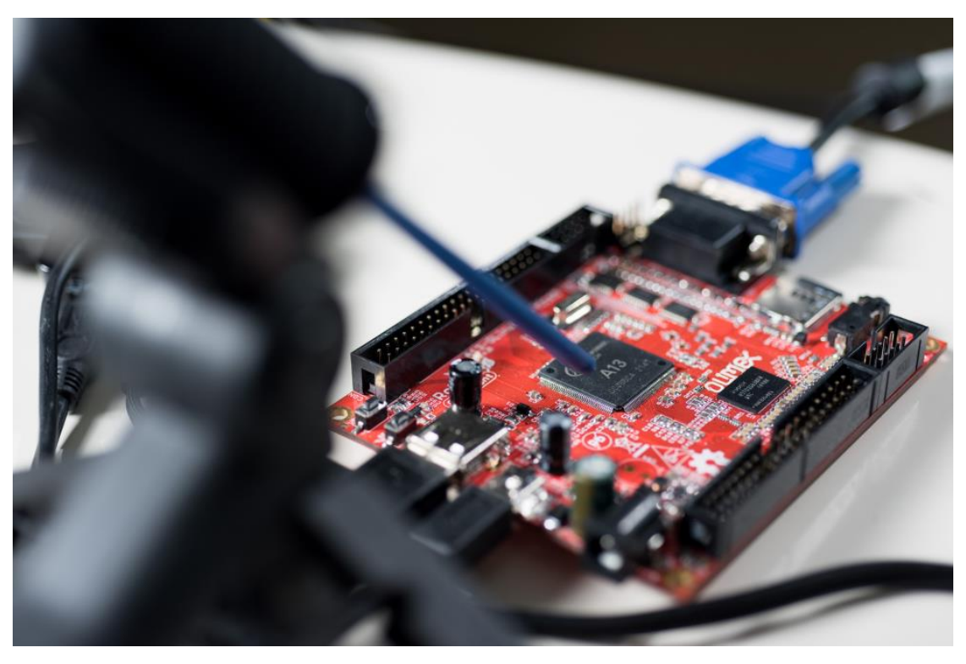
Hardware-based security analysis, optimised solutions for attack detection

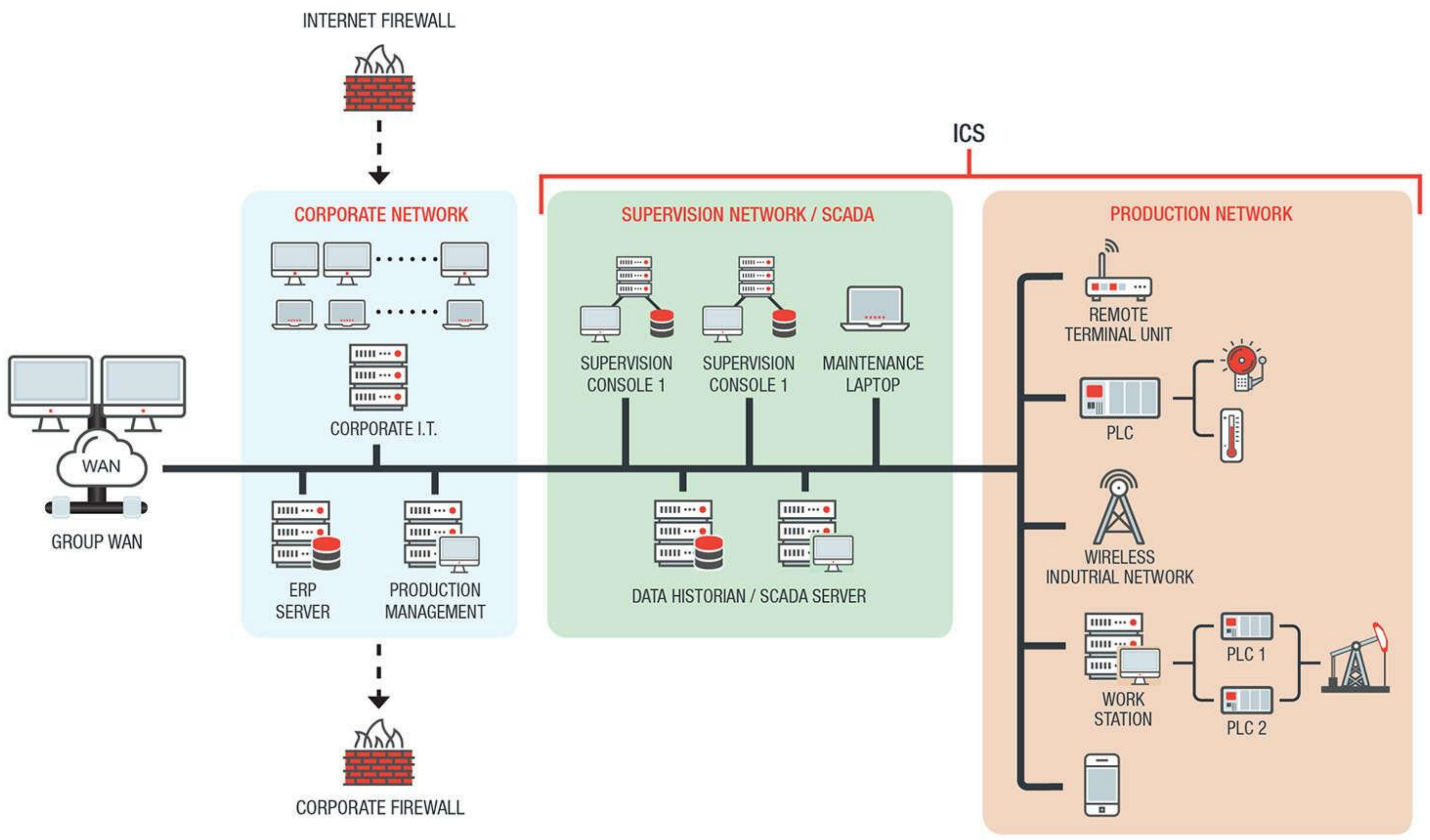
Lucas Georget, Vincent Migliore, Youssef Laarouchi, Vincent Nicomette

Critical Infrastructure: Security in ICS (End-to-End security enforcement)

Malicious component

Certification: test bench





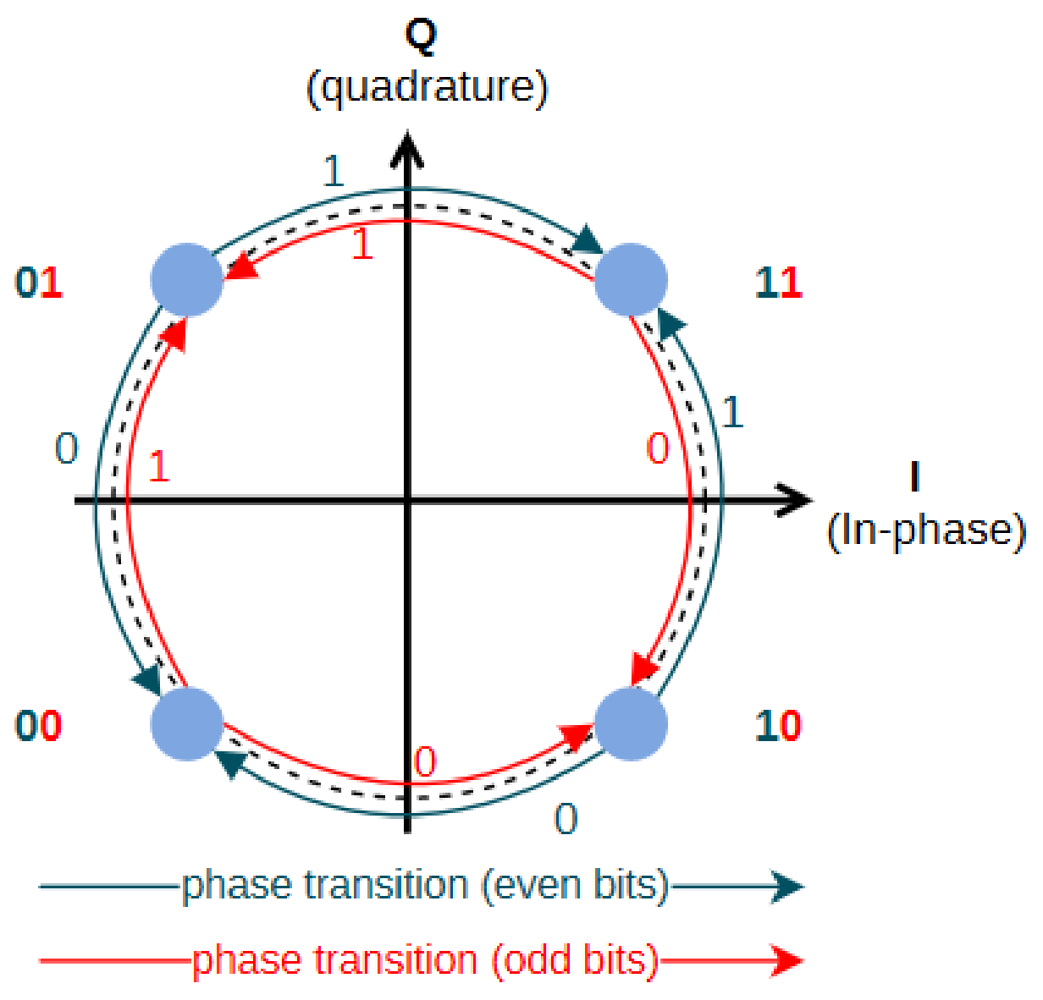
The increasing complexity of systems has also led to an attack surface increase which may lead to compromission or information extraction.
Today, new critical attacks exploit hardware features of systems to overcome the classical security countermeasures of systems, designed for software.

Wireless Communications

- ### WazaBee [1]

WazaBee is a pivotal attack of protocols based on 802.15.4 (in particular Zigbee) through BLE devices.

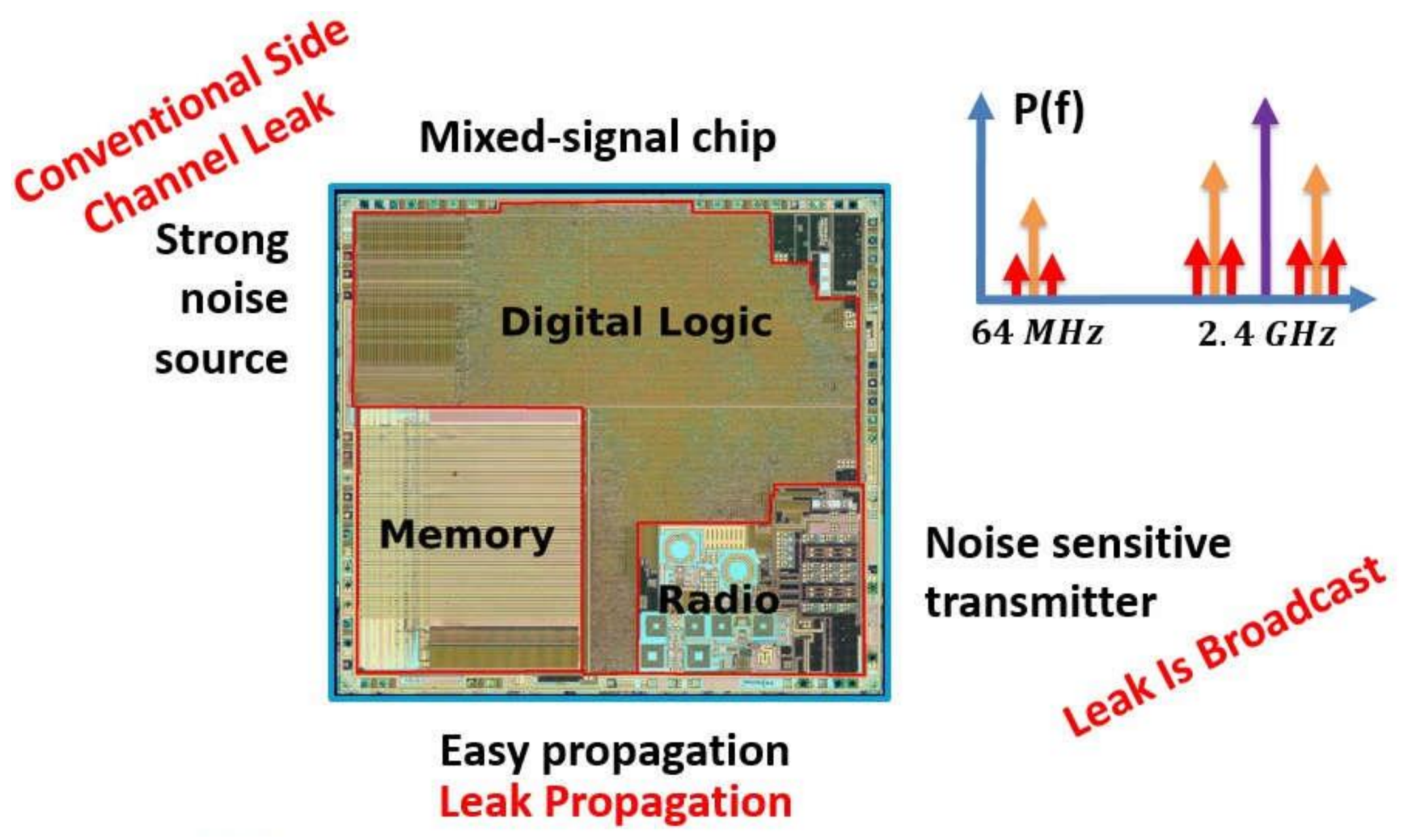
The attack takes advantage of the compatibility that exists between the two modulation techniques used by these two protocols.



The direct consequence is an increase in the attack surface, wireless system communicating being potentially accessible from another radio component.

- ### Screaming Channels [2]

Screaming Channels are a novel type of (radio) side channel attacks at large distance against mixed-signal chips used in modern connected devices.



"nRF51822 - Bluetooth LE SoC : weekend die-shot" - CC-BY - Modified with annotations. Original by zeptobars.

EURECOM
Sophia Antipolis

Hardware Communications

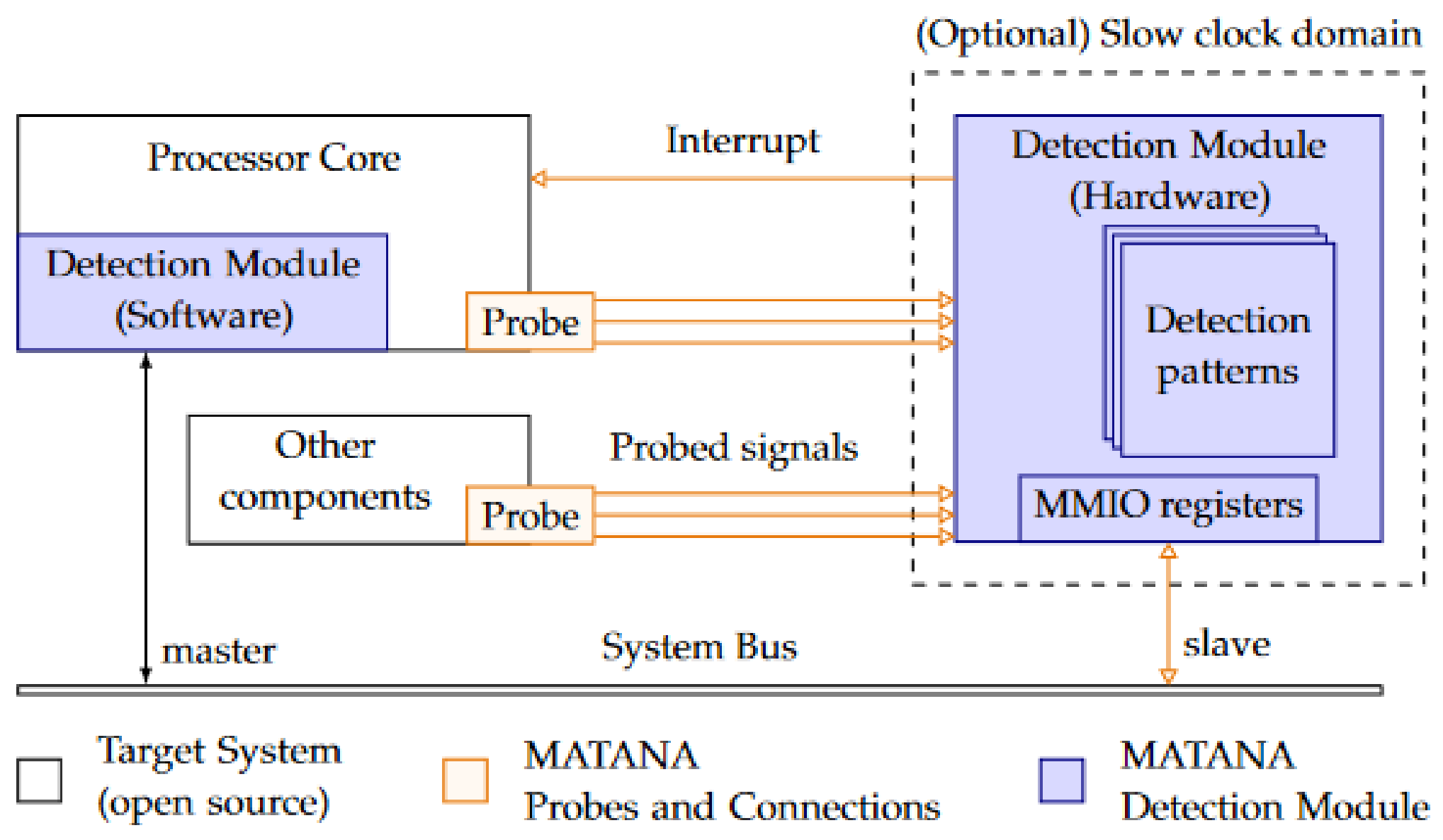
- ### Intrusion detection based on Hardware Performance Counters analysis [3]

Detection of compromised devices among a massive population of similar devices by analyzing the processor's Hardware Performance Counters. This analysis is based on existing outlier detection algorithms, with low computational and network traffic overhead, without modeling the behavior of the applications running on the devices.
This approach is then easily adaptable to devices' updates. Moreover, as it only rely on the counters' analysis, we can detect anomalies of various origins, such as a compromised OS.

The results obtained show that a high detection efficiency can be achieved, with low overhead and low execution time.

- ### Dynamic software and hardware attack detection based on microarchitectural signals analysis [4]

A framework allowing the dynamic detection of attacks that leave fingerprints at the system's microarchitecture layer.



It shows that, thanks to the analysis of microarchitectural information, relatively simple logic implemented in the detection module is sufficient to detect different classes of attacks (cache side-channel attack and ROP attack).

For the moment, the methods that have been proposed in the literature are based on either a hardware modification or the execution of a detection software code directly on the system. In the case of critical industrial infrastructures, these methods are not directly applicable.

In order to provide effective solutions to hardware attacks, it is now important to study the possibilities of detecting attacks not only from the critical system, but also remotely, in order to be able to react thanks to a more global vision of the industrial infrastructure.

seido LAB
eDF
LAAS CNRS

[1] Romain Cayre, et al.. WazaBee: attacking Zigbee networks by diverting Bluetooth Low Energy chips. DSN 2021.
[2] Giovanni Camurati, et al.. Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks. TCHES 2020.
[3] Malcolm Bourdon. Détection d'intrusion basée sur l'analyse de compteurs matériels pour des objets connectés. INSA de Toulouse, 2021. Français.
[4] Yuxiao Mao. Détection dynamique d'attaques logicielles et matérielles basée sur l'analyse de signaux microarchitecturaux. Architectures Matérielles. INSA de Toulouse, 2022. Français.