Sensor Network for Intelligent Predictive Enterprise: il progetto SNIPE di FAE Technology

Ing. Manuel Lobati

Innovation & Project Manager

FAE Technology Spa

FAE TECHNOLOGY: company overview

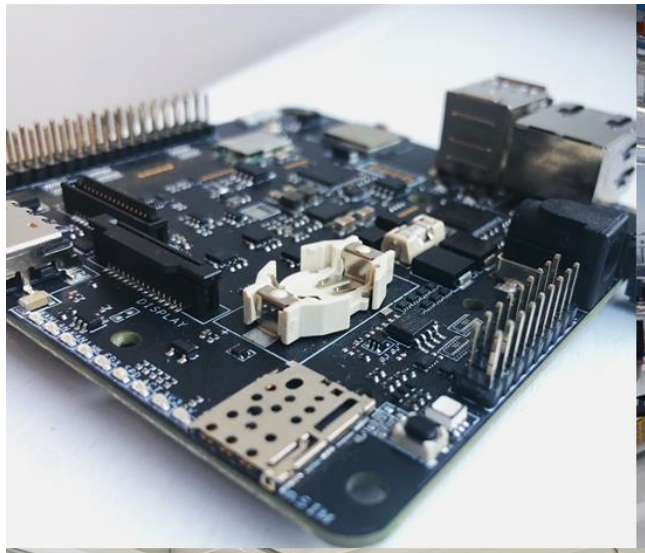
FAE Technology is an italian SME company established in 1991 that works in the EEMS market (*Electronics Engineering and Manufacturing Services)* : focused on the electronic design and production, FAE Technology can manage the complete lifecycle of a PCBA or Smart Device from the design to mass production and direct fulfillment.

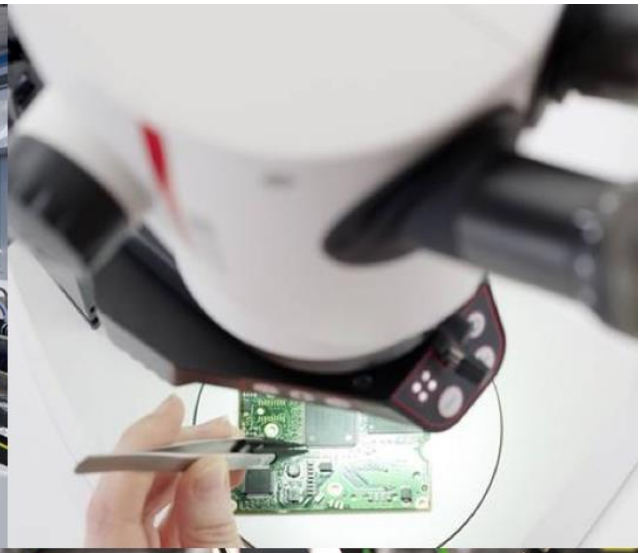
FAE Technology company that enables electronic technology for the digital transformation and Internet of Things (IoT), through the offer of three main added-value competences:

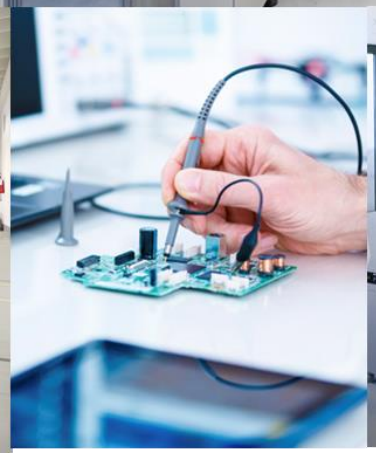
- **INNOVATION**: PoC & Collaborative Design Center based in Kilometro Rosso (BG).
- **SERVICES**: Added value EMS, PCBA manufacturing, Fast Prototyping and Engineering Design Center.
- **SOLUTION**: Products and complete end-to-end solutions to empower the digital transformation.

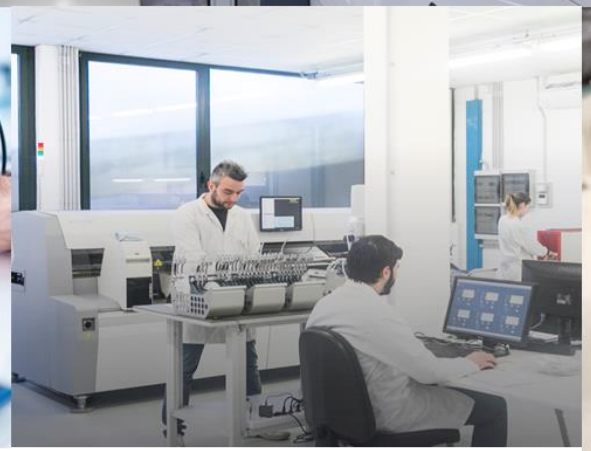
Enablers for IoT and electronic

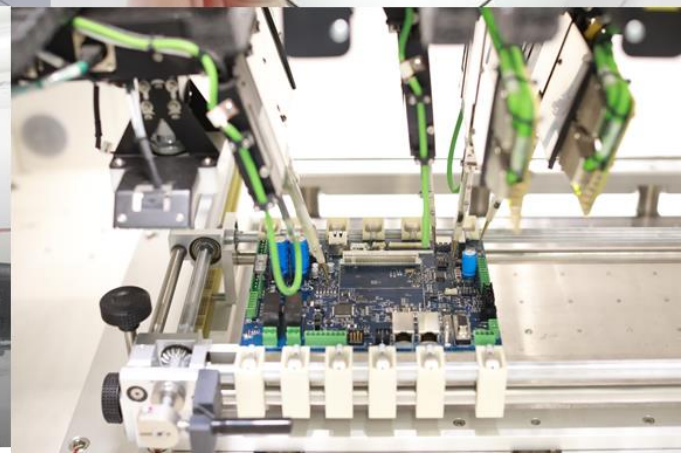
FAE TECHNOLOGY: company overview







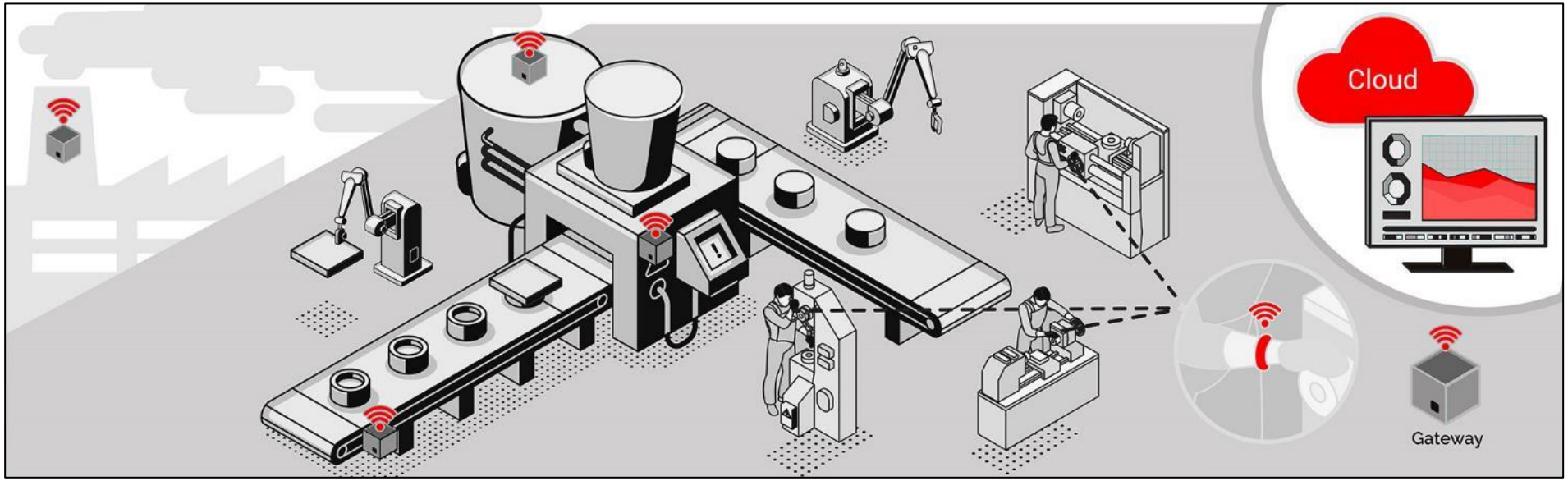




SNIPE Project

Sensor Network for Intelligent Predictive Enterprise
www.kilometrorosso.com/en/services/projects/snipe-en/

SNIPE project, lead by **FAE Technology** is one of the European R&I projects funded by the Open Call #1 of the Trinity Consortium of Digital Innovation Hubs (https://trinityrobotics.eu/) for advanced robotics, IoT and cyber security technologies to support the introduction of Agile Manufacturing in the production processes.

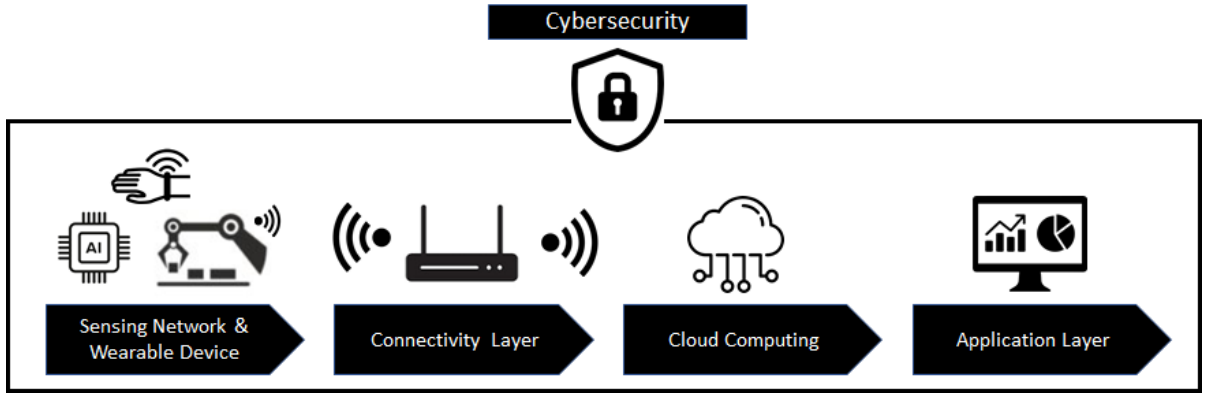


SNIPE Project Overview

SNIPE project will create an **AI** (Artificial intelligence) enabled **IoT** network system for machinery Revamping in foundries, to have a real-time monitoring of production processes and enable predictive maintenance on critical phases.

A **modular Smart Monitoring** infrastructure will be developed to collect machine process data (temperature, engine vibration, humidity etc.) and predict maintenance on critical processes through custom algorithms with the scope to reduce energy consumption and increase Overall Equipment Effectiveness (OEE).

Cybersecurity is a fundamental element of the proposed architecture: cybercrime and hacking can become even more of a threat when the whole plant is Cloud connected, therefore SNIPE will have a dedicated cross-activity focused on the implementation of a best-in-class cybersecurity approach from sensor to Cloud.



SNIPE Technical breakdown

SNIPE project will create an end-to-end solution, therefore several IoT layers must be developed and designed through parallel project activities:

- ✓ **Sensor Network** (HW/ FW design and prototyping): custom sensor IoT nodes to be implemented, collecting data and parameters from the field (vibration, gyro, belt thickness, humidity, energy consumption…).
- ✓ **Wearable device**: demo units based on BLE connectivity to push information to workers through haptic motors, vibration and LED.
- ✓ **IoT Gateway**: multi-protocol data gathering device, to collect data from IoT sensors and transfer to Cloud platform with MQTT communication protocol.
- ✓ **Cloud Dashboard**: data visualization, storage and data analysis.
- ✓ **AI algorithm**: custom algorithm to enable prognostic maintenance operations with a machine learning model based on raw data collected from the field.
- ✓ **Cybersecurity E2E suite**: secure procedure for Device certification, Private Key generation and connection protocol with crypto Token Key to secure data exchange.

Belt conveyor monitoring

- IoT sensors have been applied to some critical belt conveyor machines, collecting process data in Real Time such as engine vibration, noise, temperature, current consumption and speed of rotation of the driving drum.
- Other IoT sensors have been applied to detect in Real Time the thickness of the belt, using ToF sensors.
- All the data collected from the field are transmitted to an IoT Gateway through a dedicated Wi-Fi network connection and then sent to the Cloud monitoring platform to create a custom predictive maintenance algorithm.

Sensor Board with Wi-Fi module

Sensor Board with time of flight sensor

Humidity monitoring for green sand production

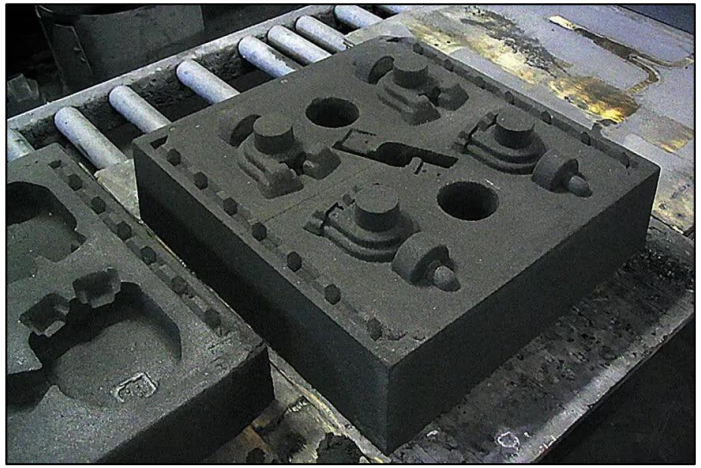
- IoT sensors have been applied to some specific measurement point in the production process for the green sand, in order to collect Real Time data for the Humidity % of the sand right before the moulding process. Humidity is a critical parameter that has a high impact on the down-time linked to the metal injection process.

- Environmental Humidity % is detected on critical areas to determine the influence on the final humidity range of the sand used in production line: all data are sent to the Cloud monitoring platform to create a custom algorithm to prevent the shift of the humidity level from ideal set-point.

Sensor Board with Wi-Fi module & humidity sensor

Humidity Sensor Probe

Sand pressing pistons.

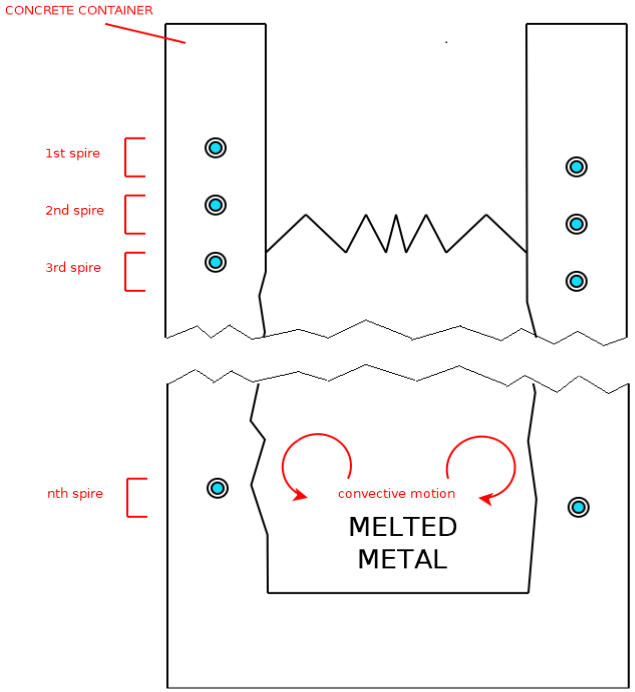


Sand mould

Energy monitoring on melting furnaces

- Working data and parameters are collected from the PLC of the melting furnaces in order to implement a detailed energy consumption analysis to prevent un-expected down-times. Operating data such as real time power consumption, temperature of the water in the heating spires, energy consumption are transmitted to the Cloud monitoring platform.

- Scope of this analysis will be to define a more detailed preventive maintenance of the melting furnace, by-passing a traditional approach of the time-based maintenance (typically four times per year).



Melting furnace layout

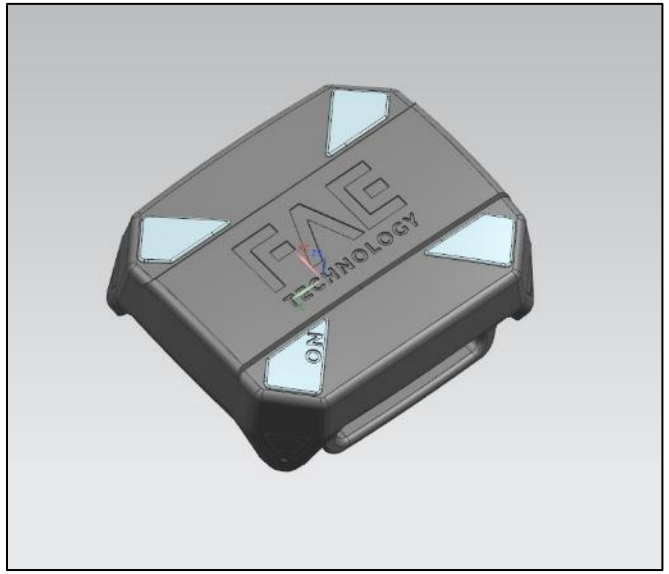
PLC for melting furnace

IoT Gateway (Modbus)

Wearable device for Smart Worker

- The information collected by the Smart Monitoring infrastructure are sent through Wi-Fi to the wearable devices provided to the operators in order to give vibration and light feedback: currently the IoT devices have been applied to give the user an immediate feedback on the detected Humidity % level of the sand before the moulding process.

- The wearable device unit integrates a microcontroller MCU Cortex-M7, a Wi-fi Module, a vibro-motor driver and 4 RGB LED plus a buzzer to transfer acoustic alarm to the operator.



3D render of wearable device

Sample of wearable device

Cybersecurity E2E approach

The main security requirements is to protect the data of the production process and to not have the Gateway being used as an entry point for the IT infrastructure of the site, as cybercrime can become a hack when machines and plants are connected to the Cloud.

A various set of security measures have been implemented to define a system that can cover the whole end-to-end data flow, such as:

- **DEVICE AUTHENTICATION**: devices of the system, sensors and gateways, are authenticated thanks to the use of a Public Key Infra-structure (PKI). Each device is equipped with a digital certificate that follows the standard X509 format.

- **PUBLIC KEY INFRASTRUCTURE:** PKI is a simplified version of the public key infrastructure used in the internet. It is based on a single root CA, with two intermediate CAs, the first for issuing certificates to the devices and the second for the certificates of the cloud services.

- **USER AUTHENTICATION:** definition and roles of the system installer, data user and system administration. A specific procedure will allow the initial enrollment of a brand new device into the system by the system installer.

- **SECURE COMMUNICATION**: the communication between sensor and gateway, and between gateway and cloud are protected using the standard TLS (Transport Layer Security). The communication between sensor and gateway, which is done over Wi-Fi, is protected by the dedicated WPA mechanism.

- **SECURE FIRMWARE UPGRADE:** One fundamental property of every device is the capability to upgrade its software with a secure mechanism. This allows the upgrade of the devices only in case of genuine software dispatched by the system administrator.

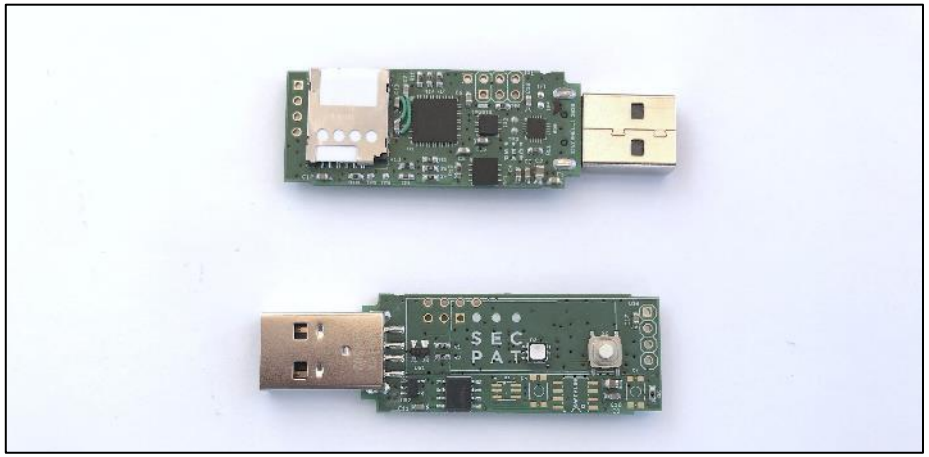
Cybersecurity for Hardware devices

- Authentication of the IoT devices on the Cloud platform is managed via digital signatures: the Private Key is securely stored in each device using a secure element.

- The Secure Element board is a custom board developed to be used in addiction to the IoT Sensor Node, to store the Private Key in a safe way. In the case of the IoT sensors, the secure element is directly connected to the microcontroller installed on the board, while in the case of the IoT Gateway the secure element has been developed on a USB dongle.

- Secure Element boards have been developed in partnership with our partner in FAE Technology HUB, Security Pattern (https://www.securitypattern.com).

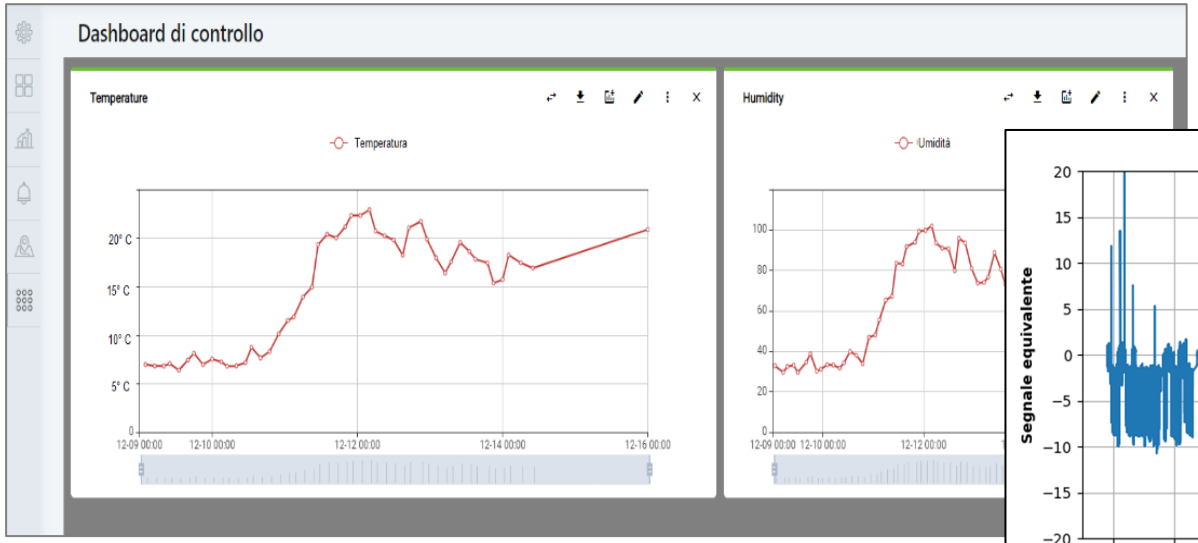
Custom Secure Element board for IoT sensor

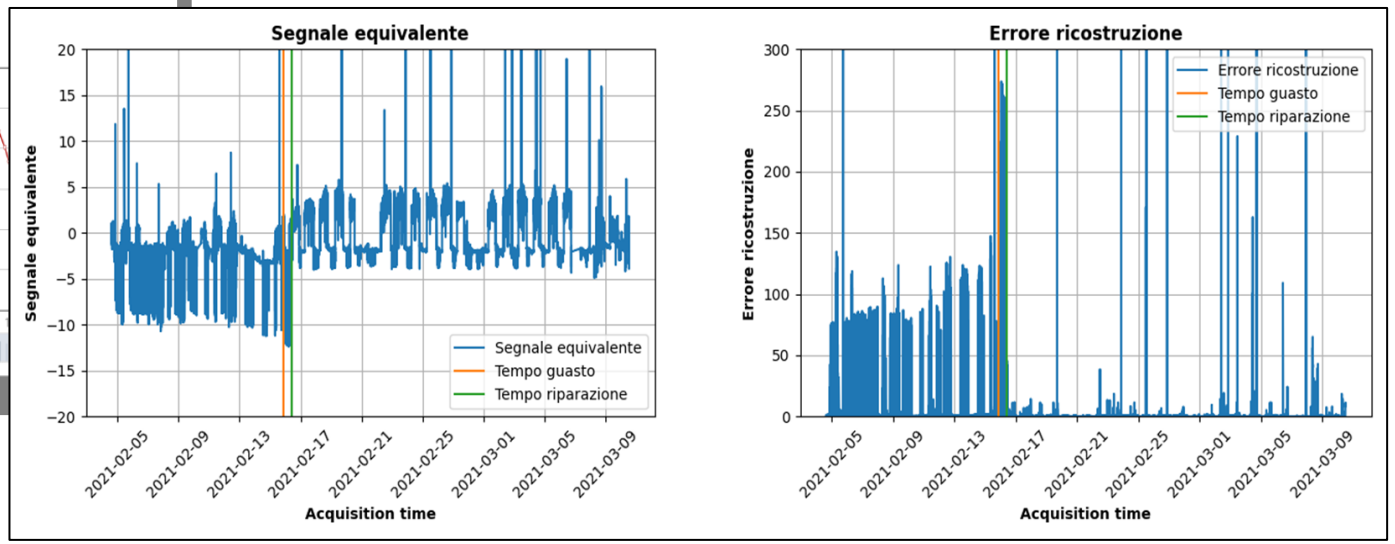


Custom Crypto USB dongle for IoT Gateway

Cloud Dashboard for Smart Monitoring

- The information collected by the Smart Monitoring infrastructure are showed in a Cloud Dashboard and raw data are used to build the AI model for predictive maintenance and prognostic fault detection.
- The access dashboard gives visibility to the enabled sensors and shows the complete list of sensors and their details, the communication state of each sensor (on-going communication, anomaly, alarm, no-communication) and the sensor localization on the floorplan.





Consortium PARTNER overview

Technology end-to-end provider, Hardware Firmware and Software development.
www.fae.technology

Foundry company, end-user of SNIPE technology demonstrator.
www.arizzifonderie.com

Innovation district, partner for communication & dissemination activities.
www.kilometrorosso.com

Thanks!

FAE TECHNOLOGY S.P.A

Via C. Battisti, 136 - Gazzaniga (BG) - 24025 – Italia

P.IVA 02032310167 - T +39 035 73 81 30

info@fae.technology - www.fae.technology