DigiFed

CYBERSECURITY techno for DigiFed

12th May, 2020

CEA Leti NanoElec
Ikerlan

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

Welcome

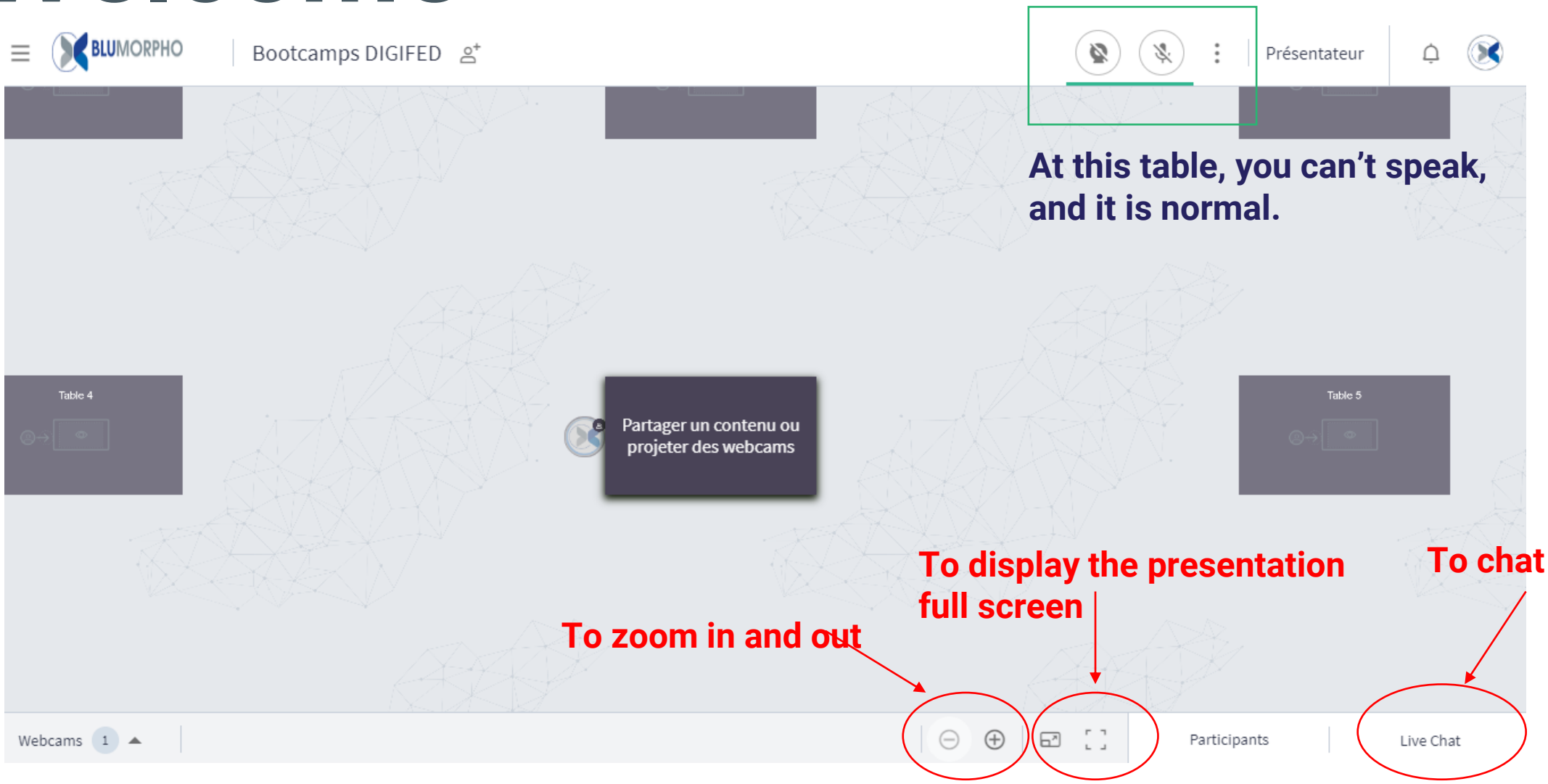
leti
cea tech

NANOELEC.

BLUMORPHO

ikerlan
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

Welcome


BLUMORPHO
Bootcamps DIGIFED
Présentateur
At this table, you can't speak, and it is normal.
Table 4
Partager un contenu ou projeter des webcams
Table 5
To zoom in and out
To display the presentation full screen
To chat with us
Webcams 1
Participants
Live Chat

Agenda

- **Introduction, objectives and agenda** (5 minutes)
- **Introduction to Open call proposition** (5 minutes)
- **Cybersecurity technologies proposedby DigiFed partners** (50 minutes)
  - CEA-LETI (25 minutes)
  - Ikerlan (25 minutes)

- **Open floor discussion between participants and DigiFed experts**
  - **Q&A** (55 minutes)

Two types of Application Experiment

SINGLE AE: one company (55k€ max)

- Company : idea of an innovation, clear market vision, need technical support to validate the concept
- DigiFed technical partner: bring the technical expertise to the company
- DigiFed Innovation partner : bring expertise for innovation and business

TWIN AE: 2 companies from 2 different countries (2x 55k€ max)

- Company #1 : idea of an innovation, clear market vision, need complementary expertise to validate the concept,
- Company #2 : bring the complementary expertise to realize the prototype
- DigiFed Innovation partner : bring expertise for innovation and business

Open Calls: Proposal Submission

- **Registration on the website**

- **Proposal submission in two documents**

- Proposal description
  - ~10 pages, pdf document, written in English
  - Technic oriented
  - Proposal template

Excellence
Impact
Quality

- Recorded pitch
  - 5 min, in English
  - Business oriented
  - Slide deck template

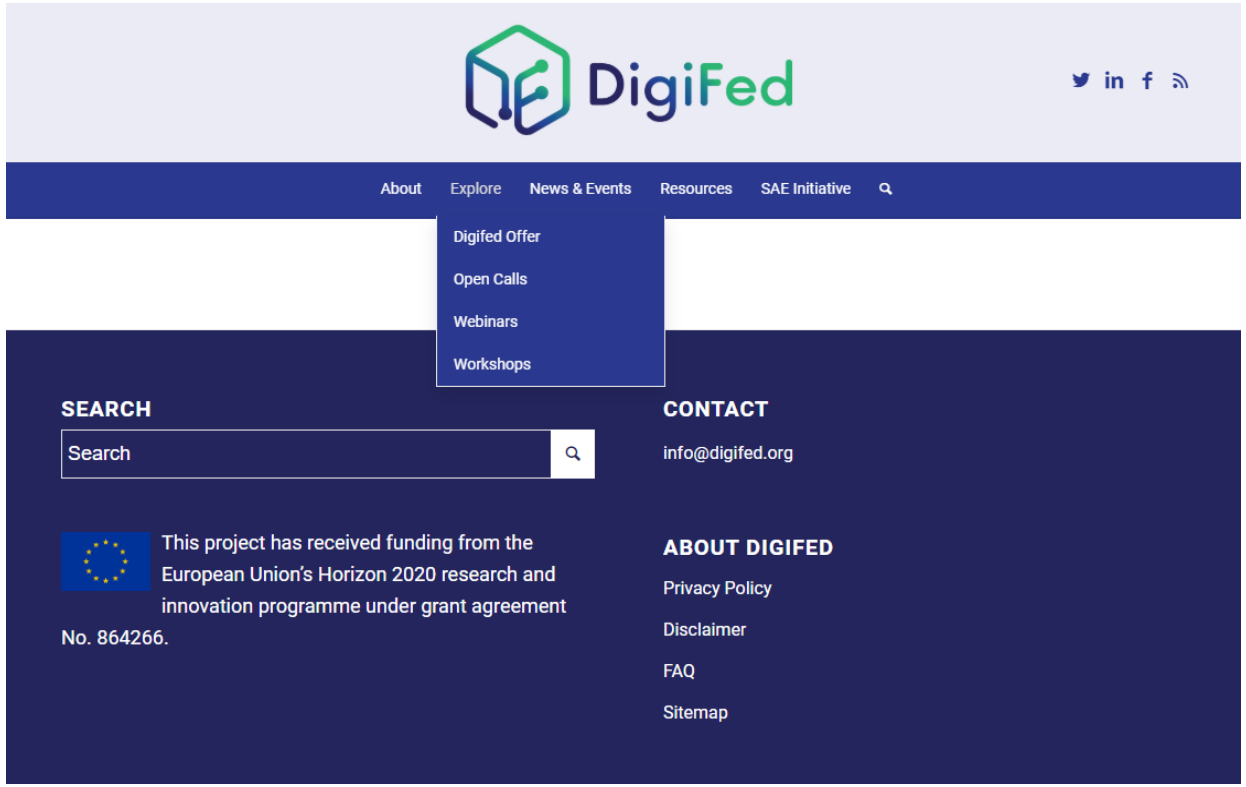
Business quality

Guidelines through bootcamp, webinars

Direct contact with DigiFed partners

DigiFed Open Calls - how2

- Open call will look for SINGLE / TWIN Application experiments
- All information available on the website at https://digifed.org/explore/

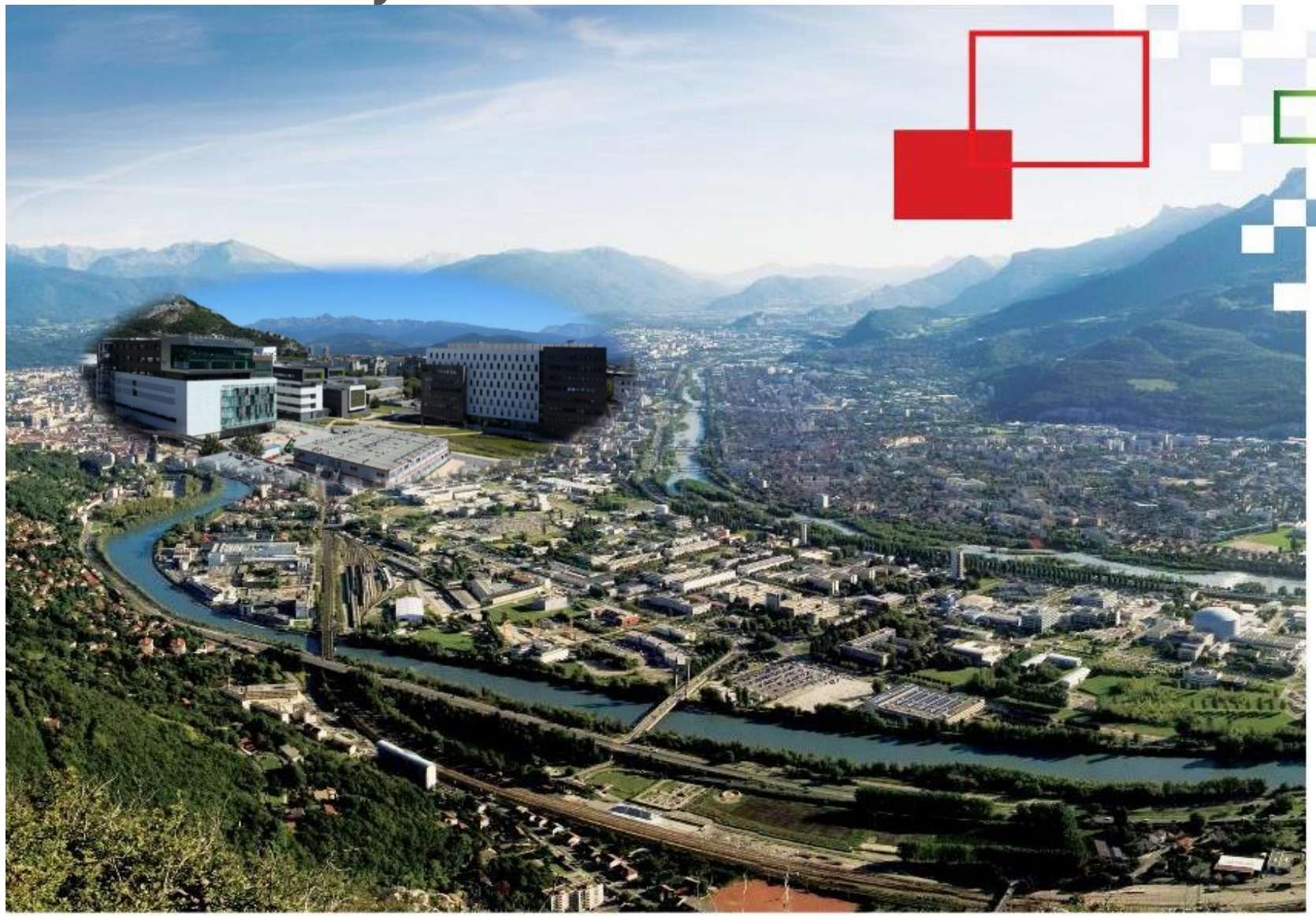


DigiFed

CEA LETI ACTIVITY in CYBERSECURITY

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

Micro & nanotechnologies R&D partner to build your next best tech innovations



- Since **1967**
- France, USA, Japan
- **2,000** People
- **> 2,760** Patents in Portfolio
- **350** Industrial Partners
- **> 65** Startups Created
- **10,000 m²** Cleanroom 200-300mm
- **315 M€** Budget
  (**85%** from R&D contracts)

CYBERSECURITY SERVICE FOR EMBEDED SYSTEM

Analyze systems and characterize the threats

Secure systems through patented HW/SW technologies

Security evaluation tools and capabilities (ITSEF)

Mission

- **Identify product vulnerabilities**
- **Develop innovative ways to protect hardware from cyber-attacks.**

An world unique innovation ecosystem to secure by design critical functions

- State-of-the art benches & tools
- A large patents portfolio
- Long time collaboration with academics and stakeholders

Research focus

- Attacks benches
- Security assessment and verification tools
- Hardware root of trust
- Disruptive technologies for cybersecurity

Teams in Grenoble & Gardanne

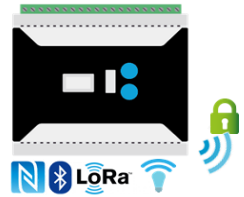
DEPL- IoT

- **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



Contact : Pierre-Henri.Thevenon@cea.fr

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

Contact : raphael.collado@cea.fr

Security assessment

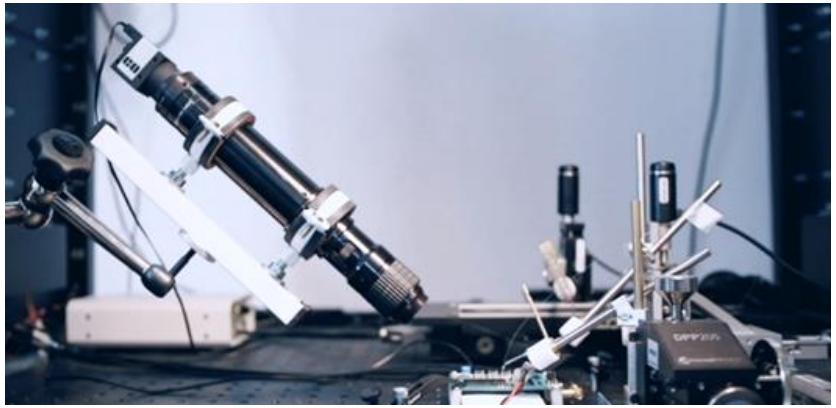
- **Service**: Security assessment of Digital prototype

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

Contact : Guillaume.herve@cea.fr

DigiFed

IKERLAN CYBERSECURITY OFFER FOR OPEN CALL

ikerlan

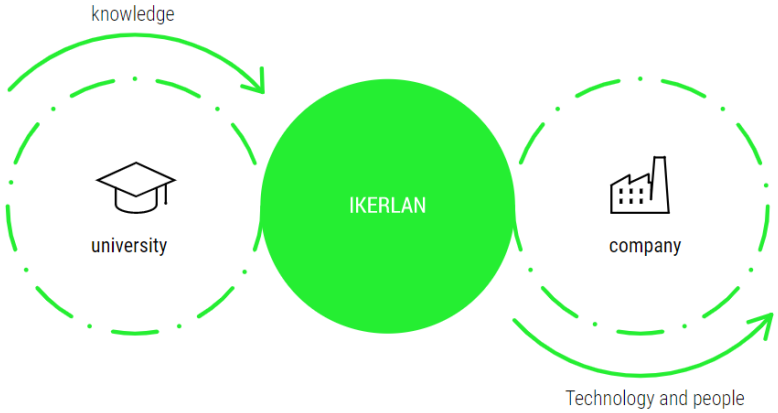
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

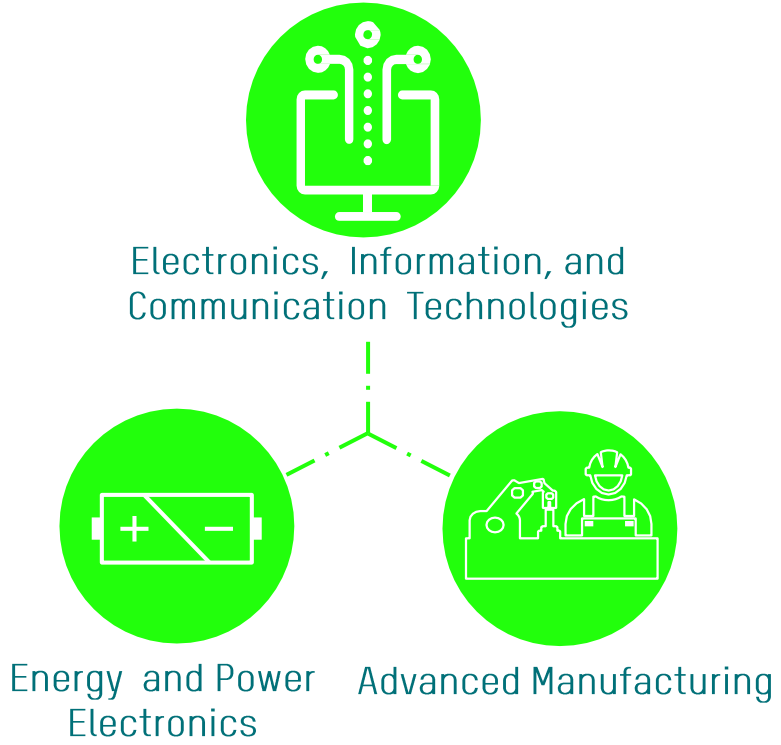
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 864266.

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

IKERLAN:
where technology is an attitude

IKERLAN **is a leading knowledge transfer** technological centre providing competitive value to companies. We seek for excellence in R&D&i, thanks to the continuous adaptation to **the needs of our customers** and the proximity with the business reality.



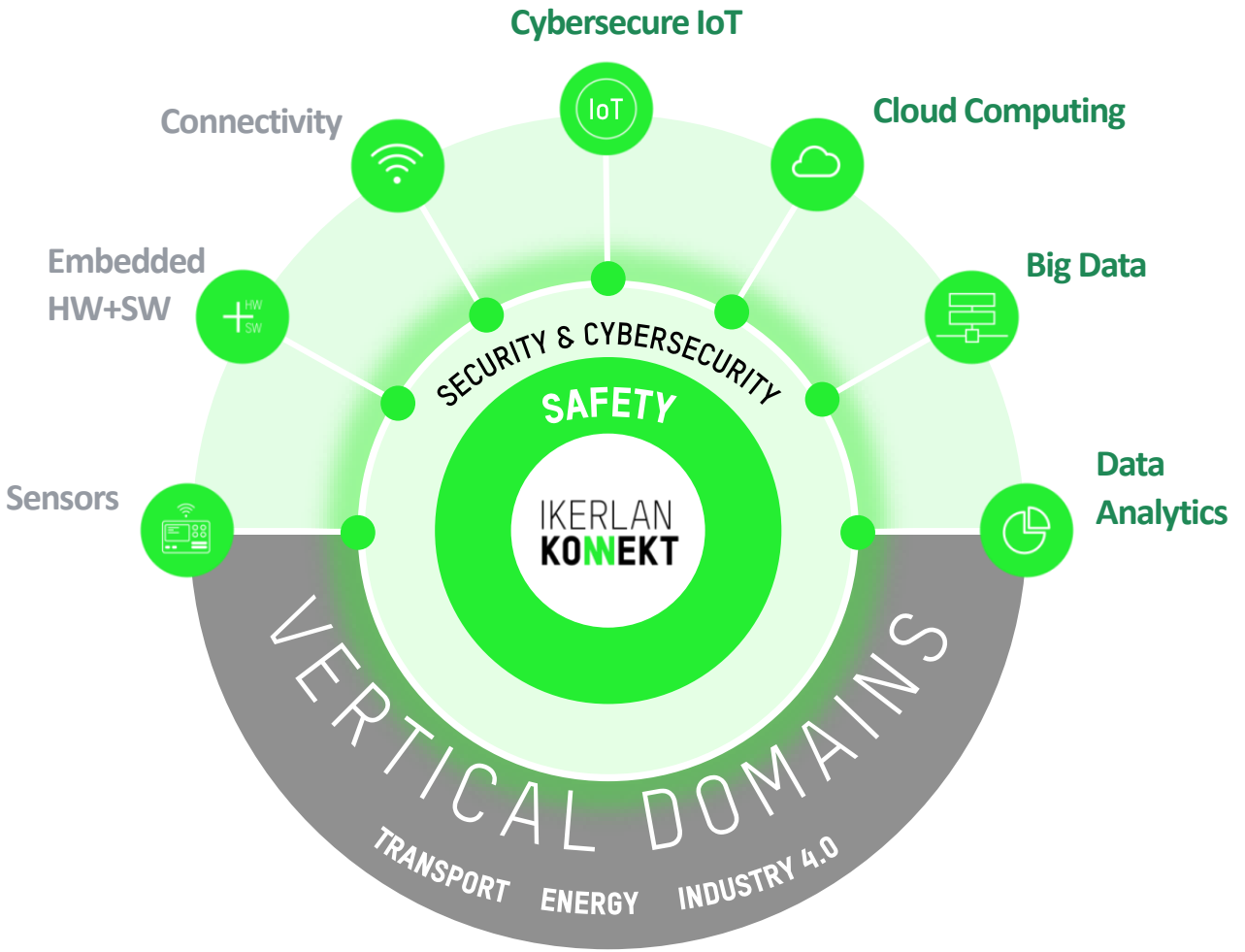


Technology Recap

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Cybersecurity for Embedded Systems

- Industrial Components
- Certification & Validation
- Dependable Software
- Security Boot, PKI certif.
- Auth. access



Cybersecurity for Digital Platforms

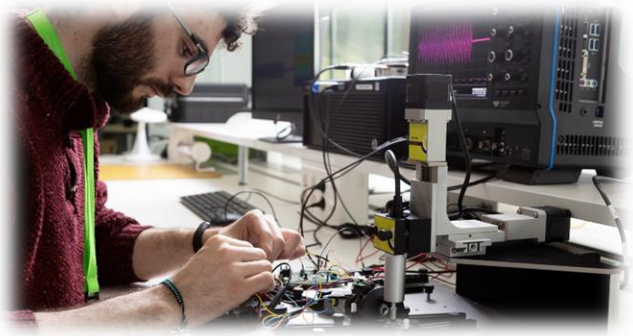
- Remote updates
- Data Privacy
- Blockchain
- Payment systems
- PKI Architectures

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Industrial cybersecurity

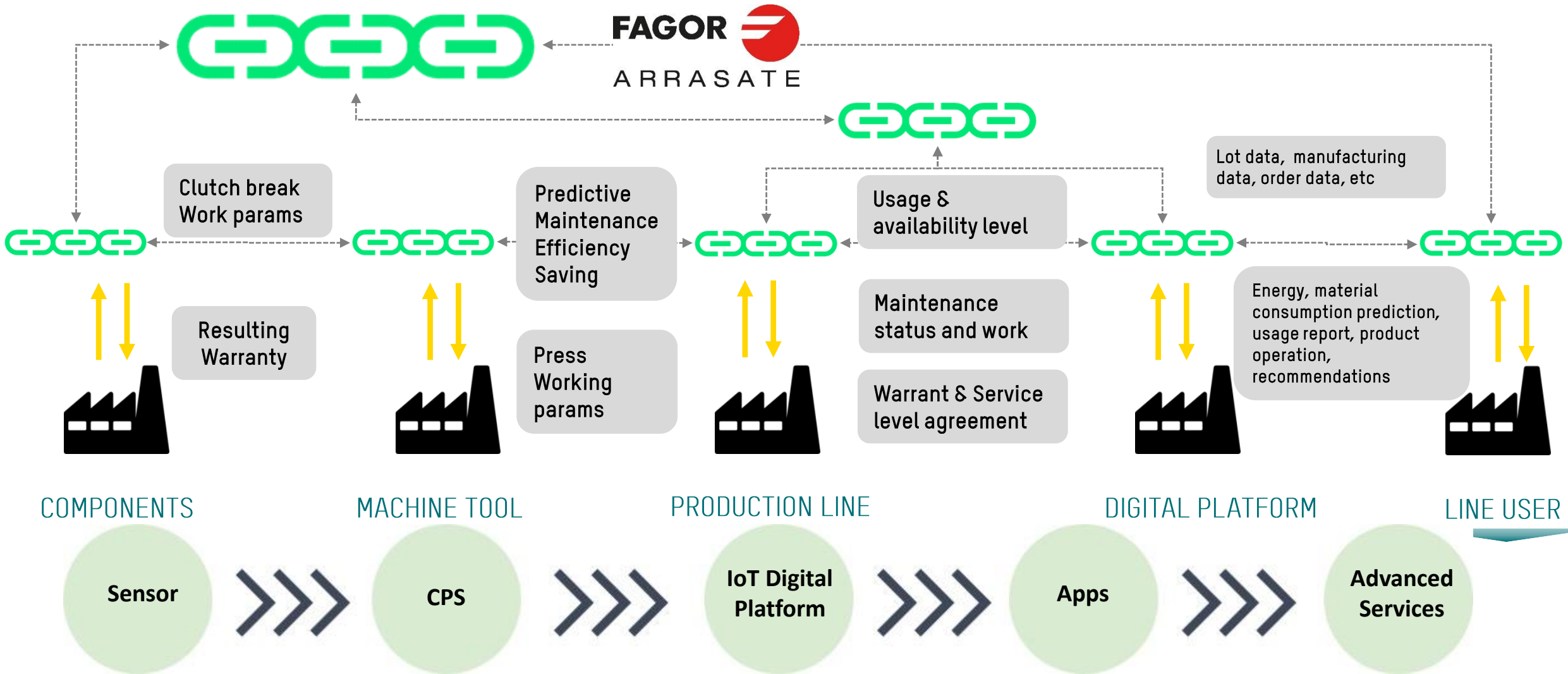
- **Function**: Protection of embedded electronic systems and digital platforms
- **Principle:**
  - Embedded System Security
  - Security Evaluation
  - Cybersecure IoT, Cloud and User Interfaces
- **Key Performances:**
  - Security Life-Cycle and Certification
  - Trust Technologies based on Distributed Ledger Technologies
- **Uniqueness:**
  - Certified methodologies and addressing compliance with product cybersecurity standards
  - Cybersecurity solutions covering the entire value chain: from the sensor, the electronics, the embedded software, the connectivity solution, the processing and data ingestion platform, to the analytics and its advanced display

- **Maturity/TRL:**
  - Technology Readiness Level
  - 1 2 3 4 5 6 7 8 9
- **Applications:**
  - Cybersecure Digital platform and IIoT oriented to teleservice.
  - Cybersecure Digital platform for fleets of automatic warehouses. Multi-business deployment, multi-warehouse



ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

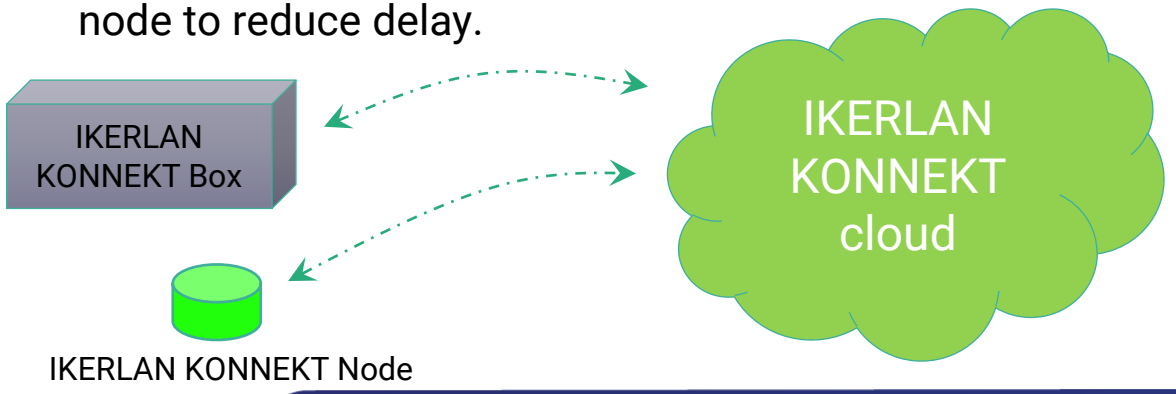
Digital Machinery Cybersecurity Functionalities



ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

AI-powered Digital Platforms

- **Function**: Digital Platform to provide tools to develop AI-powered fog/edge-to-cloud solutions.
- **Principle :**
  - Fog/Edge-to-cloud dynamic architectures.
  - AI-powered Digital platform scenario.
  - Microservices oriented edge devices architecture.
- **Uniqueness:**
  - **Artificial Intelligence**→ fog-to-cloud architecture.
  - **Microservices based architecture**→ Deployment of AI-models to the edge.
  - **Edge computing** → Early analytics in the edge node to reduce delay.

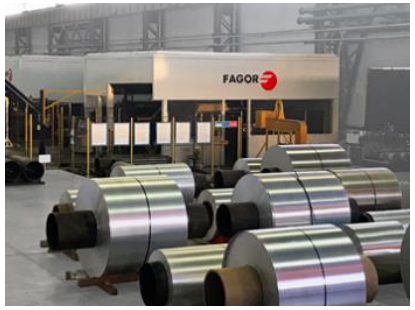


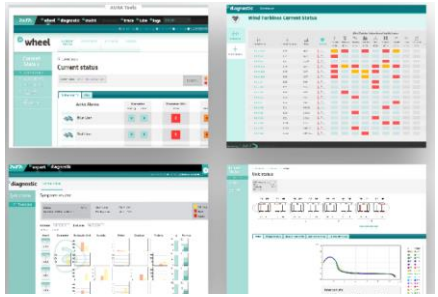
- **Maturity:**

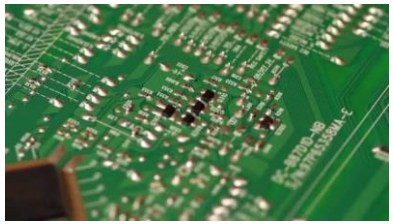
1 2 3 4 5 6 7 8 9

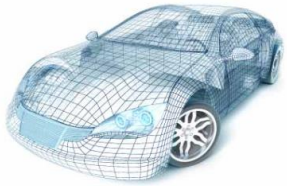
  - Heterogenous cloud architecture (private, public and hybrid).
  - Smart Data Lakes provisioning.
  - Microservice-oriented service deployment.
- **Key performances:**
  - AI-powered Digital Platform.
  - Data Lake provision for Data analytics.
  - AI-powered predictive techniques.
- **Applications:**
  - Industry 4.0 & Smart Factories.
  - Smart Cities.
  - Smart Living and Ageing Well.
  - Smart Mobility.
  - Smart Buildings.
  - Etc.

Industrial Partners









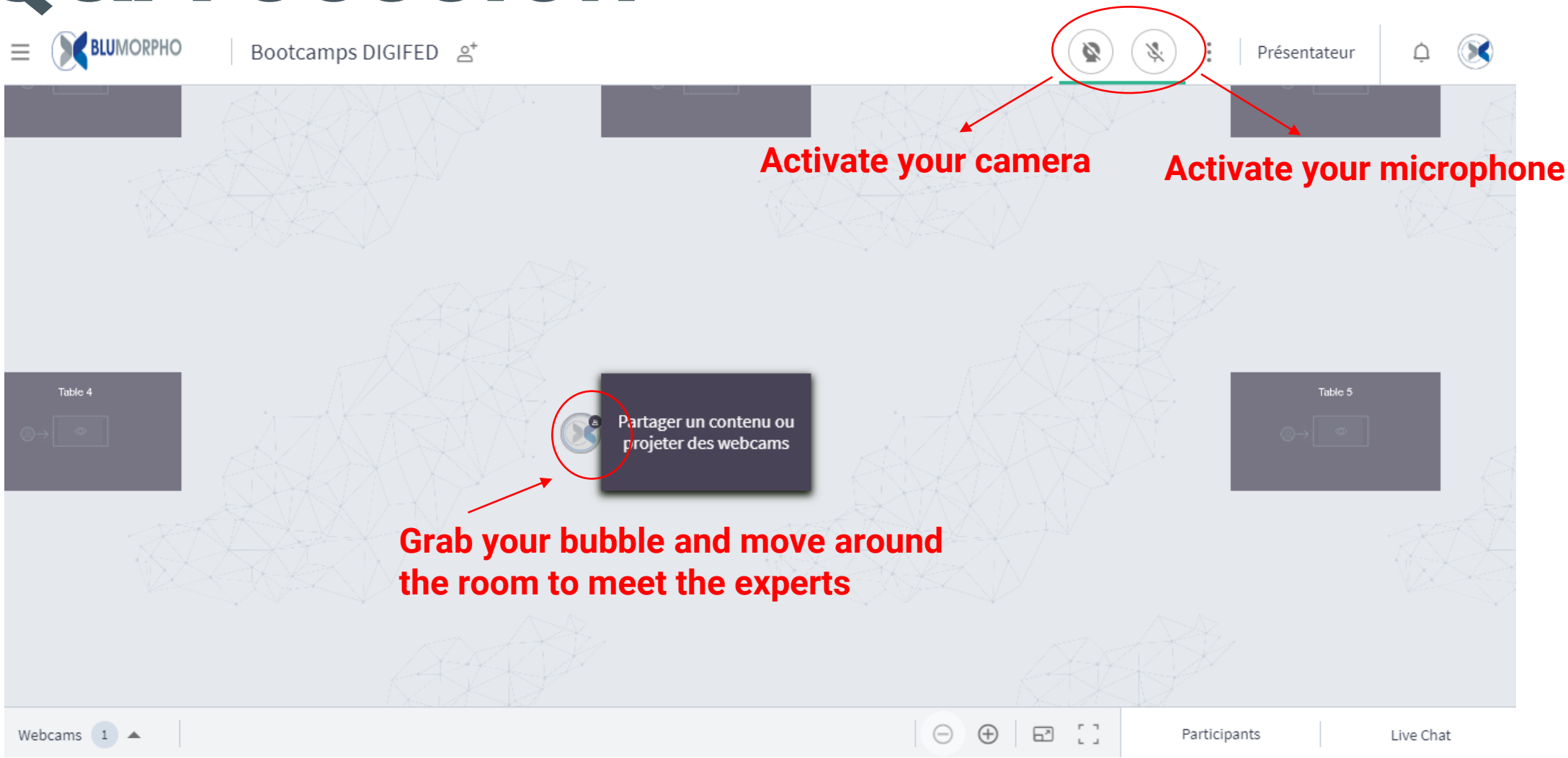
ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Industrial cybersecurity partners

Orona
CAF
FAGOR ARRASATE
LKS Next
Telefónica
NEM solutions
COUTH INDUSTRIAL MARKING SYSTEMS
Ingeteam
arteche
SIEMENS Gamesa RENEWABLE ENERGY
MONDRAGON ASSEMBLY
orkli
ULMA
Danfoss
its
FAGOR AUTOMATION
ONA WE ARE EDM

Introduction to the Q&A session

Q&A session


BLUMORPHO
Bootcamps DIGIFED
Présentateur
Activate your camera
Activate your microphone
Table 4
Partager un contenu ou projeter des webcams
Table 5
Grab your bubble and move around the room to meet the experts
Webcams 1
Participants
Live Chat

Q&A session

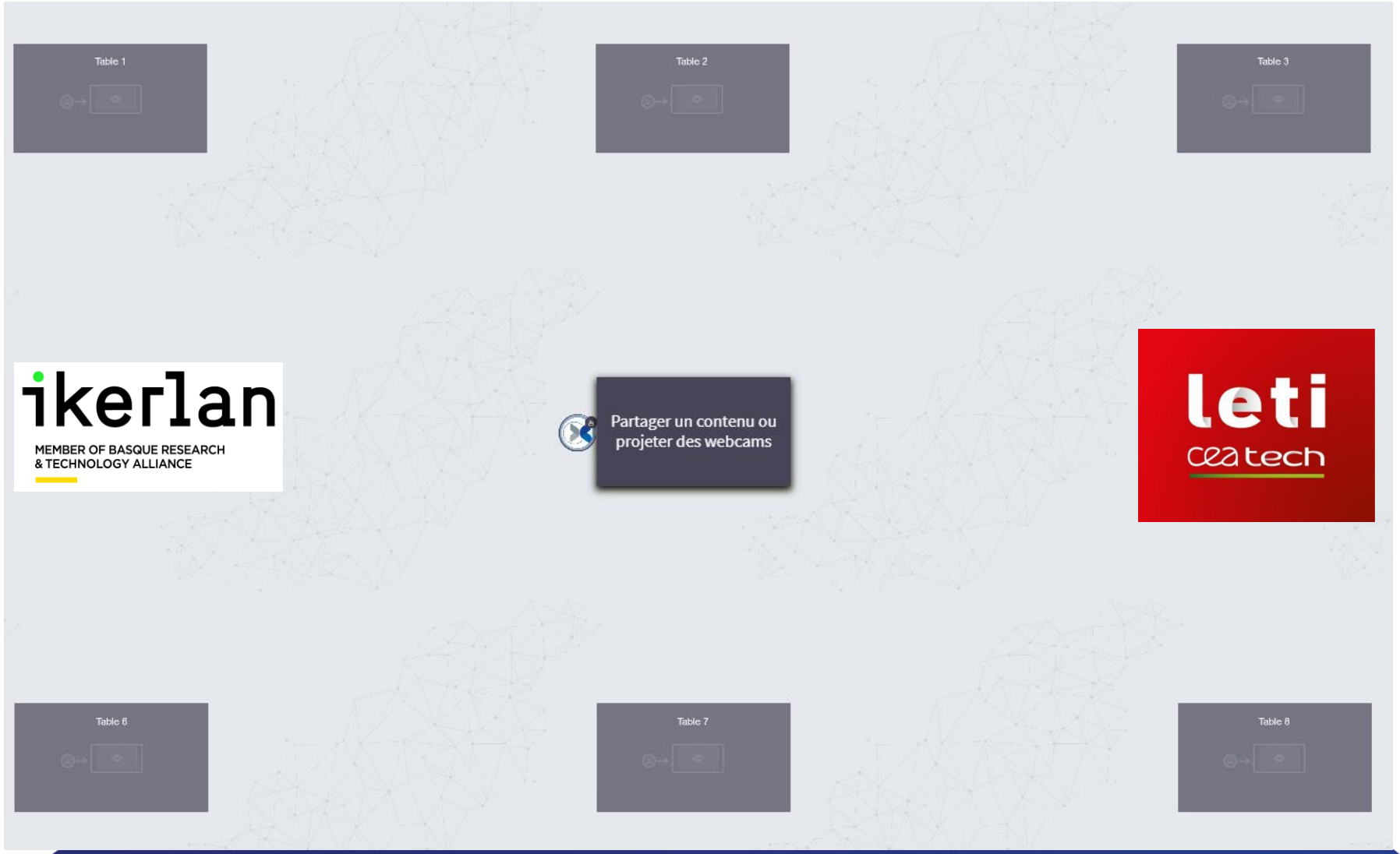


Table 1
Table 2
Table 3
ikerlan
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE
Partager un contenu ou
projeter des webcams
leti
cea tech
Table 6
Table 7
Table 8