Secure Collaborative Intelligent Industrial Assets

- SeCoIIA aims at securing the digital transition of the manufacturing industry towards more connected, collaborative, flexible and automated production techniques.
- Enhanced process monitoring, optimisation and control is achieved by intelligent use of digital twin technology, Industrial IoT, Cloud Manufacturing (CMfg), collaborative robotics and Industrial AI.

‘Enhancing security and safety for collaborative manufacturing’

Challenges

- The transition from hierarchised supply chains to collaborative networks of smart factories opens an attack surface so far never reached.
- Enhanced collaboration on manufacturing activities may not safely apply without collaborative security monitoring and incident response.
- The increased reliance on machine-learning-based decision making sets a technical challenge in terms of security assurance and a legal challenge in terms of accountability and law enforcement.

Application sectors

With 4 large strategic industry players, 4 highly innovative SMEs and 4 highly recognised research centres, SeCoIIA consortium is best suited to achieve enhanced competitiveness and resilience for European manufacturing industry.

12 partners from the following countries:
5 Objectives

1. Secure the adoption of smart collaborative manufacturing techniques by European Transport Systems Manufacturing Industries
2. Identify and prevent threats to collaborative manufacturing environments, build, sustain and exchange smart OT security knowledge and know-how
3. Create trust across smart manufacturing value chain, secure access to dynamic collaborative Cloud Manufacturing (CMfg) services
4. Detect and react in collaboration, improve OT intrusion detection accuracy, reduce decision time and response cost, improve coordination of safety and security teams
5. Empower and responsibilise key actors of the manufacturing value chain, secure machine decision making, adapt regulatory framework and enforce the law

16 Key capabilities

The key capabilities enable to enforce the security of production systems on:

- **Organisation to Organisation**
  - Collaborative industrial CyberRange
  - Secure collaborative Mfg backbone
  - Collaborative SOC for distributed OT
  - Accountability framework for collab. Mfg

- **Human to Human**
  - Community-based industrial CyberRange
  - Fine-grained access control & encryption
  - Cognitive & emotional behavior analytics
  - Privacy-preserving cloud manf. techniques

- **Machine to Human**
  - Cyber-physical security training platform
  - Smart combined asset & user authentication
  - Safe and securere collaborative robotics
  - Collaborative OT security forensics

- **Machine to Machine**
  - Cyber-physical security testing platform
  - IIOT authentication & encryption
  - Detection over encrypted ICS traffic
  - Adversarial/ robust Al techniques

**HORIZON 2020**: ec.europa.eu/programmes/horizon2020
**SECOIIA**: http://secoiia.eu
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 871967

**AIRBUS**

FRANCE
Metapole 1, boulevard Jean Moulin
CS 40001 / 78996 Elancourt Cedex
France

GERMANY
Willy-Messerschmitt-Str. 1
82024 Taufkirchen
Germany

UNITED KINGDOM
Quadrant House / Celtic Springs
Coedkernew / South Wales
NP10 8FZ / United Kingdom

contact.cybersecurity@airbus.com
www.airbus-cyber-security.com

This document is not contractual. Subject to change without notice. © 2021 Airbus CyberSecurity. AIRBUS, its logo and the product names are registered trademarks. All rights reserved.