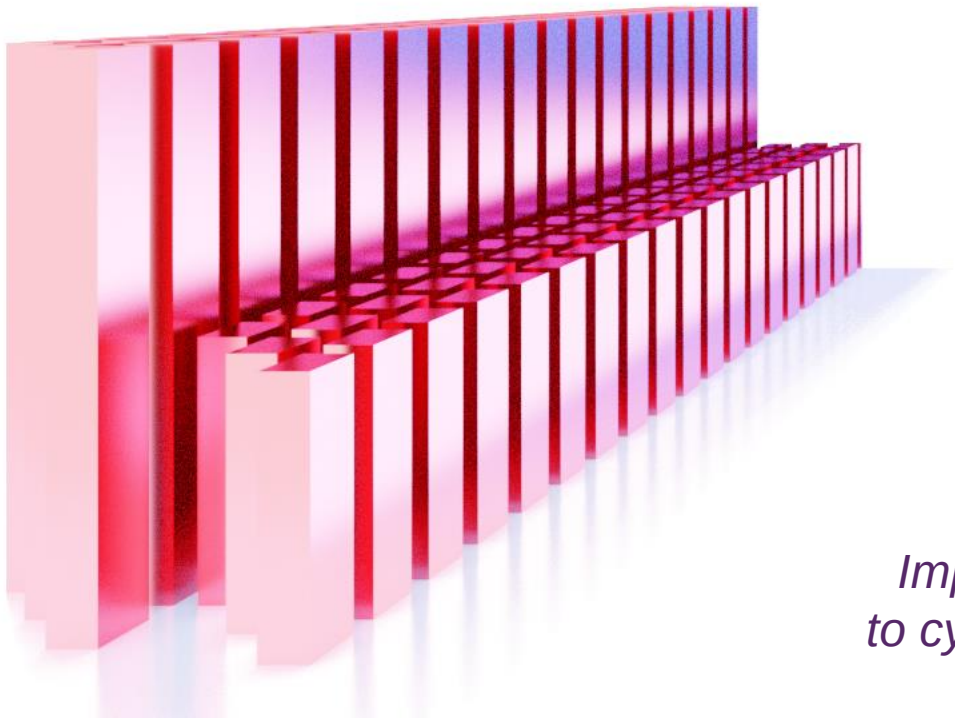
How to protect Industry 4.0 Sensitive Industrial Plants from cyber and physical attacks

Luigi Romano

InfraStress Technical Manager



INFRA STRESS

Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats by means of an open testbed stress-testing system

Outline

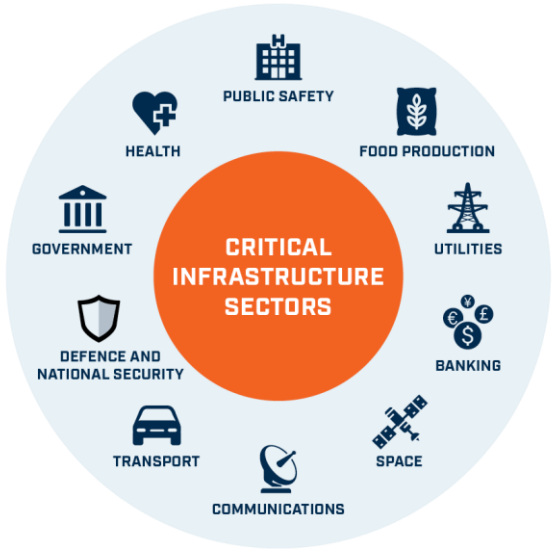
- The importance of cyber-security for Sensitive Industrial Plants and Systems (SIPS)
- Examples of cyber-physical attacks
- Challenges when IT and OT coexist
- An advanced SIEM solution implemented in the context of InfraStress:
  - The detection of attacks in IIoT (LP-WAN) deployments
  - The Intrusion Detection System monitoring the compliance of the business process

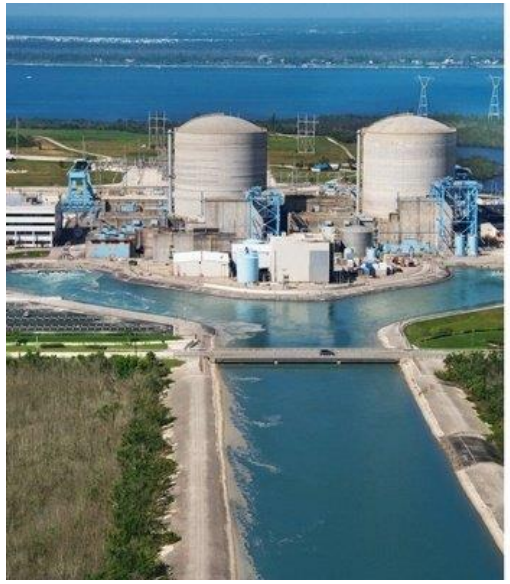
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

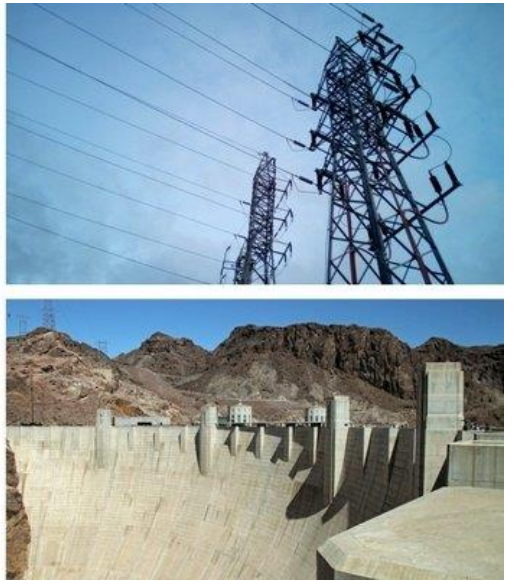
INFRA STRESS

Cyber-security is key in SIPS

- Attacks to Industrial Control Systems of SIPS cost money, reputation, and even human lives







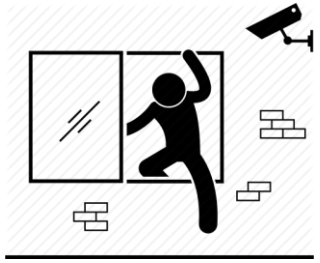
- Domino effects in the physical world could arise from cyber attacks, causing environmental disasters or serious damage to production lines

* The Official 2019 Annual Cybercrime Report https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

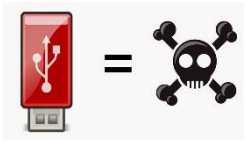
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

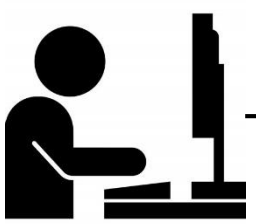
INFRA STRESS

Environmental Disaster Example



The malicious user violates the site's security





A malware is inserted in the control room desktop machine.
It exploits a vulnerability to achieve privilege escalation

The attacker can now inspect the internal industrial network

The malware forces the valve of a critical tank to remain in an open state

Flammable liquid leaks, causing a fire

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Production Line Damage Example

An insider attacker injects a **malicious G-code** in a **CAD machine** and in the **product control system**

The CAD machine will use the malicious G-code to build, e.g., a medical prosthesis, with different specifications

The entire product line is compromised

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Why the SIPS protection is challenging?

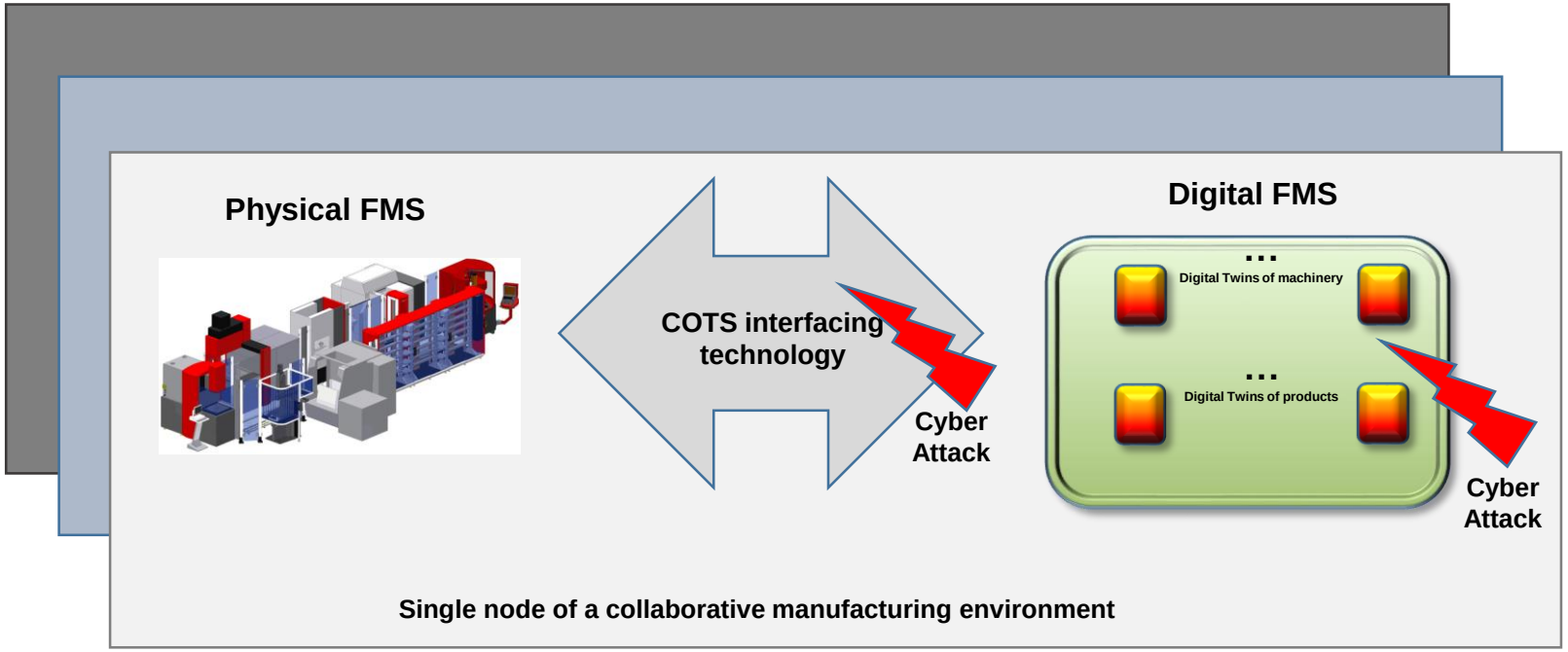
- In Industrial Control Systems, two different technologies coexist:
  - **Information Technologies (IT)** → e.g., database, app server, web server, log server, …
  - **Operational Technologies (OT)** → e.g., valves actuators, sensors, tanks, robotic arm controllers, pumps controllers, …
- Typically, weaknesses are due to the usage of legacy technologies to link IT and OT solutions
- The security mechanisms should be able to take into account the two worlds together

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

The InfraStress DePuy Case Study

- In Septemer 2018 DePuy has been recognized as one of the nine Industry 4.0 Lighthouse projects/companies
- It was explicitly mentioned that they “use legacy technology to build Digital Twins”



DePuy Synthes
COMPANIES OF Johnson&Johnson

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

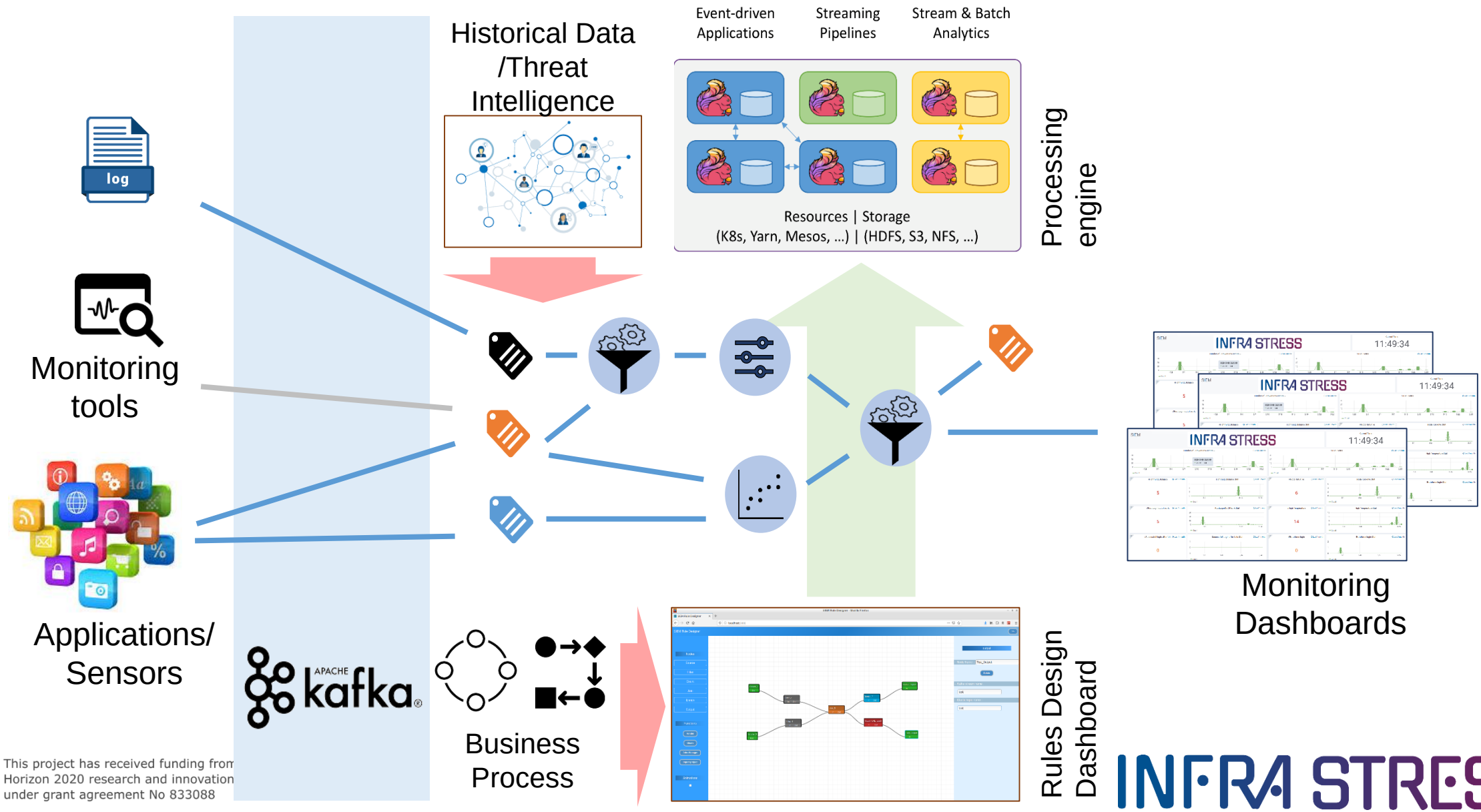
The InfraStress Solution for Situational Awareness

- In the context of the InfraStress project we build tools for monitoring the situation in the SIPS infrastructure
- We propose a **SIEM** (*Security Information and Event Management)* system that provides real-time analysis of data coming from OT and IT worlds by correlating their on-going events
- With respect to the state-of-the-art, the InfraStress SIEM encloses:
  - **IIoT IDS** → A detection system that monitors attacks in IIoT (LP-WAN) deployments
  - **BAM-based IDS** → A detection system that monitors business process violations

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Architecture of the InfraStress SIEM



This project has received funding from Horizon 2020 research and innovation under grant agreement No 833088

INFRA STRESS

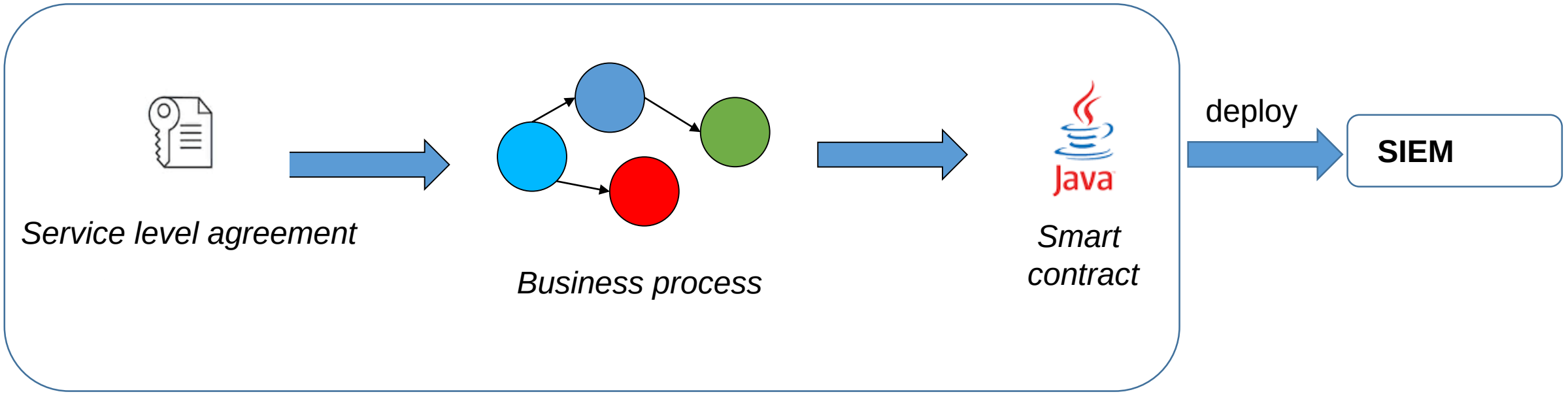
Intrusion detection based on Business Process knowledge

- A business process can be fully monitored through a *smart contract*
  - » A *smart contract* is an agreement embedded in a program managed by a blockchain
  - » The program contains a set of rules under which the parties of that smart contract agree to interact with each other
- A finite state machine (**FSM)** representation provides a clearer view of the business process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

IDS based on BP knowledge



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Intrusion Detection in the IIoT world

- We have implemented an IDS that analyzes traffic in a LoRa-based IIoT network:

» Design and implementation of **LoRa-specific IDS probes**.

» Design and implementation of an intelligence module **for detecting the possible attacks** on the LoRaWAN protocol.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Why LoRa

- **LoRa is widely used in IIoT since its features are:**
  - ✓ low energy consumption;
  - ✓ high coverage;
  - ✓ secure communication;
  - ✓ high scalability;
  - ✓ minimal infrastructure;
  - ✓ end nodes may not be connected to the internet

- **LoRa (Long Range) is a LPWAN (Low-Power Wide Area Network) technology that refers to a stack consisting of two levels:**

» **The first level is the physical layer** (PHY) which exploits a proprietary modulation derived from the Chirp Spread Spectrum (CSS).

» **The second level is the protocol** for the MAC level called LoRaWAN.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

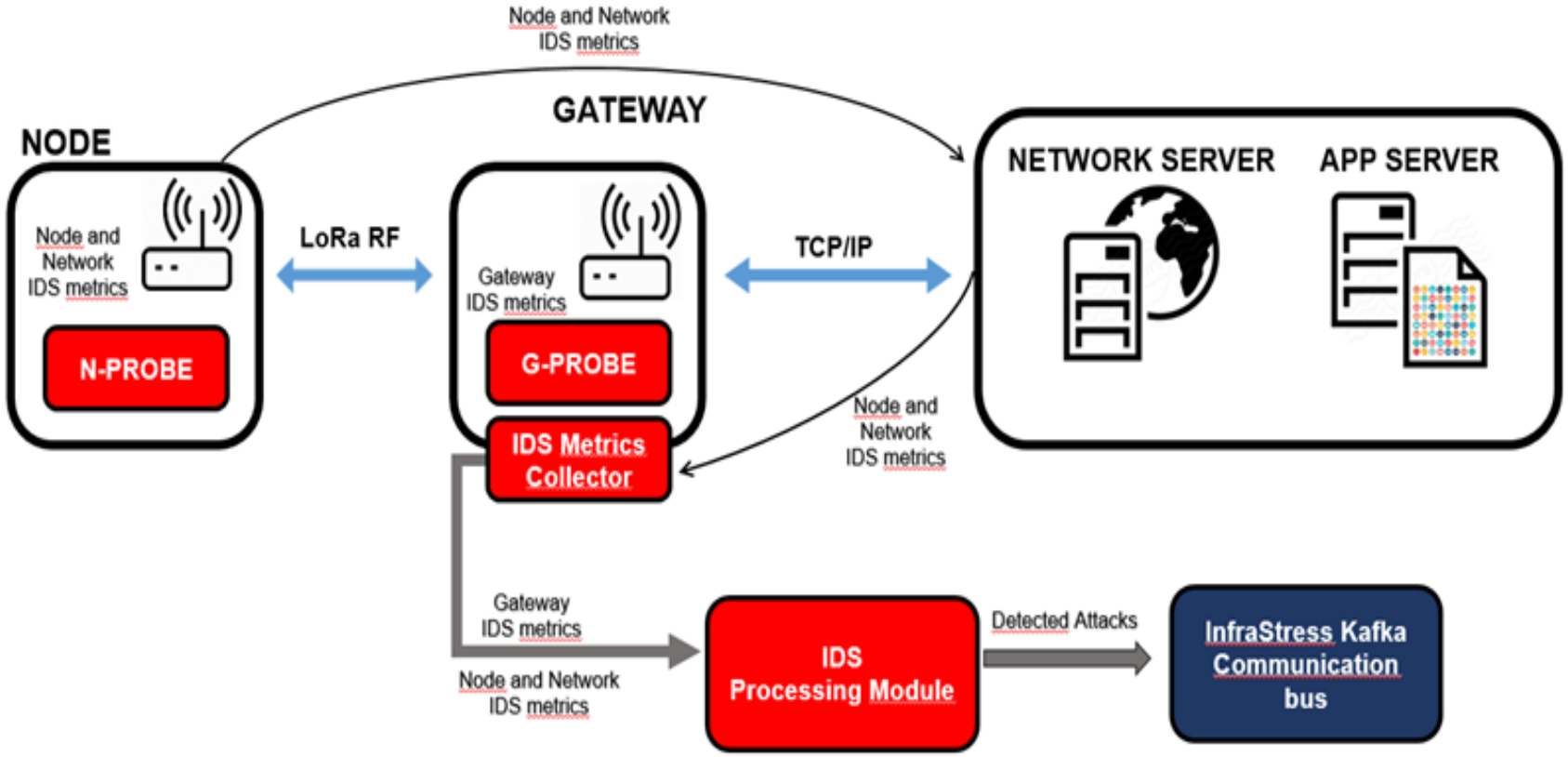
Possible attacks on LPWAN

ATTACK	Attack Typology	Details
RF Jamming	*DoS*	Disrupting radio transmission with Malicious radio signals in proximity of application devices
Beacon Synchronization	*DoS*	Setting up a GW to send fake beacons to put EDs and GWs out-of-sync
Flooding	*DoS*	Increasing the number of packets to be sent to the gateway
Firmware Replacement	*DoS or Information Leak*	Replacing firmware to either steal keys or enforce some DoS attack
Key Disclosure	*Information Leak*	Dumping the memory to steal keys exchanged with the radio module
Parameters Manipulation	*DoS*	Manipulating frequency parameters in the GW to increase power consumption of EDs

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

InfraStress LoRa IDS Architecture



This project has received funding from the European Union's
Horizon 2020 research and innovation programme
under grant agreement No 833088

Contact Info

Luigi Romano
InfraStress Technical Manager
prof.luigi.romano@gmail.com
+39 333 301 68 17

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS