6

ARM Artisan 7nm logic kit (TSMC process)



128-b AES core in 4.54 ns: AES 28 Gbps @ 2.425 GHz

	This work	[233]	[234]
Technology node	7 nm	90 nm	65 nm
Supply Voltage	$0.9\ V$	$0.8\ V$	$1.2\ V$
Power consumption	$3834.6\ \mu W$	$55.2\ \mu W$	$6070\ \mu W$
Frequency	$2425\ MHz$	$100\ MHz$	$100\ MHz$
Latency (cc)	$11\ cc$	$499\ cc$	$12\ cc$
Latency (time)	$4.54\ \eta s$	$4.99\ \mu s$	$0.12\ \mu s$
Energy	$0.73\ pJ$	$0.28\ \eta J$	$0.73\ \eta J$
Energy efficiency	$5.75\ fJ/bit$	$2.15\ pJ/bit$	$5.69\ pJ/bit$

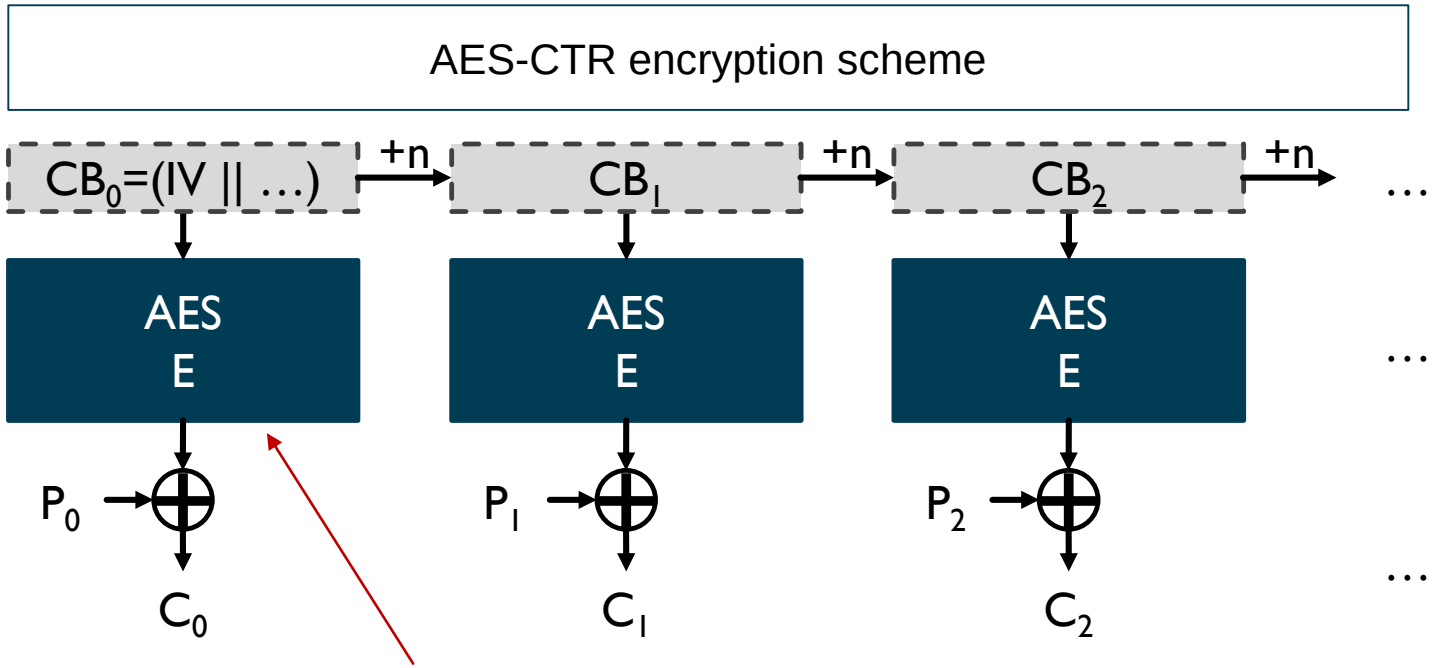
HIGH-SPEED AES ENCRYPTION ENGINE

Nr. of stages	AES-128/256	Fmax [GHz]	Throughput [Gbps]	Complexity [kGE]
14	ON	2.60	332.80	149.92

- High-speed encryption engine for CCA

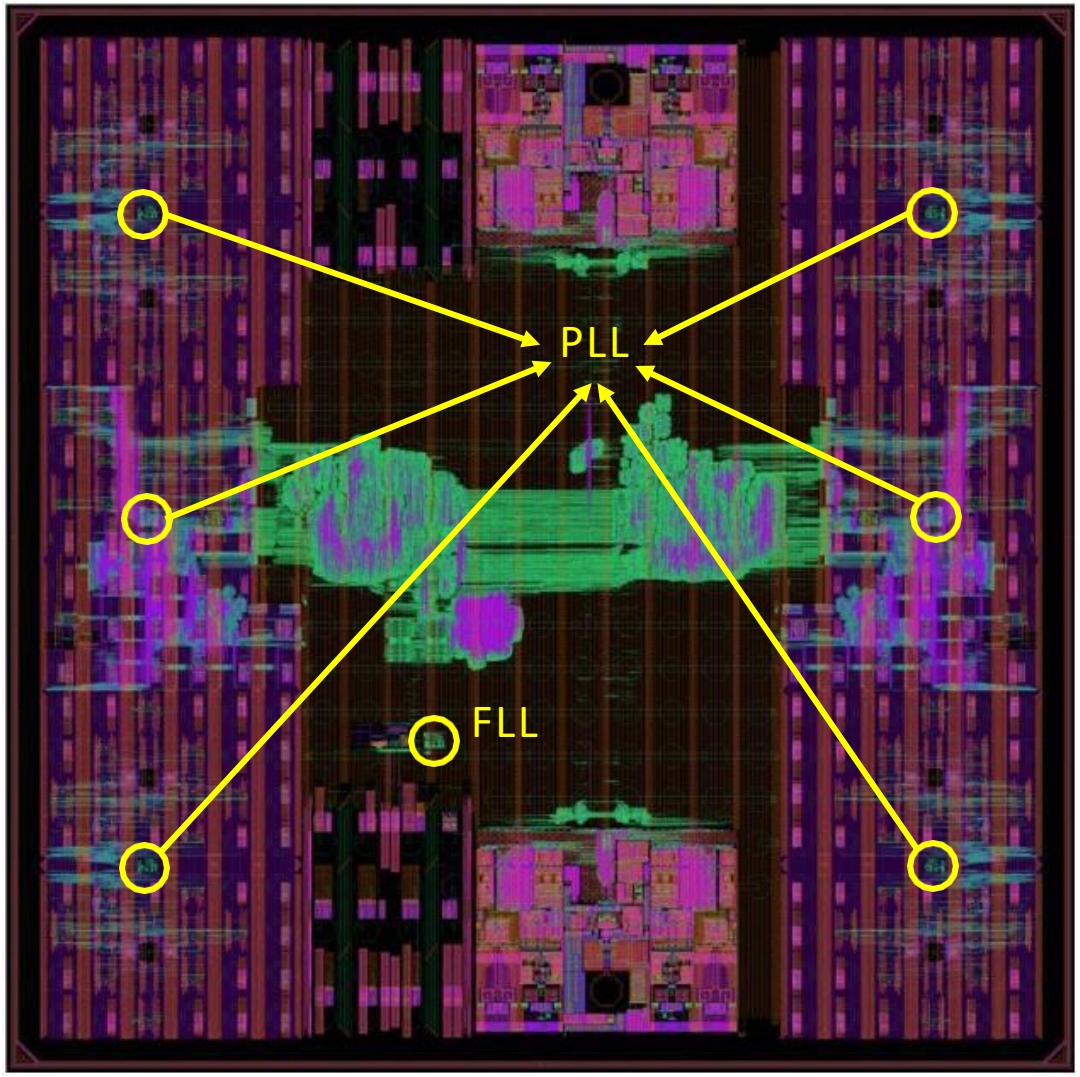
– real-time memory encryption or protection of VM in servers

- Synthesis results on EPI 7 nm technology
  - TSMC CLN07FF41001, library H300 BASE SVT C8, Standard Voltage Threshold (SVT)
  - Operating conditions: Voltage Supply = 0.90 V, Temperature = 125°C, Process corner = Slow



Optimized AES engine, configured for high-speed throughput

EXAMPLE CHIP DESIGNED & TESTED @ DII



3.5 x 3.5 mm2

- GlobalFoundries 12nm FinFet chip
- The European Pilot EUROHPC project

HW AND SW SOLUTIONS FOR VEHICULAR CYBERSECURITY

1) Secure FOTA (Firmware Over The air) update with Post-Quantum Cryptography (PQC) signature

2) Anomaly, Intrusion Detection & Fingerprint

3) SEAL-Embedded Homomorphic Encryption library for user's privacy

4) HSM (HW Security Module) for the European Processor Initiative

5) Hacking Keyless Entry System

KEYLESS ENTRY SYSTEMS

Remote Keyless Entry System (RKES)

Jam-and-replay attack

Passive Keyless Entry System (PKES)

Relay attack

Research performed in collaboration with

- Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato
- NITEL

nitel
Consorzio Nazionale Interuniversitario per i Trasporti e la Logistica

LIST OF HACKED CARS

1. Toyota Aygo 2013
2. Suzuki Alto 2011
3. Citroen C2 2003
4. Peugeot 206 2006
5. Subaru Xv 2013
6. Fiat Grande Punto 2012
7. Fiat 500L 2012
8. Suzuki 2017
9. Smart For4 2004
10. Toyota Yaris 2017
11. Opel Corsa 2012
12. Audi X6

Results presented at

Centro Addestramento Polizia di Stato (CAPS), Cesena, 5 July 2018

Italian Conference on Cybersecurity (ITASEC19), Pisa, 12-15, Feb. 2019

28° Convegno Nazionale Italiano PIARC, Scuola delle Specialità della Polizia di Stato, 14 – 16 May 2019

ITASEC19
ITALIAN CONFERENCE ON CYBERSECURITY
Pisa, 12-15 February 2019
cini Cybersecurity National Lab

POSSIBLE CONSEQUENCES

Steal the baggage

Steal the car

«Create» a terrorist

VEHICLE CYBERSECURITY RECENT BIBLIOGRAPHY

1) **On hardware acceleration of quantum-resistant FOTA systems in automotive,** Perazzo, P., Di Matteo, S., Dini, G., Saponara, S., ***Computers and Electrical Engineering***, 2024

2) **CRYPHTOR: A Memory-Unified NTT-Based Hardware Accelerator for Post-Quantum CRYSTALS Algorithms,** Di Matteo, S., Sarno, I., Saponara, S., ***IEEE Access***, 2024,

3) **VLSI Design and FPGA Implementation of an NTT Hardware Accelerator for Homomorphic SEAL-Embedded Library,** Di Matteo, S., Gerfo, M.L., Saponara, S., ***IEEE Access***, 2023

4) **Hardware Design of an Advanced-Feature Cryptographic Tile within the European Processor Initiative,** Nannipieri, P., Crocetti, L., Matteo, S.D., Fanucci, L., Saponara, S., ***IEEE Transactions on Computers***, 2023

5) **VLSI Design of Advanced-Features AES Cryptoprocessor in the Framework of the European Processor Initiative,** Nannipieri, P., Crocetti, L., Baldanzi, L., Fanucci, L., Saponara, S., ***IEEE Transactions on Very Large Scale Integration (VLSI) Systems***, 2022

6) **Design and Testing Novel One-Class Classifier Based on Polynomial Interpolation with Application to Networking Security,** Dini, P., Saponara, S. et al., ***IEEE Access***, 2022

MODEL-BASED DESIGN AND VERIFICATION OF ECU SW

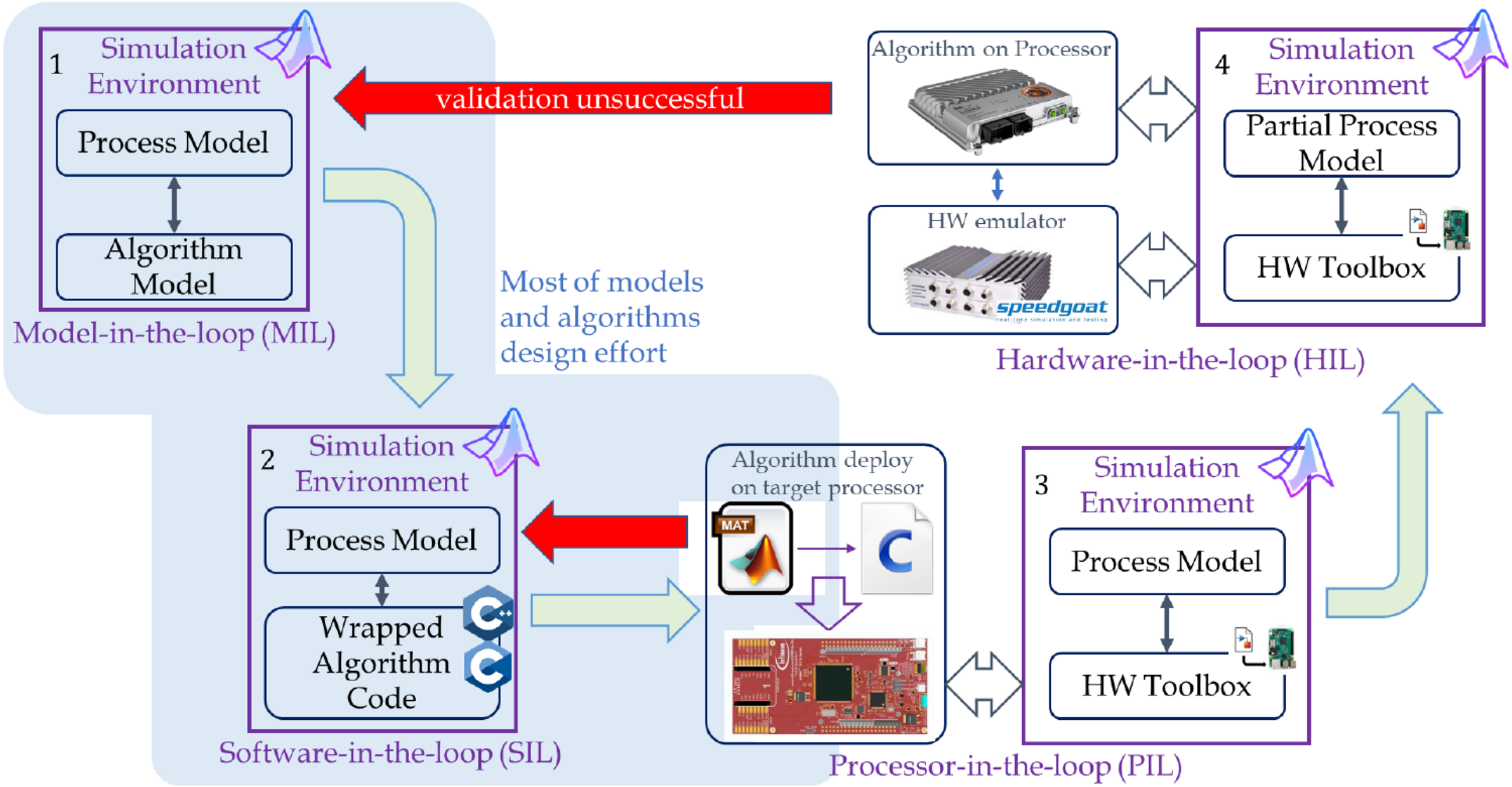
1) **Model-based design and verification flow**
2) **Application examples:**

   - Bidirectional on-board charger with Model Predictive Control

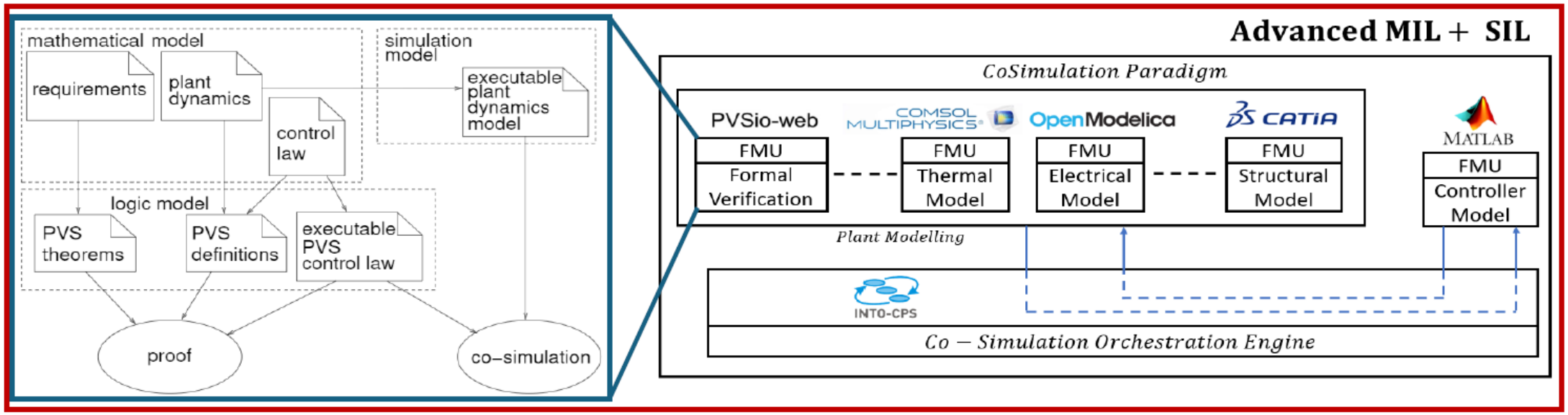
   - Dual-inverter for Power Drive

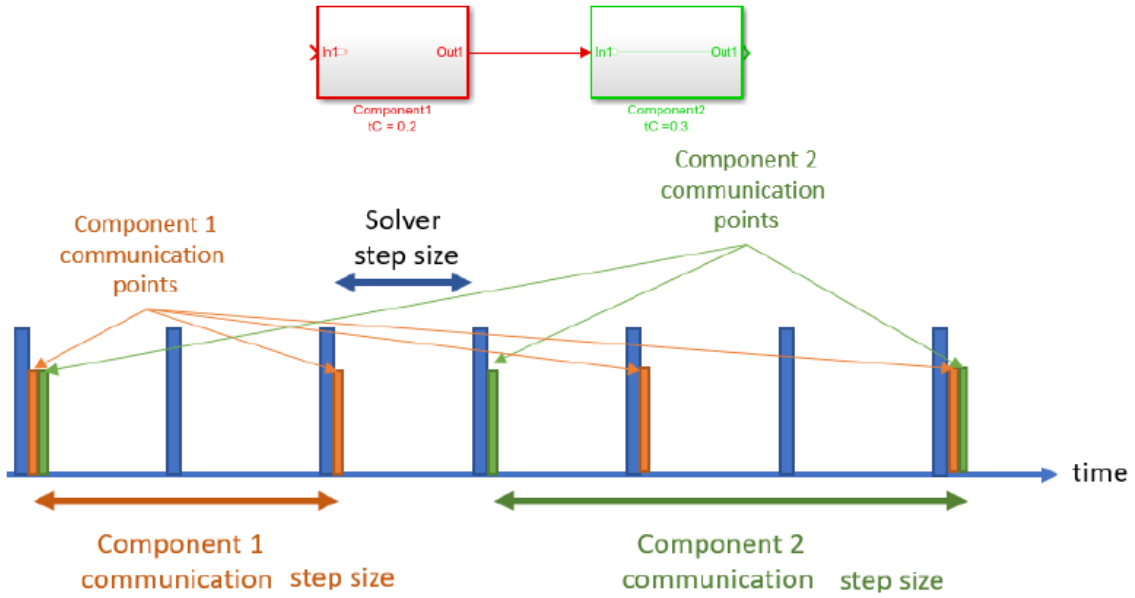
   - HIL for BSG testing

MODEL-BASED DESIGN & VERIFICATION OF ECU SW

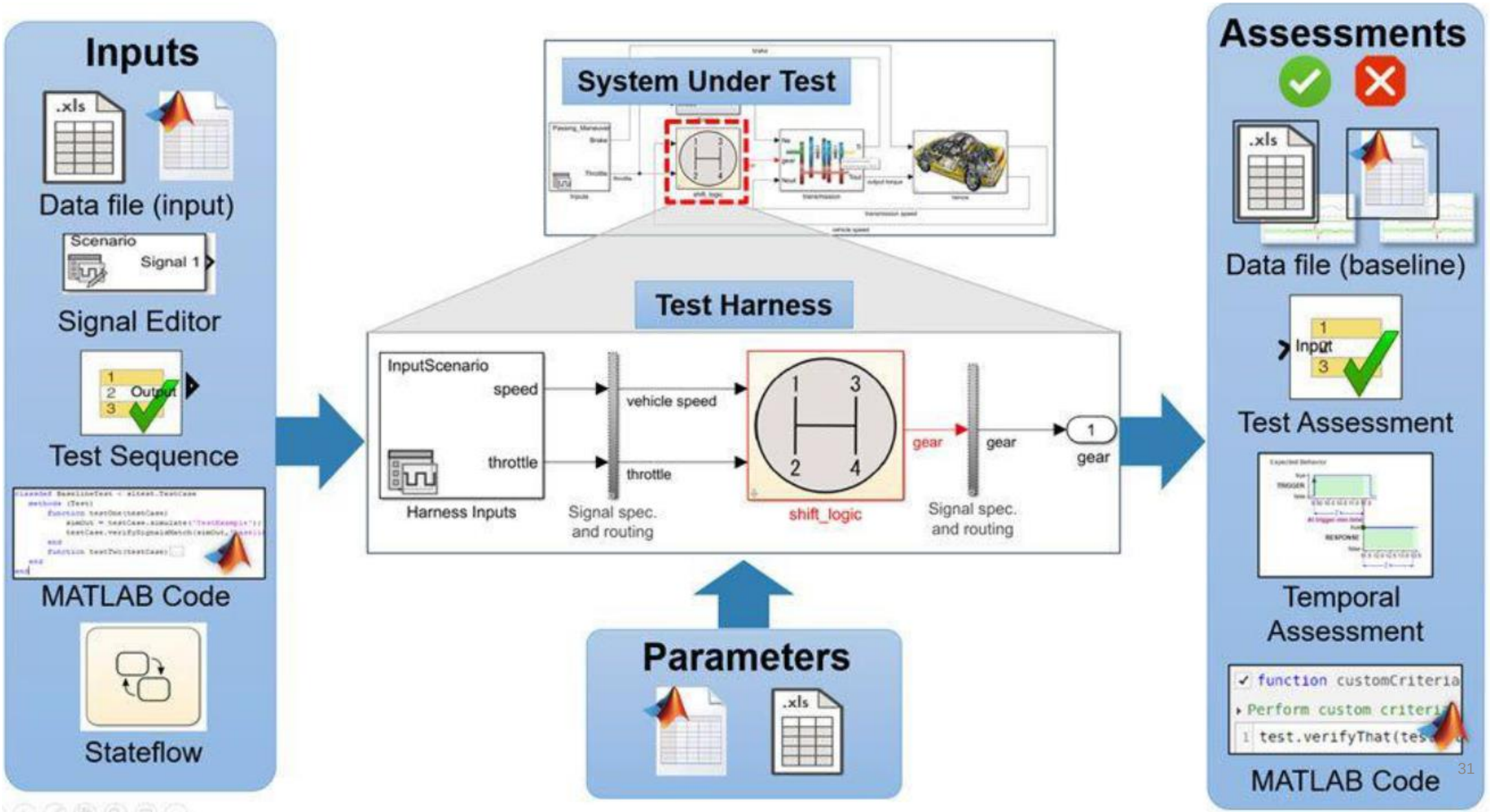


FORMAL-VERIFICATION & MULTI-SCALE/-PHYSICS ANALYSIS

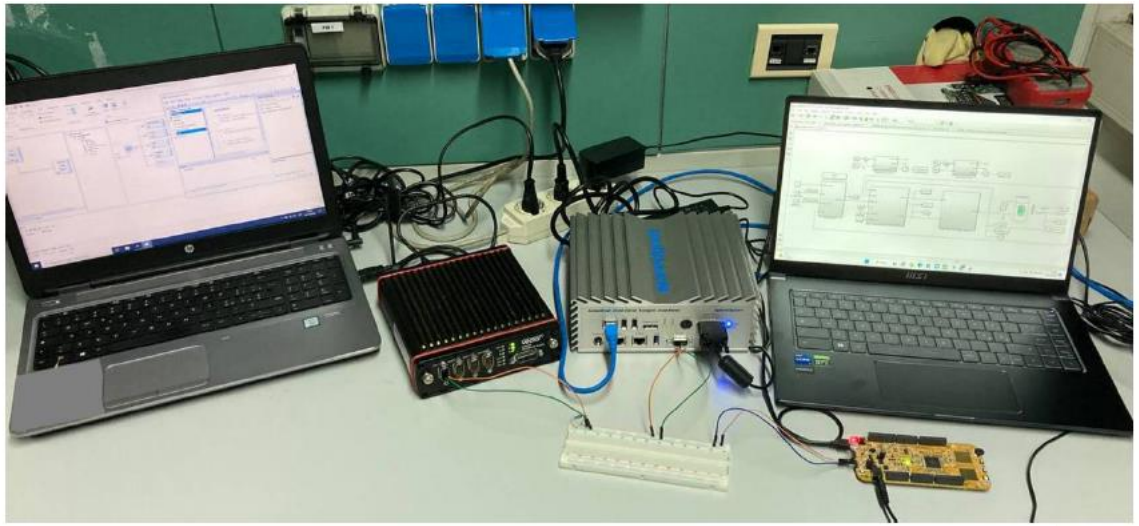


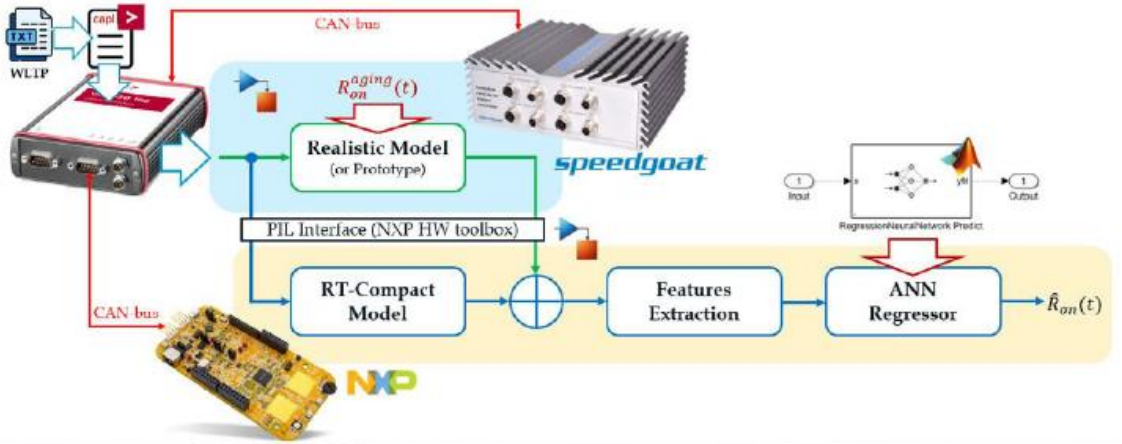


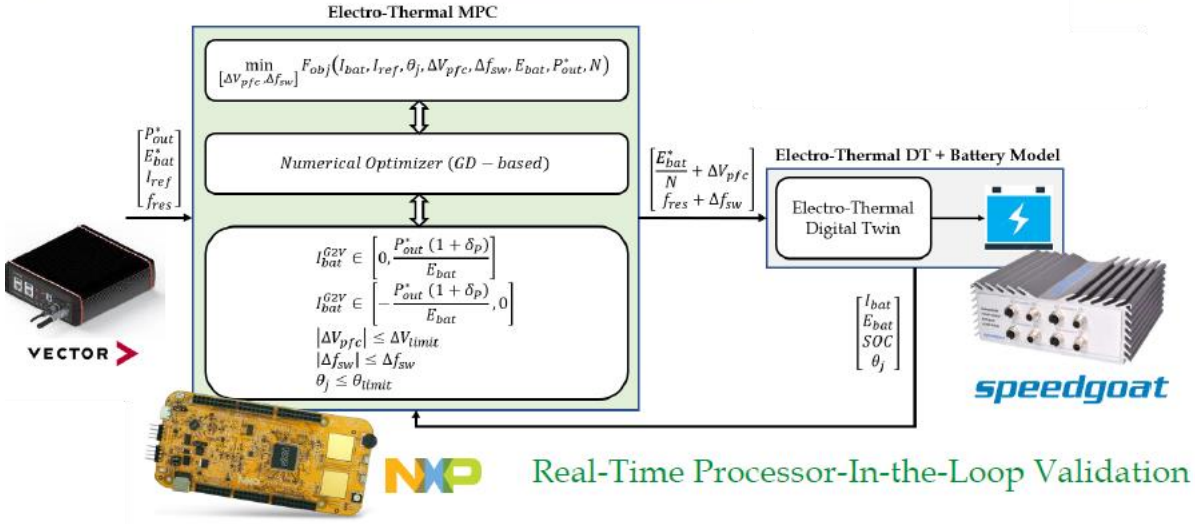
VIRTUAL PROTOTYPING & TESTING

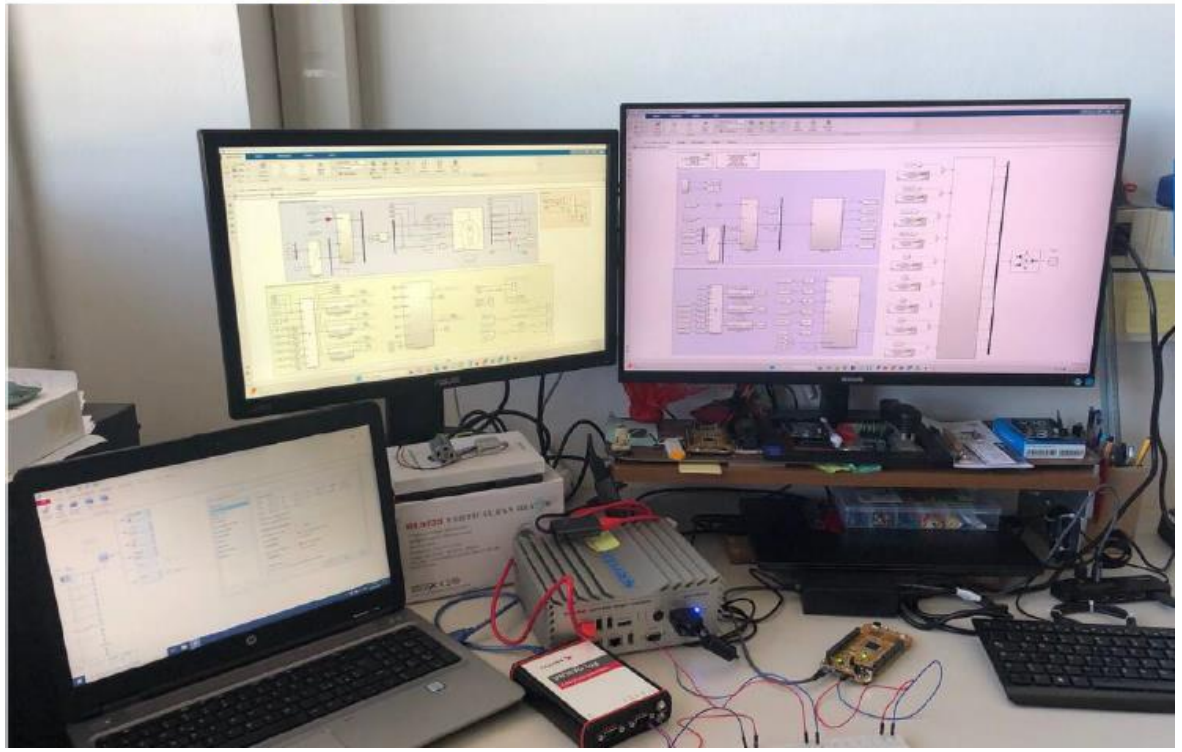


THE SAME SET-UP FOR ECU SW DESIGN AND VERIFICATION









MODEL-BASED DESIGN AND VERIFICATION OF ECU SW

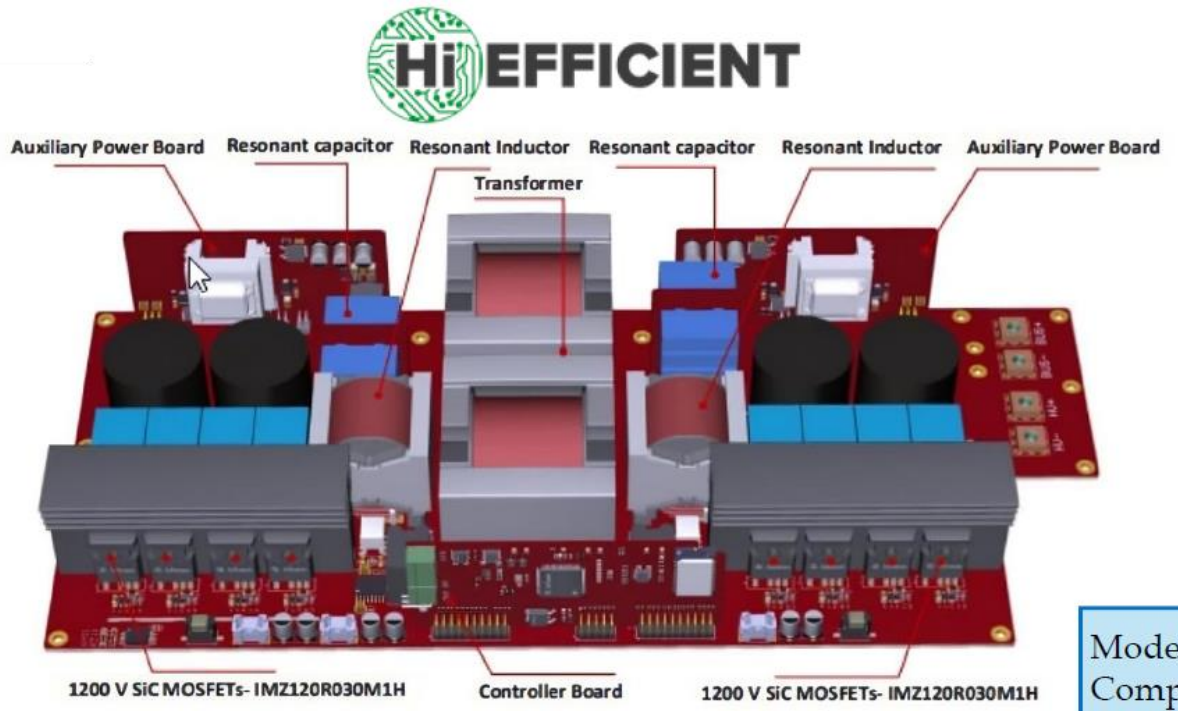
1) **Model-based design and verification flow**
2) **Application examples:**

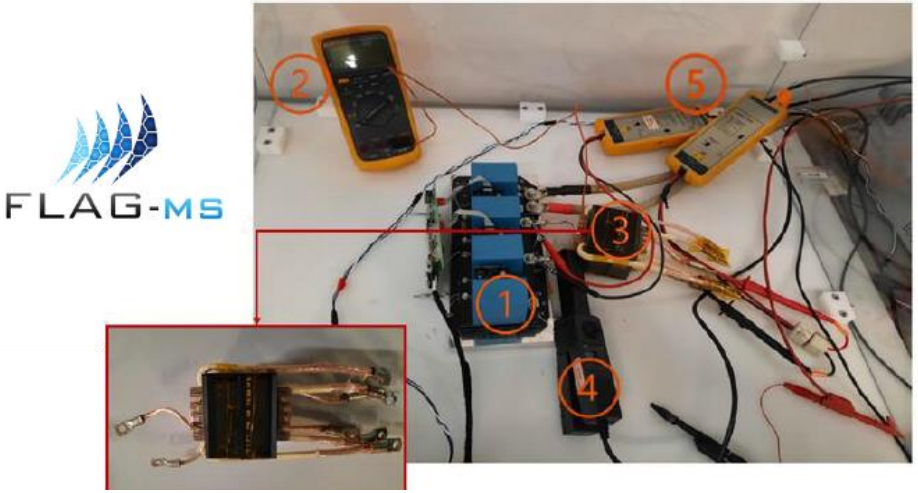
   - Bidirectional on-board charger with Model Predictive Control

   - Dual-inverter for Power Drive

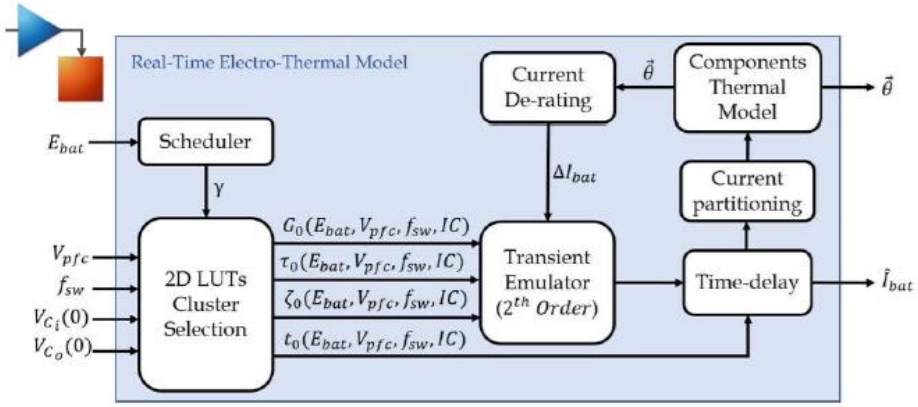
   - HIL for BSG testing

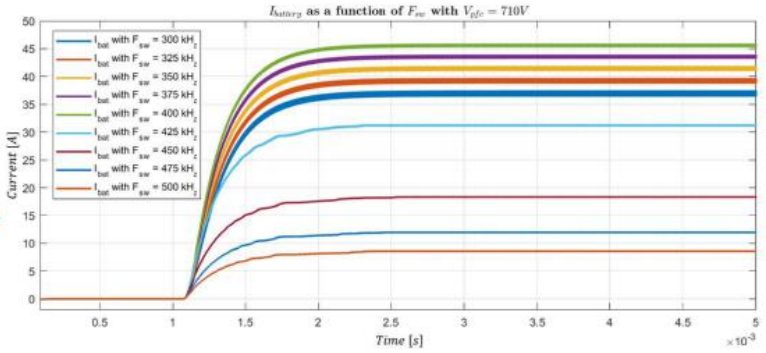
APPLICATION 1: BIDIRECTIONAL ON-BOARD CHARGER WITH MODEL-PREDICTIVE CONTROL

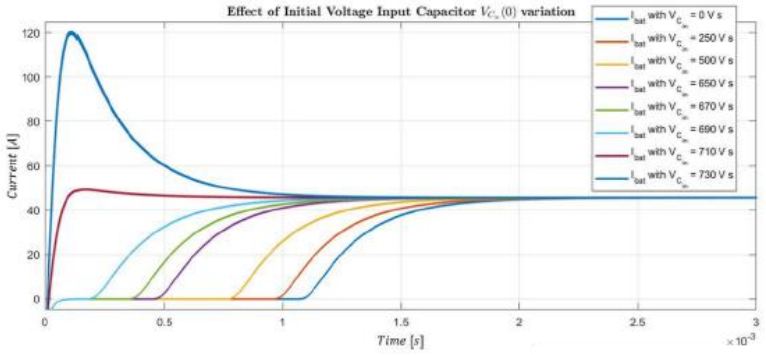




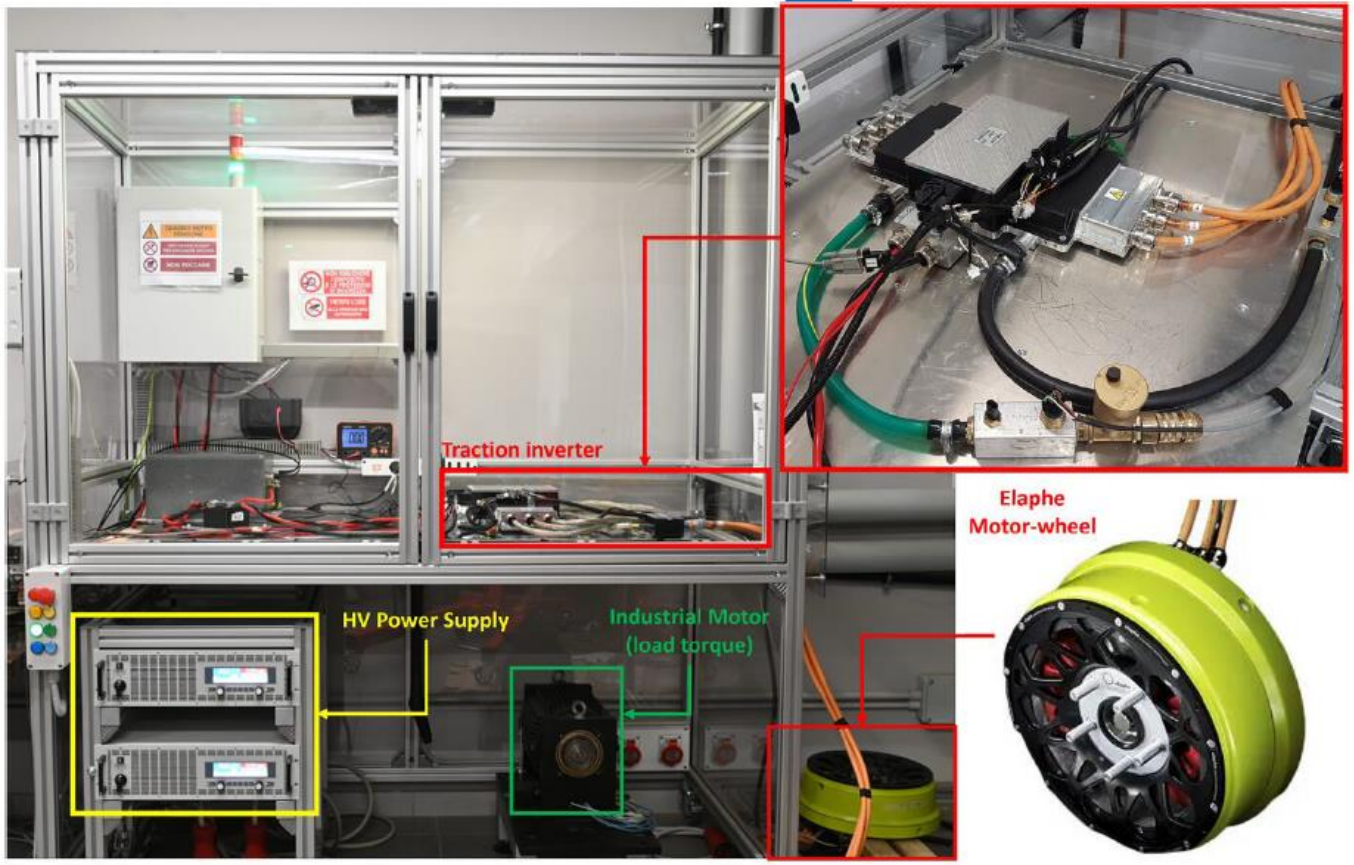
Model assessment & Complexity reduction



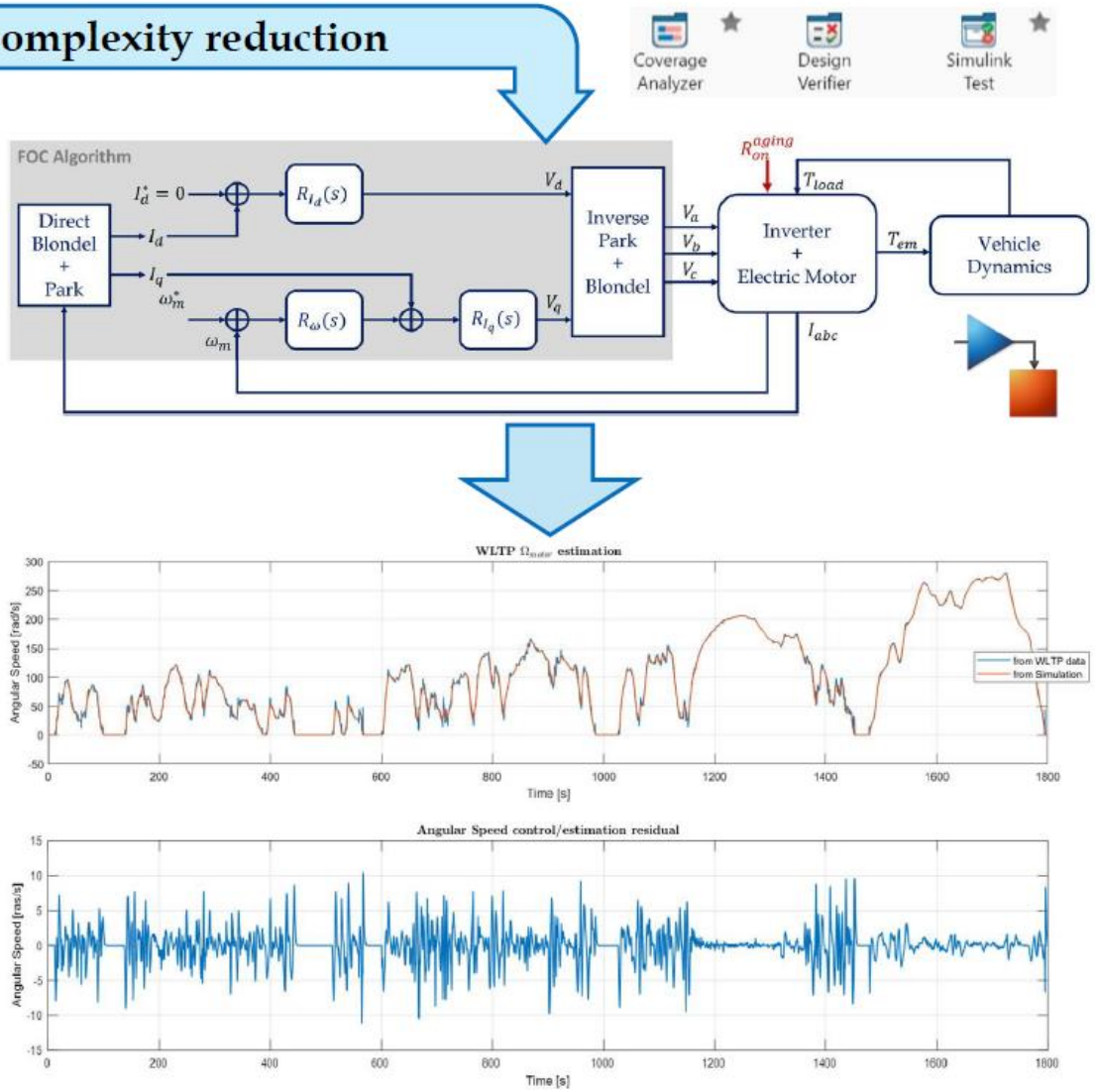


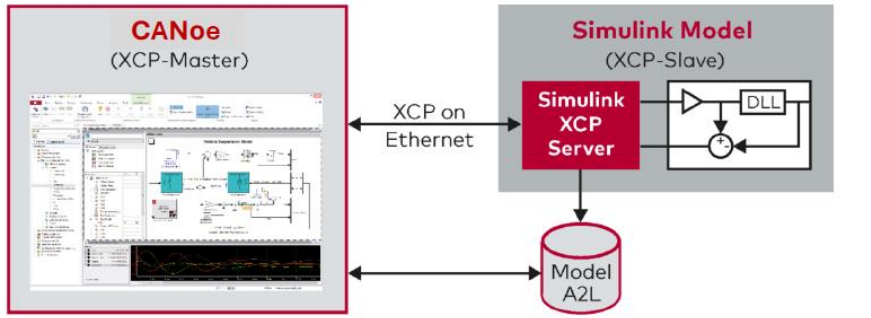


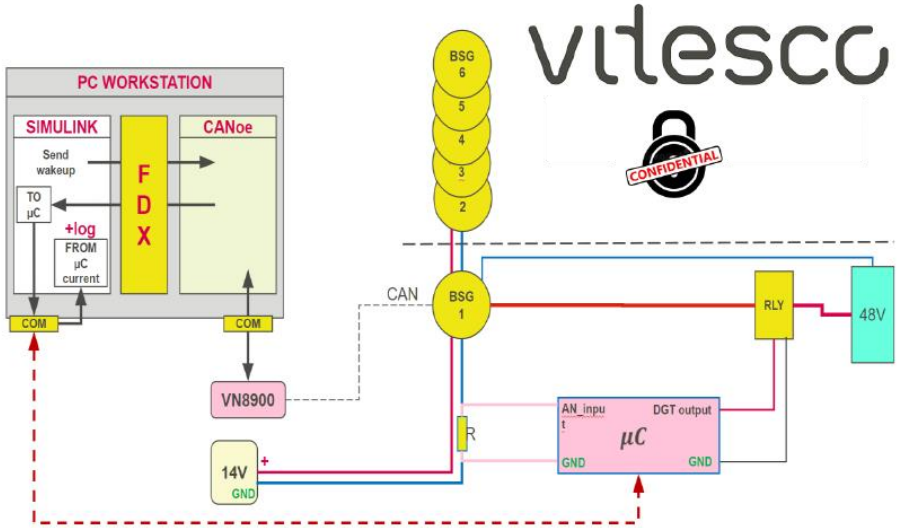
APPLICATION 2: DUAL-INVERTER FOR POWER DRIVE

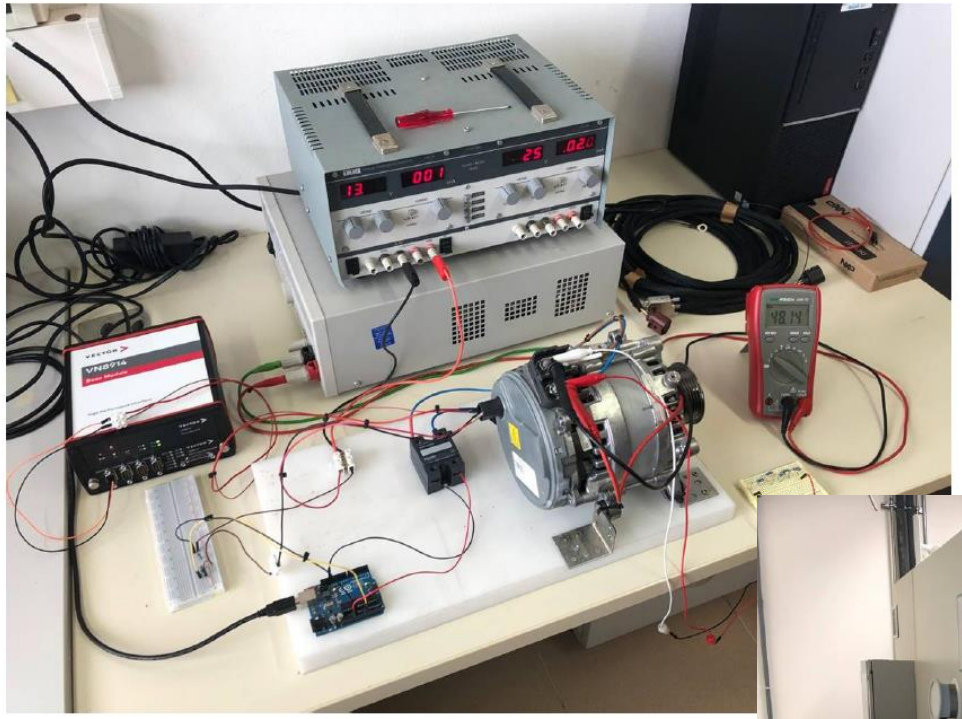


Elaphe
Motor-wheel









APPLICATION 3: HIL FOR BSG TESTING

ECU SW DESIGN & VERIFICATION RECENT BIBLIOGRAPHY

1) **Real-time monitoring and ageing detection algorithm design with application on SiC-based automotive power drive system,** Dini, P., Basso, G., Saponara, S., Romano, C., ***IET Power Electronics***, 2024

2) **Review on Modeling and SOC/SOH Estimation of Batteries for Automotive Applications,** Dini, P., Colicelli, A., Saponara, S., ***Batteries***, 2024

3) **Real-time electro-thermal modelling and predictive control design of resonant power converter in full electric vehicle applications,** Dini, P., Saponara, S**., et al.,** ***IET Power Electronics***, 2023

4) **Experimental Characterization and Electro-Thermal Modeling of Double Side Cooled SiC MOSFETs for Accurate and Rapid Power Converter Simulations,** Dini, P., Saponara, S., Hegazy, O., et al., ***IEEE Access***, 2023

5) **Processor-in-the-Loop Validation of a Gradient Descent-Based Model Predictive Control for Assisted Driving and Obstacles Avoidance Applications,** Dini, P., Saponara, S., ***IEEE Access***, 2022

6) **An Embedded System for Acoustic Data Processing and AI-Based Real-Time Classification for Road Surface Analysis,** Gagliardi, A., Staderini, V., Saponara, S., ***IEEE Access***, 2022

Thanks for your attention - Any Question?

Contact: **Sergio Saponara, sergio.saponara@unipi.it, + 39 3468790937**

Dipartimento Ingegneria della Informazione (DII), Università di Pisa

3rd July 2024

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

IN SUPREMÆ DIGNITATIS 1343