DigiFed

Expertise

Advanced Technology

Digitising Europe's Industry Together

Competencies

Funding

Innovative Solutions

Technical offer Webinar

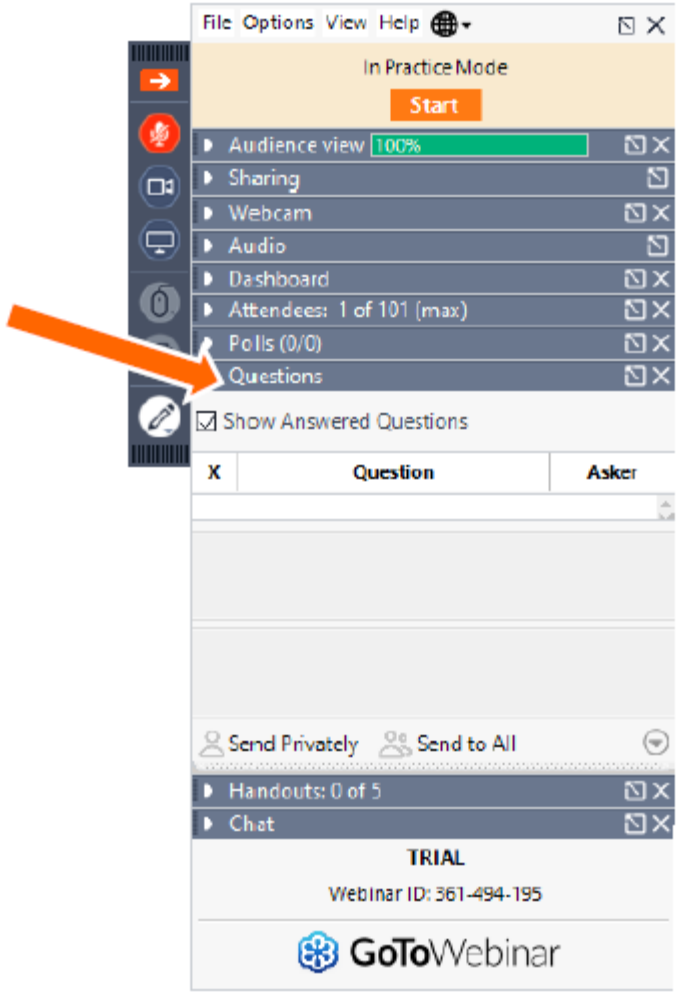
17/03/2020

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864266.

Welcome

Before we start

- This webinar will be recorded & published
- During the webinar you can use the question box to ask all your questions, we will answer them during the Q&A session at the end
- After the webinar, the slides will be available for download on the Digifed website : https://digifed.org/



Before we start

- There will be 1 more webinar in this series to present the second part of the project's technical offer :

24/03/2020

ikerlan

life.augmented

Univerza v Ljubljani

MŰEGYETEM 1782

CATAPULT Digital

Register →

What is DigiFed?

DigiFed is a EU funded innovation action on the H2020 programme

Drive innovation across European SMEs via large scale adoption of Cyber Physical Systems (CPS) & embedded Systems

12 Partners from 9 European Countries

Duration: 3 years, 01 January 2020 to 31 December 22,

Cascade Funding: € 3.9 million in direct support for SMEs and MidCaps

DigiFed offer :

“Application Experiment” projects

- 55k€ Funding to carry out Digital product / service demonstrators
- Technical expertise & innovation management expertise

2 types of Application Experiments

- SINGLE: a company has the idea of an innovation, clear market vision, need technical support to validate the concept and partners up with a Digifed member (up to 55 k€)
- TWIN: two companies partner up: the first one hase the idea of an innovation and technical support is provided by the second company (up to 110k€, 55k€ each)

DigiFed Open Calls

40 projects will be funded

3 open calls for projects

- 1st call : opens today (17/03/2020) and closes on 09/06/2020 at 5pm.

What happens next :

- Evaluation committee in june/july
- Confirmation of the selection by European commission in July
- Notification of selection 4 & 5 of August
- Contract signature & kick off of the experiment in september

How to apply ?

- All information available on the website at https://digifed.org/explore/

- 1st step : register on the website

- Then submit before the 9th of June, 5pm :
  - 1 written proposal, technical oriented
    → 10 pages document

  - 1 recorded pitch, business oriented.
    → 5 minutes video

Criteria to be eligible

- **To submit on time**

- **To submit a cross-border proposal**

  → 2 organisations from different countries

- **Company profile:**
  - Start-up / SME / Mid-cap
  - Required resources for implementation
  - Agree to sign the standard contract if selected
  - Based in EU member state or EU associated country*

  (https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf)

Funding conditions

- 70% of the budget (declared costs)
- Max of 55 k€ per company per project
- Max of 100 k€ per company if DigiFed multiple projects
- Max of 100 k€ FSTP funding per company under SAE and I4MS (H2020)

As per European Commission's rules, financial support will not be awarded for work previously or currently funded under any other (Regional, National or EU) programme.

Upcoming important dates

Event	Date
Launch of the first open call	Today : 17/03/2020
Webinar 3: Technical offer	24/03/2020
Closing of the first open call – **Application Deadline**	09/06/2020 5pm
Notification for selection to all companies	04 - 05/08/2020

SECURE infrastructure for trusted IoT platform

- **Function**: security infrastructure establishing an environment to isolate trusted code executed or data manipulation by an IoT platform from an untrusted world
- **Principle:**
  - Integration of a secure hardware module
  - Integration of a trusted OS isolated from Linux with hardware mechanisms
  - Drivers and software bricks to drive the secure hardware module inside the trusted OS
  - Interfaces between untrusted world and trusted world to drive the secure hardware module.
- **Key Performances:**
  - The security hardware module accesses and sensitive data manipulation are hardware isolated from untrusted OS
  - Trusted applications can be developed to have secure services interfacing with untrusted OS
- **Uniqueness:**
  - Hardware isolation from an untrusted world for secure hardware module accesses
  - Stack in trusted OS for hardware secure module accesses
  - Bridge between untrusted OS and trusted world

- **Maturity/TRL:** Technology Readiness Level

1 2 3 4 5 6 7 8 9

- **Applications:**
  - Any application using a set of IoT devices to collect personal and/or critical data
  - Support for IoT applications developers to secure their product
  - Smart factories, Energy production and distribution, Healthcare , critical infrastructure

Example of SECURE infrastructure implementation using STM secure elements STM32 and TPM with Linux

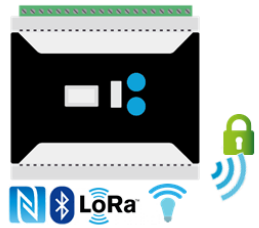
DEPL- IoT

- **Function**: End-to-End secure commissioning of iot systems, allowing to configure, deploy, and manage a product's lifecycle
- **Principle:**
  - Standardized security protocols and cryptographic primitives
  - Allows TPM integration for secure storage
  - Configuration deployment within IoT networks and robot swarms
- **Key Performances:**
  - Multiple wireless communication interface support (Bluetooth, NFC, or VLC…)
  - end-to-end security during the commissioning phase of a single device or a complete IoT network
  - lifecycle management with alert and logs monitoring and end-of-life support.
- **Uniqueness:**
  - Easy integration on existing hardware platforms
  - Low cost, low power and easy board integration
  - Simplicity of on-site configuration with smartphone application

- **Maturity/TRL:** Technology Readiness Level

1 2 3 4 5 6 7 8 9

- **Applications:**
  - Designed for Industrial-IoT networks, for automatic factory configuration or on-site deployment using a smart-phone application
  - Smart factories and Predictive maintenance
  - Smart cities, Home automation
  - Critical systems , Energy production and distribution;
  - Healthcare monitoring, hospital
  - Automotive and smart transportation, Drone swarms



Security assessment

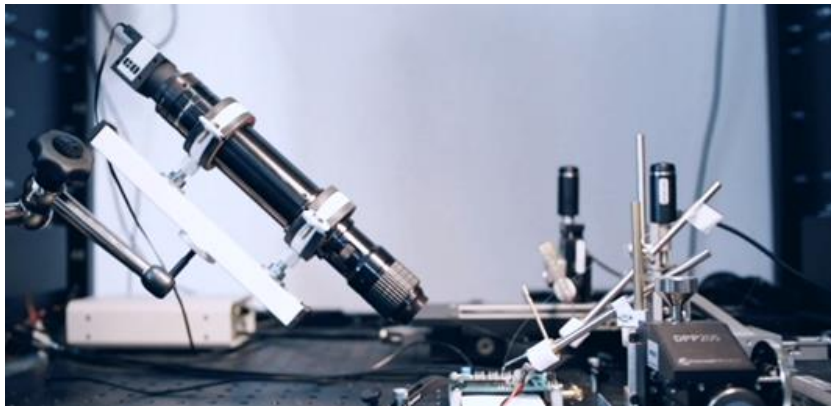
- **Service**: Security assessment of Digital prototype

A first security assessment for prototype devices to ensure a “secure by design” approach
Provide at early stage in the development process, feedback to developers to enhance their security features.

- **Key Performances:**
  - Analysis of the device to identify potential vulnerabilities
  - Draw up a test plan
  - Perform penetration testing that may include: Attacks on interfaces/ Physical tampering/ Side channel analysis/ Fault injection
- **Uniqueness:**

Skills of LETI ITSEF (Information Technology Security Evaluation Facility) are proven by its accreditations (ANSSI, EMVCo..) for evaluations up to highest Assurance Levels

- **Applications:**
  - This expertise is proposed for innovating designs in hardware, embedded software, or prototypes of ICT products that are aimed at applications **where confidentiality, integrity, availability, privacy shall be implemented.**
  - The evaluation may also focus on a new specific HW or SW security functionality in order to verify its efficiency.

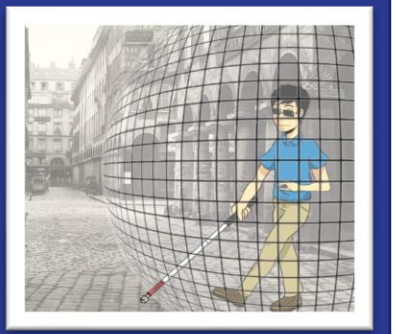


Test benches used for penetration testing on an IC

SigmaFusion™ for environment perception

- **Function**: fuse range data to build a digital model of the environment in the form of an occupancy grid
- **Principle:**
  - **Bayesian fusion** based on **integer arithmetic**
- **Key Performances:**
  - Real-time fusion of a huge quantity of data
  - Light-weight computing solution
- **Uniqueness:**
  - "Embeddable" on microcontroller
- **Maturity/TRL:**
  - Technology Readiness Level
  - 1 2 3 4 5 6 7 8 9
- **Applications:**
  - Environment perception for Automotive
  - Environment perception for urban mapping
  - Environment perception for obstacle detection embedded in a portable device – application to a smart white cane


3D dense occupancy grid with 1W PW budget, computed with 2 Velodyne VLP16



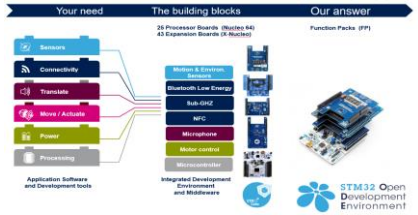
STEVAL Boards & X-Nucleo STM32 ODE

- **Function**: Fast, affordable prototyping with development and to facilitate the next hardware design.

- **Principle:**
  - STMicroelectronics Italy provides access to X-Nucleo to work in synergy with the STM32 environment to create advanced solution on smart industry, IoT, smart farm, motor control, Smart sensing
  - expansion board functionality through high-level APIs and sample applications
  - STEVAL boards to evaluate the features and performance of selected products and to facilitate the next hardware design

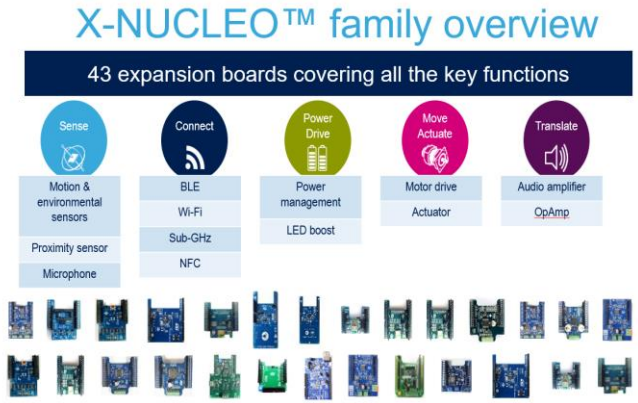
- **Key Performances:**
  - X-Nucleo on five key functions:
    Sense, Connect, Power Drive,
    Move& Actuate , Translate
  - STEVAL board with focus in four areas
    Power, Led Ligting, Motor Control, IoT

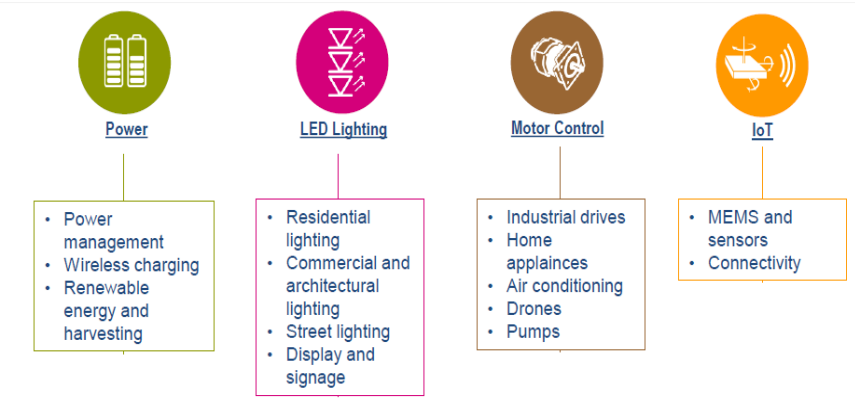
- **Uniqueness:**



- **Maturity/TRL:**
  - Technology Readiness Level

- **Applications:**
  Smart Industry, Smart City, Smart Home, Smart Things, Smart Farm…

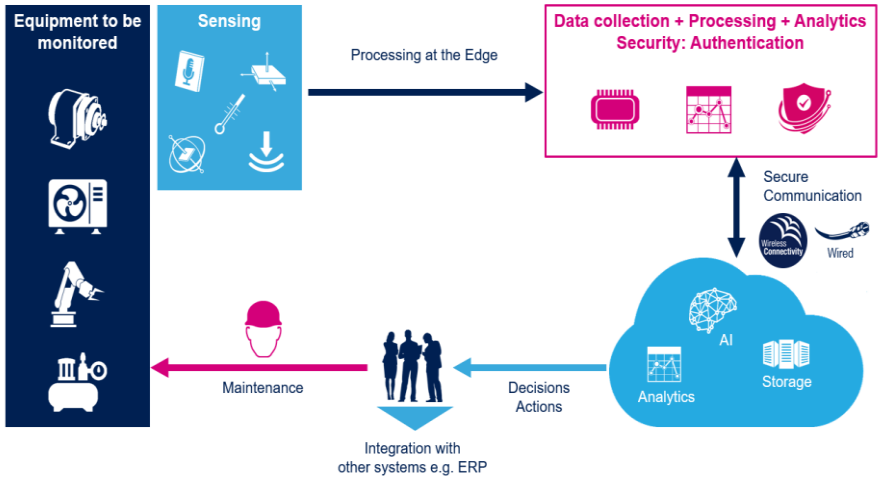




Condition monitoring

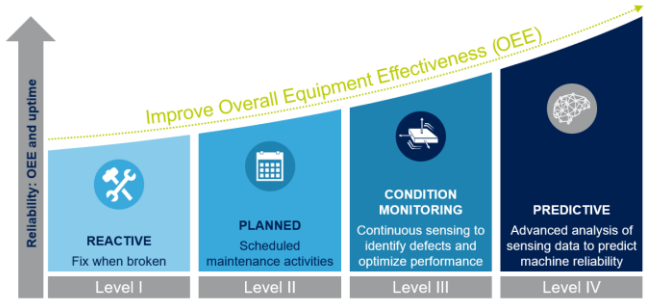
- **Function**:
  Continuous sensing to identify defect and optimize performance to exploit advanced analysis of data to predict machine reliability

- **Principle:**



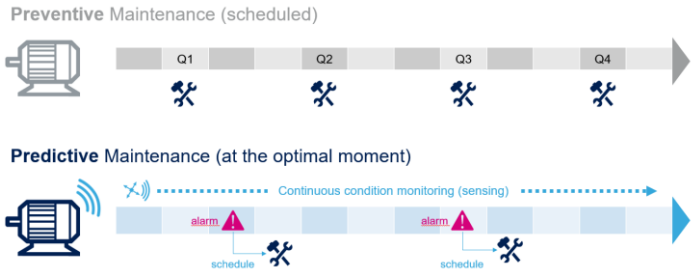
- **Key Performances:**
  - Minimizes the impact on production and optimize operative cost

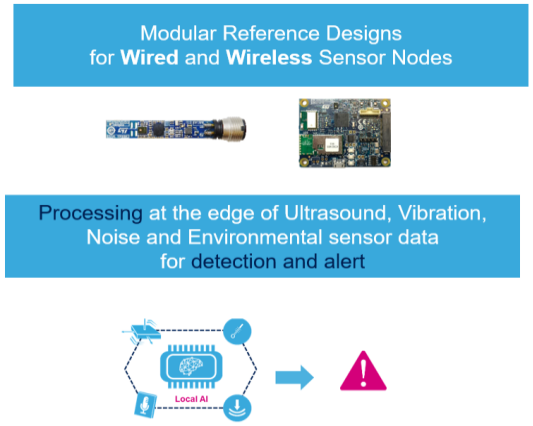
- **Uniqueness:**

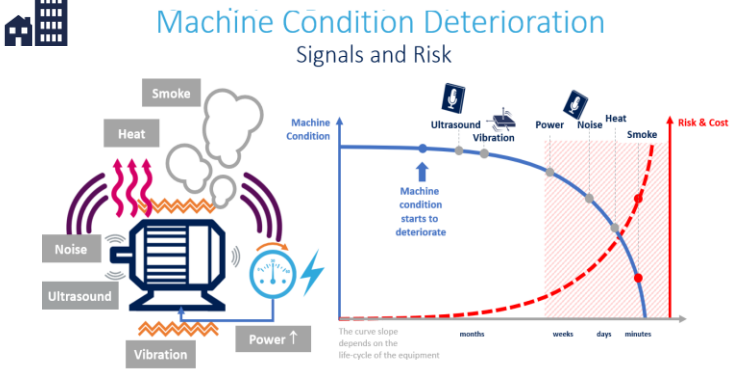


- **Maturity/TRL:**
  - Technology Readiness Level

- **Applications:**
  Smart Industry, Smart Home

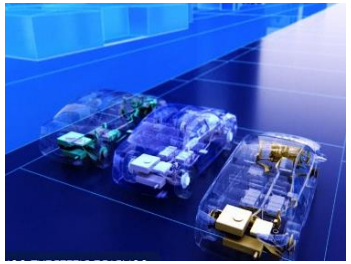






Integrated and Open Development Platform (AVL)

- **Function**: integration of all elements of the vehicle development process independent of tools
- **Principle:**
  - Utilising platform to integrate real (HW) and virtual (simulation models) development methods into a single framework
  - Bridge the gap between individual results to provide reliable, holistic decisions
  - Bringing transparent contributions into an overall context
- **Key Performances:**
  - Model.CONNECT™ enables communication between simulation models of different components and systems
  - Testbed.CONNECT™ merges simulation models and testbeds into a complete system
  - Data.CONNECT™ connects data from different sources
  - Device.CONNECT™ is a highly secure data transmission pipeline
- **Uniqueness:**
  - Collaboration through step-by-step integration
  - 100% focus on functioning structures
  - Smooth interaction of teams, processes and tools
- **Maturity/TRL:**
  - 1 2 3 4 5 6 7 8 9
- **Applications:**
  - Optimal vehicle design with exchangeable models and creation of design variants
  - Step-by-step integration of virtual/real network of the hybrid powertrain
  - Linking model libraries of different powertrain components and synchronizing them to design processing
  - Determine the optimum time for updates and maintenance work on the basis of data analysis



DigiFed

Q&A SESSION

Time for you to ask your questions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864266.