

# Requirements for Testing and Validating the Industrial Internet of Things

---

RUI PINTO

VVIoT

Västerås – Sweden

09 April 2018

Cofinanciado por:



UNIÃO EUROPEIA  
Fundo Europeu  
de Desenvolvimento Regional

**SYSTEC**  
RESEARCH CENTER  
FOR SYSTEMS & TECHNOLOGIES



Universidade do Porto  
**FEUP** Faculdade de  
Engenharia

# Outline

- Advance Manufacturing Systems
- Industrial Internet of Things
  - Five Layer IoT Architecture
  - Cyber-Physical Systems
- CPPS Validation
  - Requirements
  - Testing
  - Challenges
- Use Case Scenario
- Conclusion & Future Work

Cofinanciado por:



# Industry 4.0


---

ADVANCE MANUFACTURING SYSTEMS

Cofinanciado por:



# Industry 4.0

**1.0** | 1784 | based on mechanical production equipment driven by water and steam power 

**2.0** | 1870 | based on mass production enabled by the division of labor and the use of electrical energy 

**3.0** | 1969 | based on the use of electronics and IT to further automate production 

**4.0** | tomorrow | based on the use of cyber-physical systems 

## Technology:

- ▶ Digital networking production facilities
- ▶ Fast pace of technological change and innovative technologies

## Customers:

- ▶ Customised solutions
- ▶ Wide diversity of customers and markets
- ▶ New services

## People:

- ▶ Demographic development
- ▶ Training and qualifications
- ▶ Interaction between human beings and technology

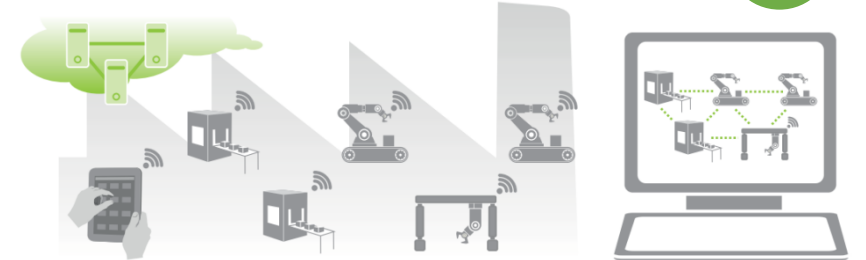
Cofinanciado por:

# Advanced Manufacturing Systems

## Digitisation and networking

- ▶ Vertical integration of hierarchical subsystems leads to smarter factories
- ▶ Supports horizontal integration through value networks
- ▶ End-to-end digital integration of engineering.
- ▶ Based on this global collaboration network, the consumers, design activities, manufacturing, and logistics can interact above the cloud

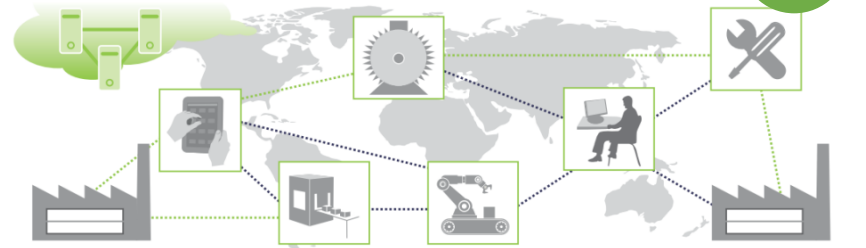
### Vertical integration (In a factory)



Quelle: Siemens 2012

Reconfiguration • Lot Sizes • Apps • Constant

### Horizontal integration



Quelle: Siemens 2012

Value chain • Life cycle costs • Customized products

Cofinanciado por:

# Advanced Manufacturing Systems

**Virtual emulation:**  
this will enable automatic  
start-up and reconfiguration.

**Plug and produce components:**  
facilitate the exchange of defective  
production units and the reuse of  
individual units for new products.

“I am finished.”

**Condition Monitoring:**  
the filter reports a  
contamination level of 95%.

“I continue on to station 2.”

Cofinanciado por:

# IIoT

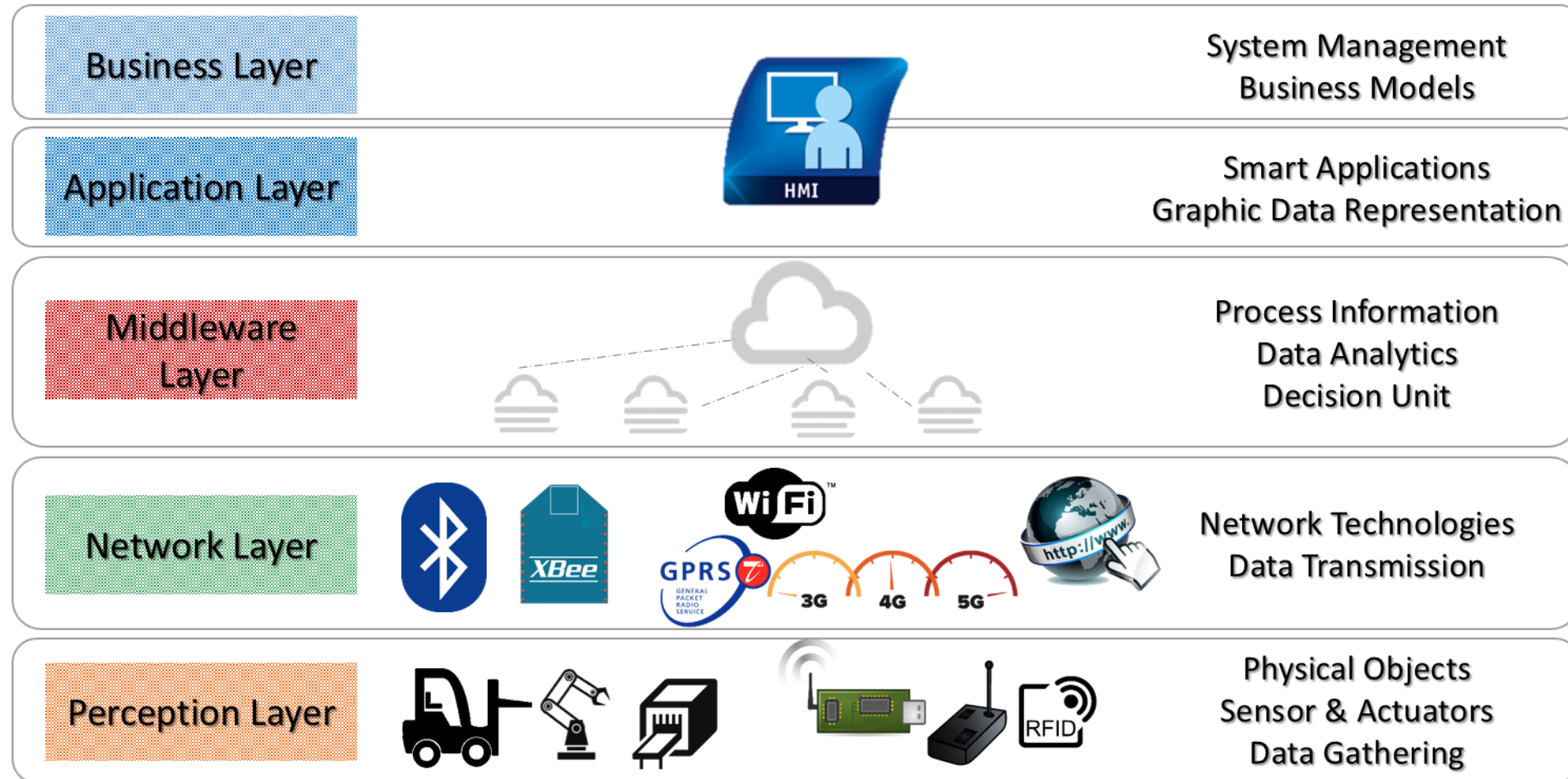
---

## CYBER-PHYSICAL PRODUCTION SYSTEMS

Cofinanciado por:



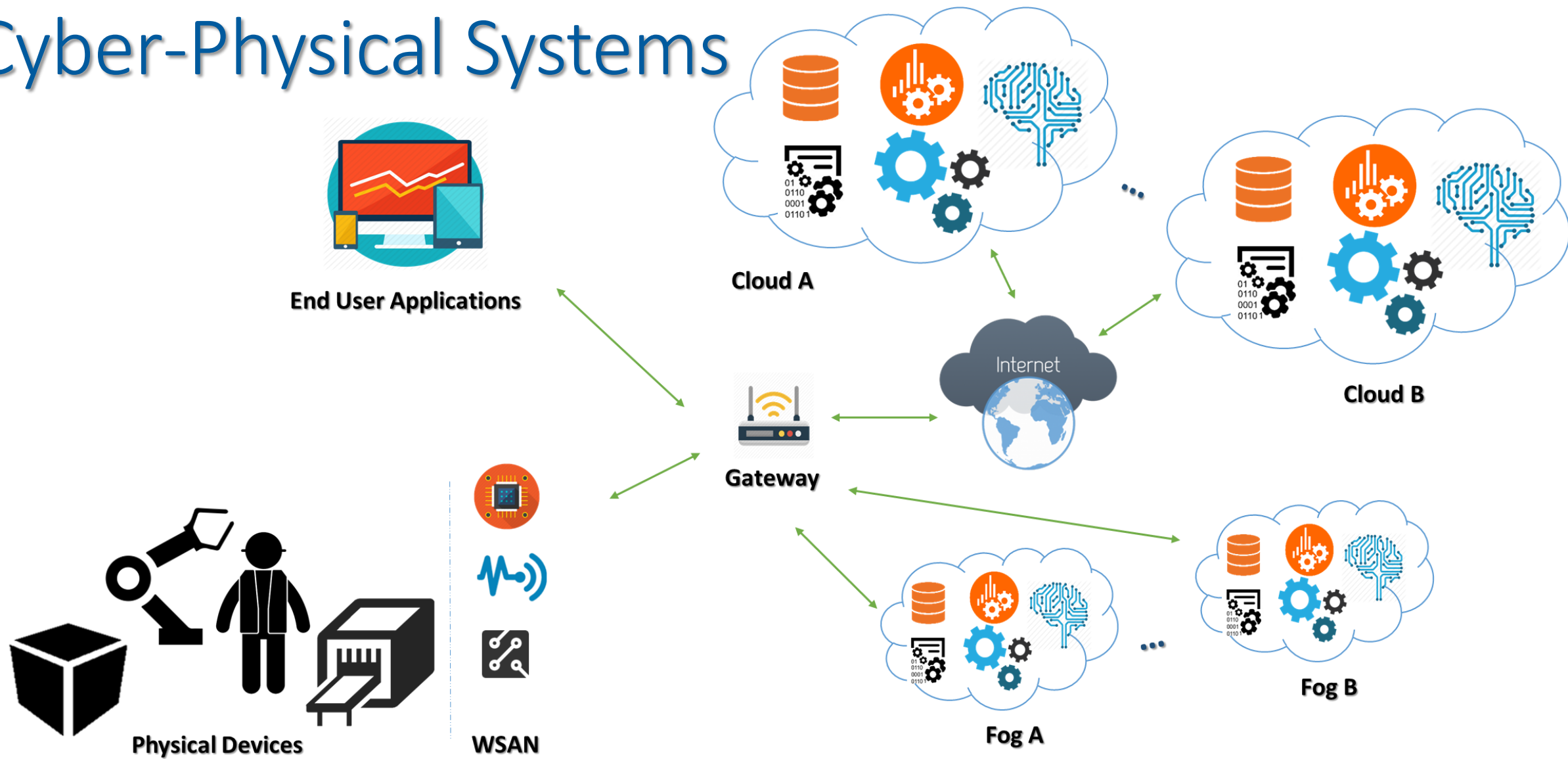
# Five Layer IoT Architecture



Cofinanciado por:



# Cyber-Physical Systems



Cofinanciado por:

# CPPS Validation

---

## REQUIREMENTS FOR CPPS TESTING

Cofinanciado por:



UNIÃO EUROPEIA  
Fundo Europeu  
de Desenvolvimento Regional

**SYSTEC**  
RESEARCH CENTER  
FOR SYSTEMS & TECHNOLOGIES



Universidade do Porto  
**FEUP** Faculdade de  
Engenharia

# CPPS Testing Requirements

Scalability

Reliability

Security &  
Privacy

Timing &  
Determinism

Safety

Recovery

Interoperability

Reconfigurability

Cofinanciado por:

# 1. Scalability

- a) Increase number of network nodes, *i.e.*, number of physical devices to monitor.
  - b) Increase available data, *i.e.*, increase loads of traffic volume, by adding more sensors.
  - c) Increase Cloud data services availability, such as storage, data analytics, user interface, etc.
- i. Associated latency.
  - ii. Cost of acquiring devices and upgrading more resources.
  - iii. Constrained data processing methods.

Cofinanciado por:

# 2. Reliability

- a) Long term execution of the CPS.
- b) Anomaly injection to generate failures in the physical equipment, network infrastructure or Cloud platform.
- c) Submit CPS components to extreme environment conditions, such as temperature, humidity, air quality, etc.
- d) Overall counting of received/sent packages that are transferred using the network infrastructure.
  - i. Relationship between anomaly and corresponding generated failures.
  - ii. Difficulty to implement code verification methods in such complex systems, in order to identify faults, anomalies or software bugs.

Cofinanciado por:

# 3. Security & Privacy

- a) Cyber attack injection, which will affect the integrity of the information and devices.
- b) Stealing sensitive data.
- c) Security resources, such as anti-virus, firewalls and cryptographic systems, are up and running.
  - i. Unavailability to inject zero-day attacks, since it is impossible to simulate unknown attacks.
  - ii. Simulate the behaviour of known attacks, such as physical attacks, DoS, Sibling attacks, malware, etc.
  - iii. Lack of expertise in cyber security methods, specially the group of methods that are suited to be used in CPS.

Cofinanciado por:

# 4. Timing & Determinism

- a) Guarantee cycle time of industrial process, *i.e.*, guarantee that the implementation of CPS doesn't jeopardize product quality and process parameters.
- b) Test equipment process with varying parameters, in order to identify product quality degradation.
  - i. Identify which CPS component introduces delay to the industrial process.
  - ii. Evaluate environmental impact over the process, *i.e.*, understand if delay is caused by external uncontrollable factors or by the CPS itself.

Cofinanciado por:

# 5. Safety

- a) Simulation of safety process parameters, both in controlled and relevant environment.
- b) Counting number of physical accidents in the shop-floor, *i.e.*, events that caused harm to human operators.
  - i. Knowing the accident's cause, *i.e.*, identifying if it was caused by human or machine error.
  - ii. Reliable safety process parameters simulation while in simulated and controlled environment.
  - iii. Availability of relevant environment to test, *i.e.*, shop-floor cell for introducing failures and accidents.

Cofinanciado por:



# 6. Recovery

- a) Evaluate continuous operation of the system when some of its parts are shut-down, *i.e.*, system compensate functionalities of compromised components.
- b) Maintain previous state after rebooting, both individual node or global system.
- c) Analyse time of reboot.
  - i. Identify the damage level that prevents system's recovery and partial operation.
  - ii. Identify what is the previous state of the system.
  - iii. Identify the acceptable time of rebooting.

Cofinanciado por:

# 7. Interoperability

- a) Send messages with non matching semantics or undefined ontology between different nodes or modules in the same node.
- b) Integration with 3rd party platforms (legacy entities).
  - i. Communication API with legacy entities does not exist.
  - ii. Non compatibility between existing APIs or when communication protocols are not the same.

Cofinanciado por:



UNIÃO EUROPEIA  
Fundo Europeu  
de Desenvolvimento Regional



Universidade do Porto  
**FEUP** Faculdade de  
Engenharia

# 8. Reconfigurability

- a) Analyse time of reconfiguration, *i.e.*, duration of altering the network topology.
  - b) Verify system reconfiguration when changing communication routing between nodes.
  - c) Verify system reconfiguration when a node is added.
- i. Verify success reconfiguration in complex system.
  - ii. Identify acceptable time of reconfiguration.

Cofinanciado por:

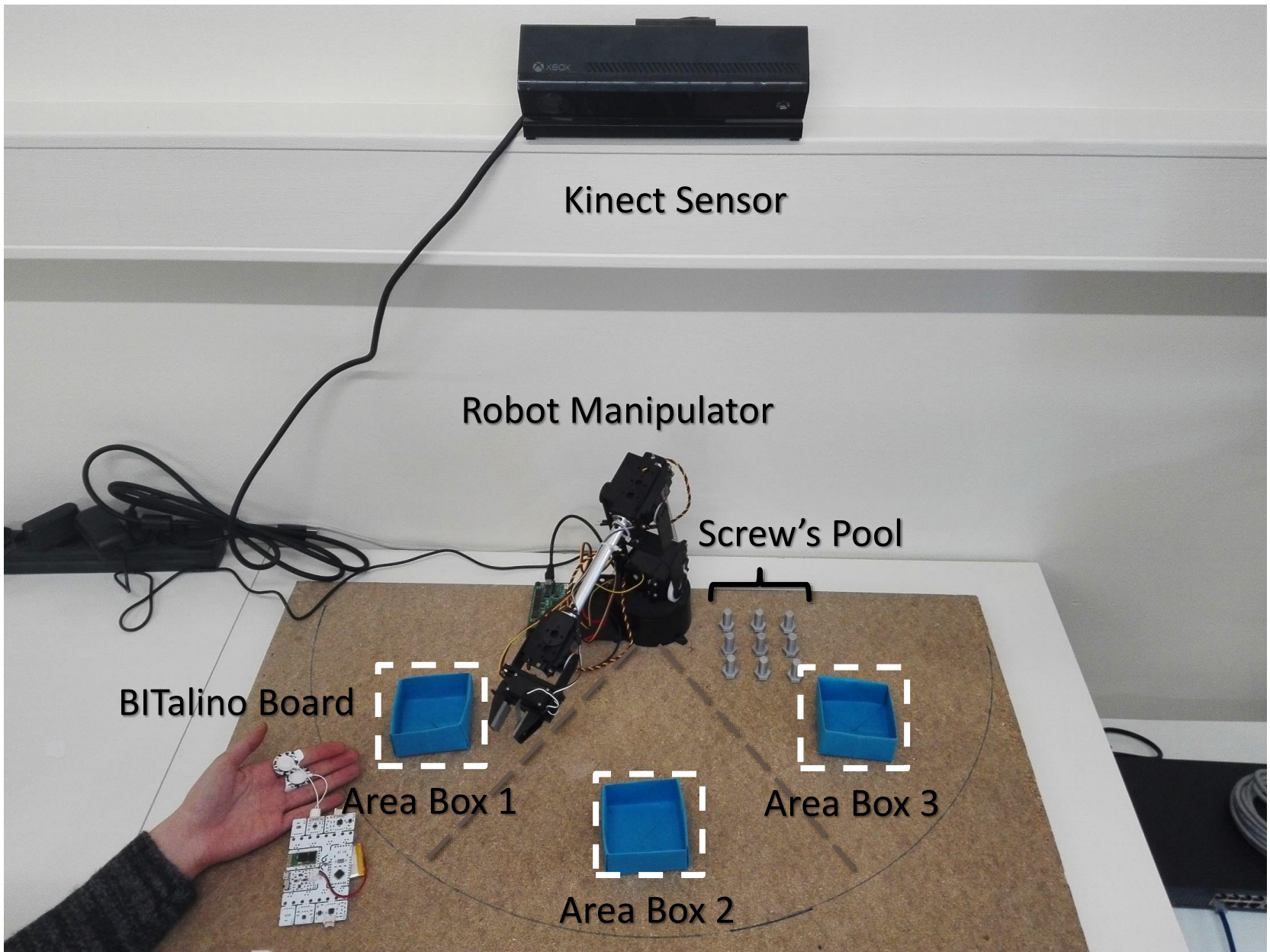
# Cobots

---

## USE CASE SCENARIO

Cofinanciado por:





Kinect Sensor

Robot Manipulator

Screw's Pool

BITalino Board

Area Box 1

Area Box 2

Area Box 3

Cofinanciado por:



# Testing Collaborative CPPS

## Scalability

- Add biometric sensors.
- Add new data analytic services.

## Reliability

- Hamper BITalino data (increase TEMP and HUM levels) & Kinect's performance (increase LUM levels).
- Introduce Random faults: unplug sensor power and send malformed messages.
- Count message drop in network

## Security & Privacy

- Break into network gateway firewall.
- Still biometric sensor data.
- Corrupt messages sent to robot.

## Timing & Determinism

- Command execution by robot is within acceptable time.
- Evaluate process performance with several stress/fatigue combinations.

## Safety

- Vary BITalino parameters for board overeating or battery explosion.
- Overflow the robot with actuation commands.

## Recovery

- Forcing reboot of sensors and Cloud.
- Evaluate if reboot is within acceptable time and previous state is maintained.

## Interoperability

- Validate success communication while integrating with legacy ERP.
- Send unexpected messages to Cloud or robot.

## Reconfigurability

- Change network topology, from star to peer-to-peer.
- Evaluate network self-organization when adding new sensors.

Cofinanciado por:

# Wrap-Up

---

CONCLUSION & FUTURE WORK

Cofinanciado por:



# Conclusions & Future Work

- i. Growing usage of IIoT platforms and CPPS demands requirement validation and testing.
  - ii. Trial and error techniques are the primary debugging methods by CPS developers.
  - iii. Simulators often fail to represent correctly process parameters.
  - iv. This work proposes 8 CPPS requirements, which are fundamental for the correct operation of the CPPS.
  - v. Most of the requirements involve end-to-end testing regarding the CPPS architecture.
- i. Implement a framework for automatic CPPS test.
  - ii. Implement and test the collaborative CPPS presented in a industrial relevant scenario.

Cofinanciado por:





# Thanks!

## Any questions?

You can find me at:  
[rpinto@fe.up.pt](mailto:rpinto@fe.up.pt)



Cofinanciado por: