CYBERSECURITY techno for DigiFed

3rd December, 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

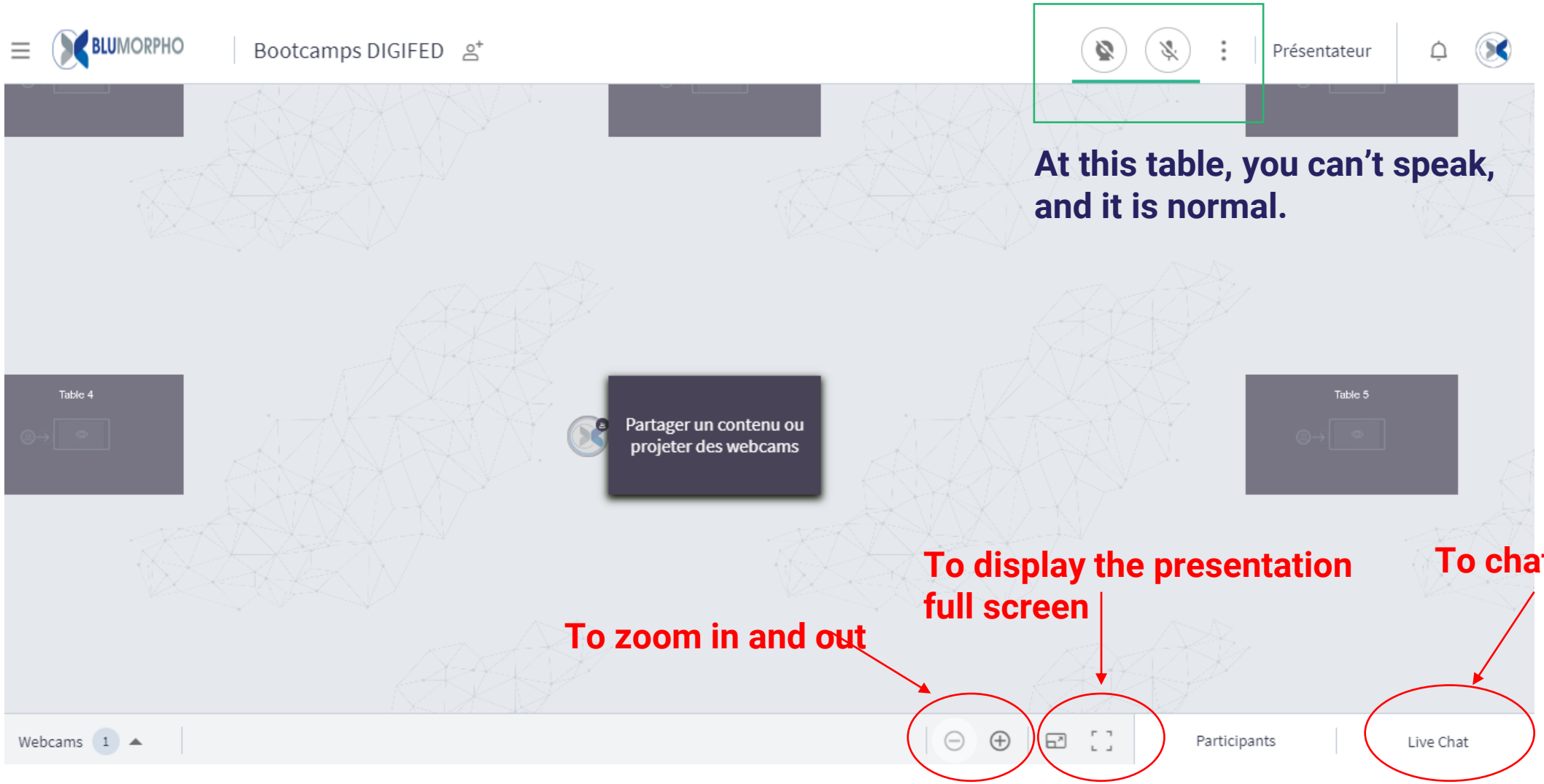
leti
ceatech

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 display the presentation full screen
To chat with us
To zoom in and out
Webcams 1
Participants
Live Chat

Agenda

- **Introduction, objectives and agenda** (5 minutes)
- **Cybersecurity technologies proposedby DigiFed partners**
  - CEA-LETI
  - Ikerlan
- **Open floor discussion between participants and DigiFed experts**
  - **Q&A** (55 minutes)

CEA LETI

Romain Jayles

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

Development of a secure platform: internal objectives

3 main objectives:

- **Platform of development**: platform for the development of *embedded internal secure solutions*, for instance PQC (Post-Quantum Cryptography) algorithms, AI solutions
- **Platform of characterization**: platform to assess the security of CTOS (Convergent Technologies Operating System) hardware and software components, for instance test suite for secure elements
- **Platform for tools development**: platform to develop and deploy tools support to security assessments, for instance fuzzing tools

➡ **Identification of a common infrastructure base of Digifed program**

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

Secure infrastructure current status

- **Software developments**
  - Developments on 2 boards STM32MP1 DK2 and EV1
  - Linux with TF-A, OPTEE-OS and u-boot. TPM supported in all software bricks
  - 3 types of TPM support available:
    - Linux mainline
    - Linux support + TPM accessible from TZ
    - TPM only available in TZ
  - TPM based secure boot available (TF-A root of trust)
  - TPM measurements on going (starting from TF-A)
  - Blockchain use case in TZ with TPM
  - Characterisation tools, for fuzzing, crypto algorithms, including SC and FA

- **Hardware Developments**:
  - Hardware design of a board. Schematics ready, waiting for SOM samples for mechanical validations

Ikerlan

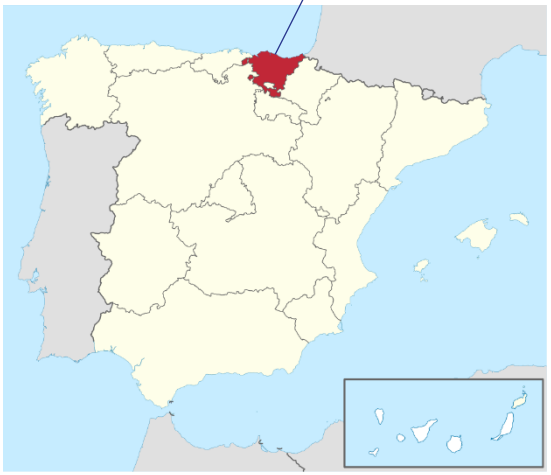
Patxi Galán

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

ikerlan in a Nutshell

Since 1974!

ikerlan



350 HIGH-SKILLED PROFESSIONALS > 150 ICT

45 PhDs

24.1 M€ TURNOVER

- 13 M€ > TECHNOLOGY TRANSFER PROJECTS
- 10 M€ > FUNDAMENTAL RESEARCH

2 M€ INVESTMENT IN WORLD-CLASS LABS

MONDRAGON HUMANITY AT WORK Finanzas Industria Distribución Conocimiento

BRTA BASQUE RESEARCH & TECHNOLOGY ALLIANCE

ikerlan Work areas

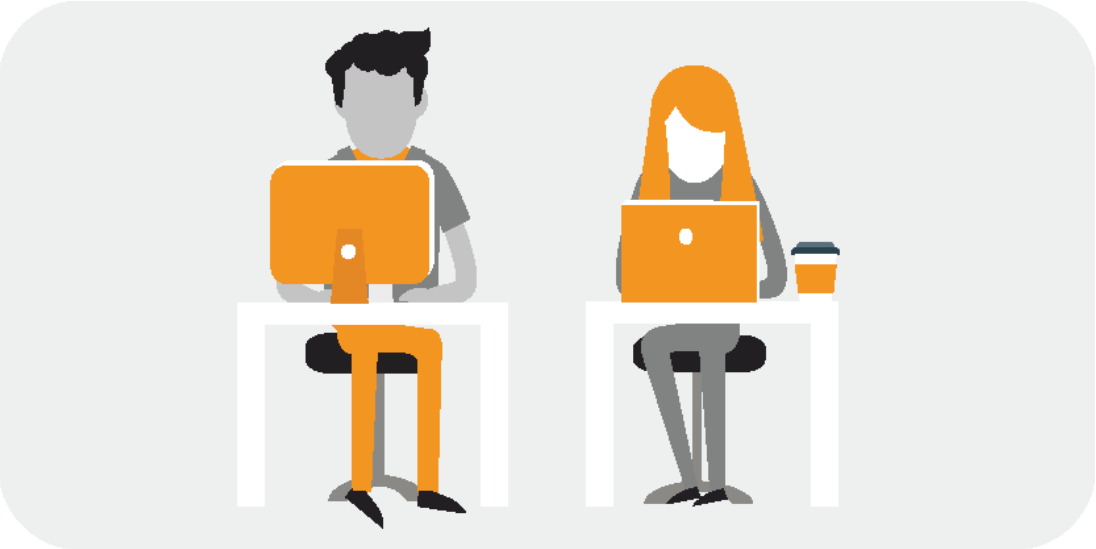
- Information and Communication Technologies

  IoT & Digital Platforms
  Data Analytics & Artificial Intelligence

- Dependable Embedded Systems

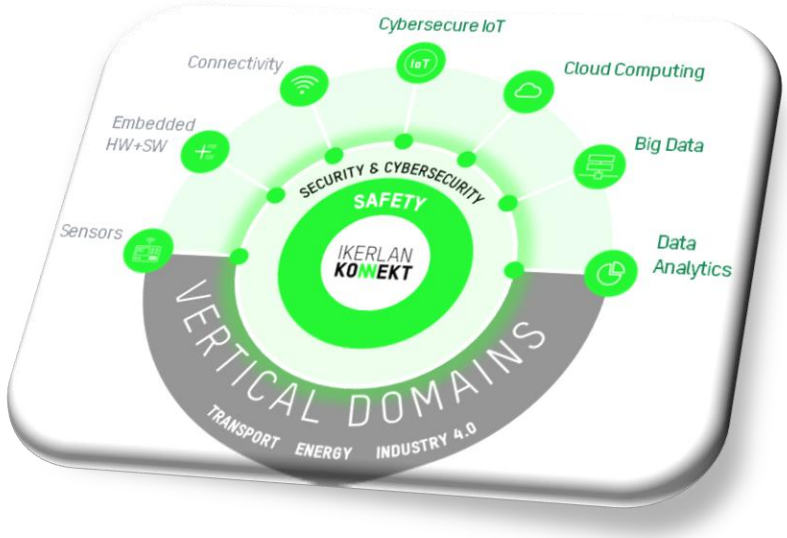
- HW and Communication Systems

- Industrial Cybersecurity



ikerlan Industrial Cybersecurity area

Integral Product

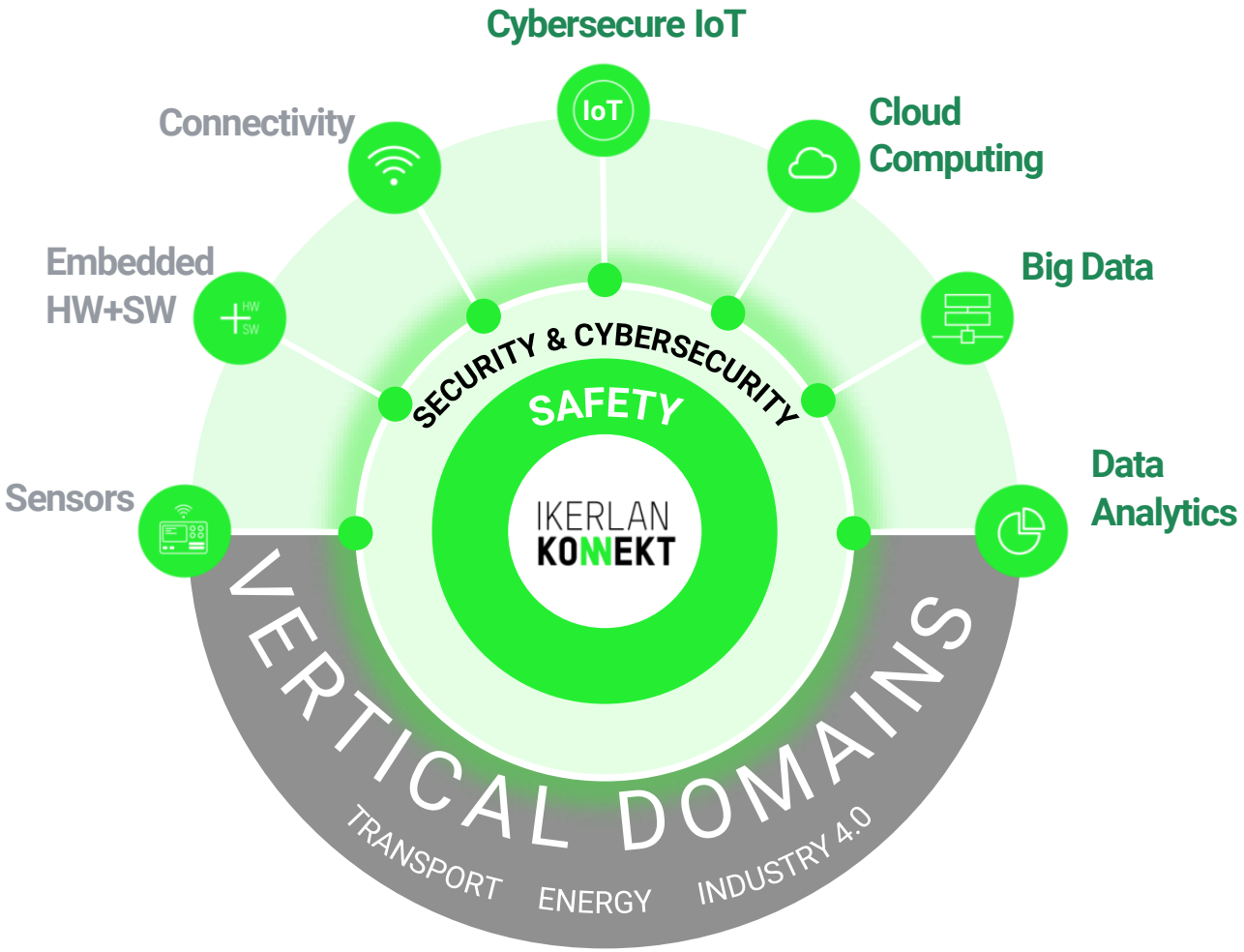


Research

Integral Product on Cybersecurity

Cybersecurity in Embedded Systems

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



Cybersecurity in Digital Platforms

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

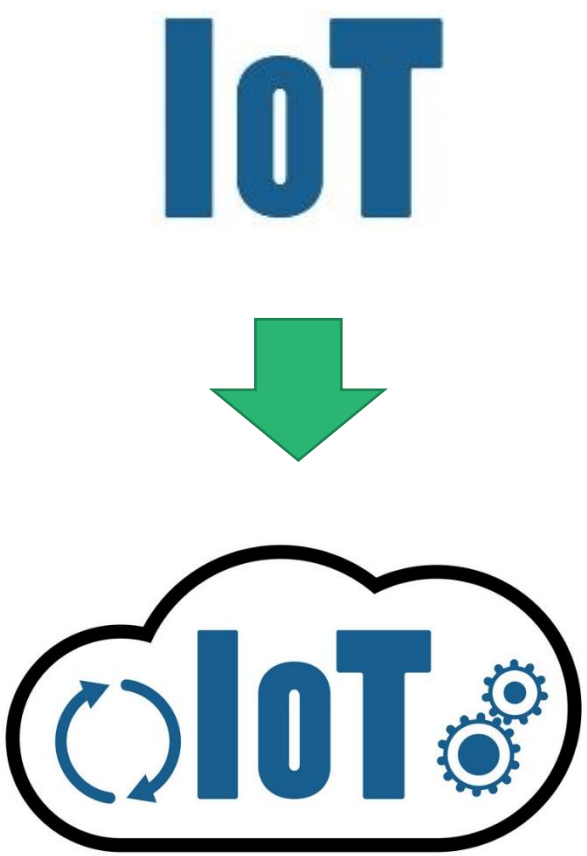
Research Topics

Cybersecure Industrial IoT

From embedded to the Internet

IoT → IoT

Cybersecure Industrial IoT

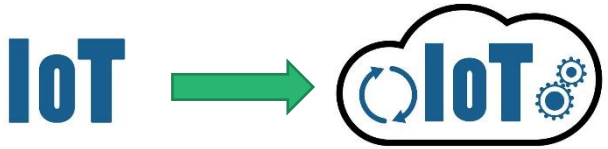


- ✓ Cybersecurity communication schemes for IoT environments.
  - ✓ KP-ABE and CP-ABE
  - ✓ Next-generation mobile networks such as 5G or LP-WAN
- ✓ Management of Public Key Infrastructures (PKI) for IoT environments.
- ✓ Threat monitoring.
- ✓ Attacks detection and mitigation.
- ✓ Security of industrial IoT devices.
  - ✓ SIEM technology
  - ✓ Applicability in ISOC and CSIRT
- ✓ Analysis for the integration of OT/IT protocols.
- ✓ Continuous methodologies on Cybersecurity in IoT Devices for:
  - ✓ Design
  - ✓ Implementation
  - ✓ Verification
  - ✓ Validation
- ✓ Development of IEC-62443 (layer3: systems) based systems.

Research Topics

Cybersecure Industrial IoT

From embedded to the Internet



Cybersecure platforms

The Internet platform (apps to server)

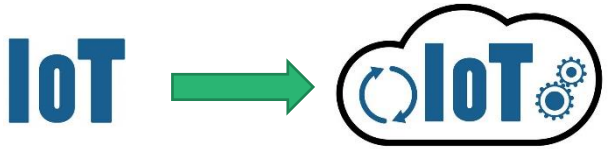
Cybersecure platforms

- ✓ Continuous monitoring of cloud infrastructures.
  - ✓ SIEM technology
  - ✓ Applicability in ISOC and CSIRT
- ✓ Mechanisms for threat detection and response in Web HMIs.
- ✓ Secure coding guidelines for cloud platforms.
- ✓ Advanced securisation of Web HMI to manage identifications and access.
- ✓ Back-end infrastructure-oriented cybersecurity.
- ✓ Continuous methodologies on Cybersecurity in Cloud Infrastructures for:
  - ✓ Design
  - ✓ Implementation
  - ✓ Verification
  - ✓ Validation

Research Topics

Cybersecure Industrial IoT

From embedded to the Internet

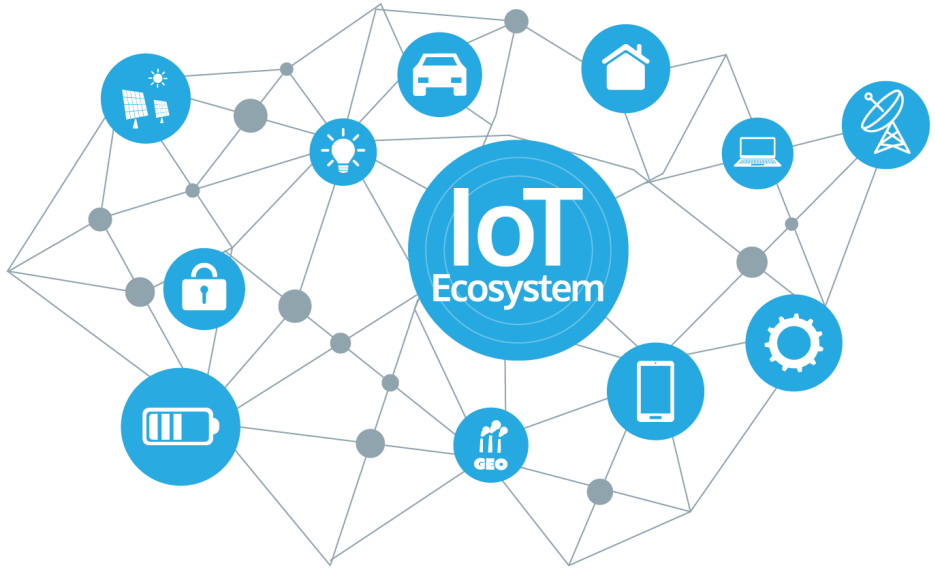


Cybersecure platforms

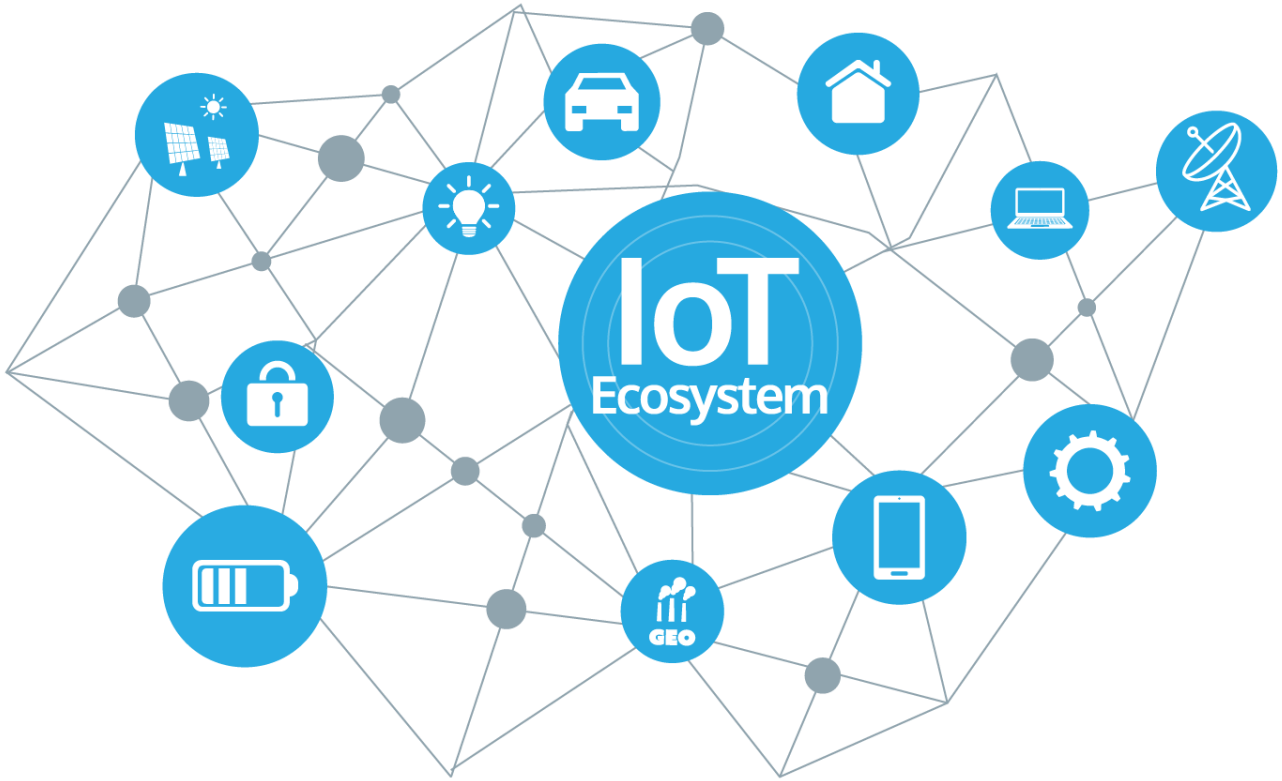
The Internet platform (apps to server)

Trust Technologies

Broader scope



Trust Technologies



- ✓ Blockchain technology
  - ✓ Research oriented to performance, architectures, security and regulation.
  - ✓ Develop demonstrators:
    - ✓ Industry 4.0
    - ✓ Energy
    - ✓ Smart Grid
    - ✓ Etc.
- ✓ Secure payment technologies.
- ✓ Remote authentication technologies.
- ✓ Trustworthy technologies for industrial environments.

Thanks!

Patxi Galán
pgalan@ikerlan.es

ikerlan