

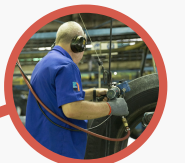
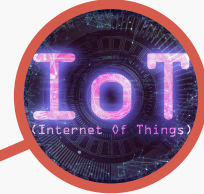


This project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 833828.

# C4IIoT

## CYBER SECURITY 4.0

Protecting the Industrial  
Internet of Things



## The Team

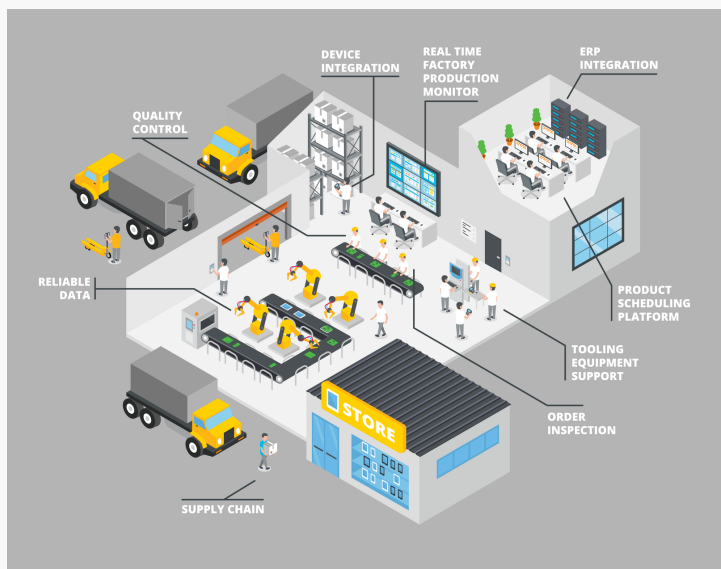


## Objectives

- Develop, validate, demonstrate, & support a holistic and disruptive and end-to-end Cybersecurity 4.0 framework for prevention & protection against Industrial IIoT cyber-attacks
- Explore C4IIoT framework in the automotive Industry and validate its potential in rea-world settings
- Offer real-time malicious and anomalous behaviour anticipation, detection, tracking, mitigation and end-user informing, within evolving IIoT applications and processes
- Consolidate international and European links, collaborate with standardizations bodies and ensure transferability of project's results.
- Boost the effectiveness of the European Security Union against cyber-attacks in IIoT infrastructures, by offering almost ready to market solutions (TRL 6).

## Overview

C4IIoT is a novel and unified cybersecurity 4.0 framework that implements an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IIoT systems.



# Use Case #1

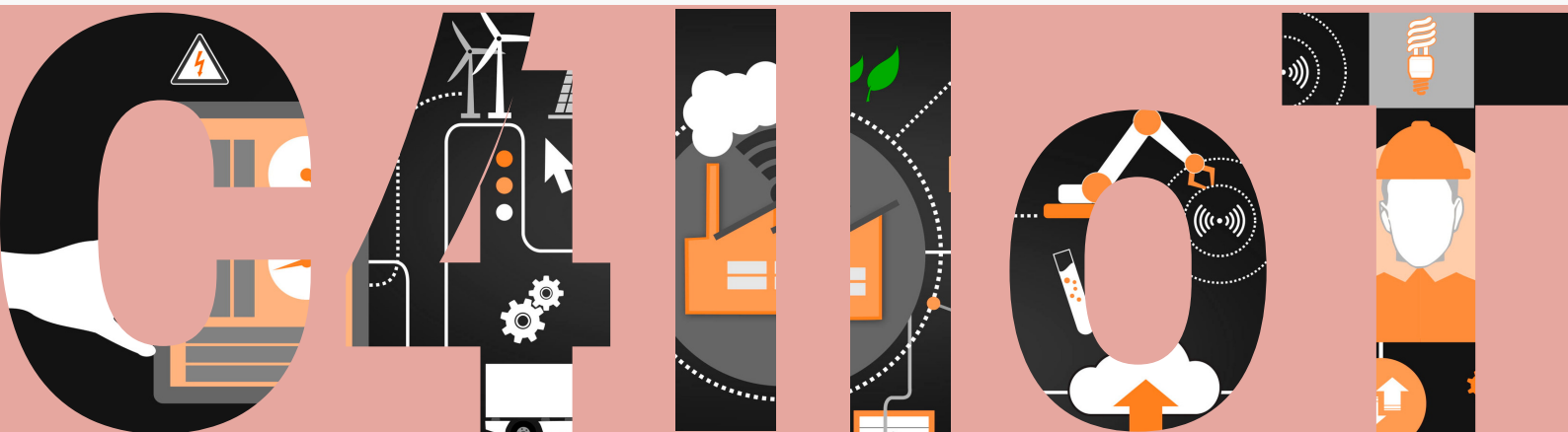
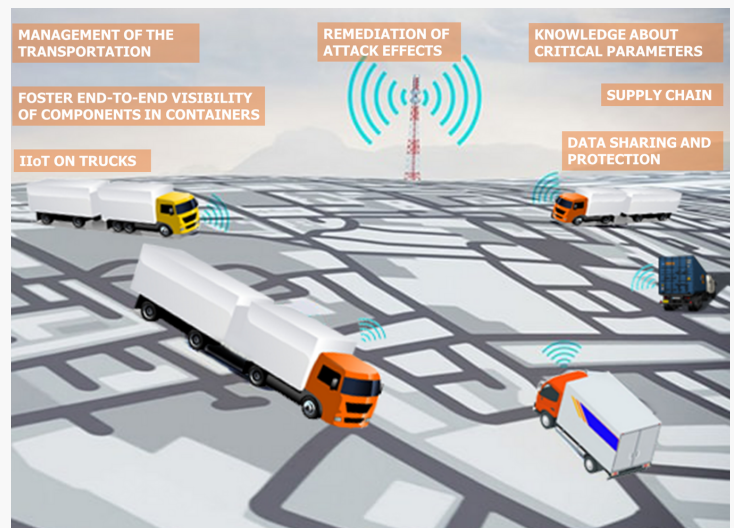
## Enabling security of IIoT in a Smart Factory

- identify cyber threats in a smart factory system from the Internet/cloud;
- protect all relevant IT/OT systems from cyber-attacks;
- improve incident response and disaster recovery in all systems;
- assess the cost of cybersecurity solutions

# Use Case #2

## Enabling security of IIoT in Inbound Logistics

Inbound Logistics deal with the complex problem of managing different parts from many origins points to manufacturing plants. IIoT are key to enable the optimisation of the logistics along the supply chain to maintain low stocks, to reduce working capital and warehousing costs and to avoid stock-outs that could cause a production stop in the plant. As the devices mainly operate outside the plant, their capacity to be resilient to threats such as intrusion, data modification and device control is the key for the rollout



Connect  
With C4IIoT



[www.c4iiot.eu](http://www.c4iiot.eu)



@c4iiot



@c4iiot



@c4iiot.eu

### Project Info

Project Coordinator: FORTH  
Project Start Date: June 2019  
Project Duration: 36 Months  
No of Participating Organizations: 14  
No of Countries: 8

