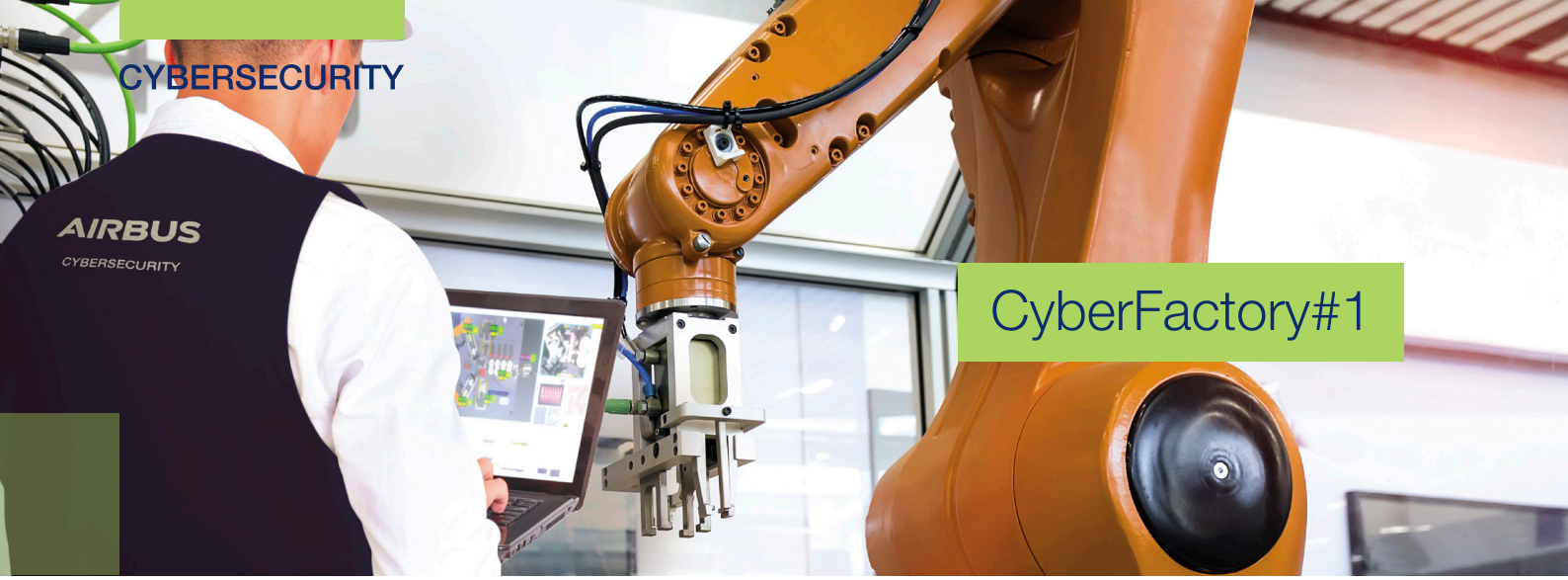
CYBERSECURITY



CyberFactory#1

Cyber security for Industry 4.0 and the Factory of the Future

The introduction of digital and autonomous technologies to industrial manufacturing is set to bring enormous benefits for the Factory of the Future (FoF). Yet at the same time, these new technologies and networks are at risk from increasingly sophisticated cyber-attacks. To address these threats, **we have created the international research project CyberFactory#1.**

The project, which is part of the ITEA cluster of the European EUREKA programme, brings together **28 industrial and research partners from seven different countries** – with the ultimate aim of enhancing the processes and the cyber-resilience of the Factory of the Future.

The CyberFactory Project

CyberFactory#1 (CF#1) aims to design, develop, integrate and demonstrate a set of key enabling capabilities to foster the optimisation and resilience of FoF. Through its pilot users, technology providers and research partners, CF#1 will thoroughly examine the technological, economic, human and societal factors associated with manufacturing technologies; evaluating their efficiency in daily use and their resilience in realistic cyber-attack scenarios.

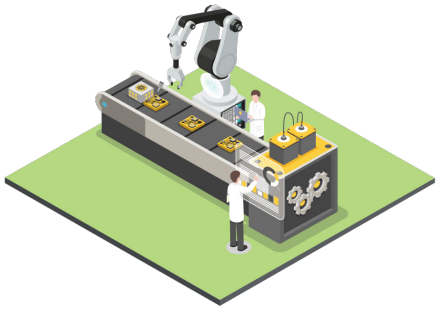
Specifically, CF#1 will assist the development of key capabilities in the following areas:

- **Factory system of systems modelling**
- **FoF optimisation**
- **FoF resilience**

Intelligent and secure factories

As factories adopt increasingly large networks of connected devices, the “Industrial Internet of Things” (IIoT) introduces a number of novel challenges concerning the efficiency, security and safety of industrial organisations.

The goal of **CyberFactory#1** is to provide a **forum for the dissemination of innovative research** in which academics, technology providers and industrial practitioners discuss the opportunities of Industry 4.0, in addition to the threats that it is set to face.



Factory of the Future Modelling:

- Cyber-physical modelling and “digital twins”
- Eco-system modelling, supporting real-time management decision-making
- Human-behaviour modelling
- Factory SoS modelling

Factory of the Future Optimisation:

- Real time sensing, tracking and supervision of tools, materials and individuals in the supply chain
- Data-lake exploitation
- Optimisation of human / machine collaboration

Factory of the Future Resilience:

- Authorisation, authentication and continuous trust level management
- Resilient AI and adversarial machine learning
- Human / machine watch and behavior-based anomaly detection
- Autonomous resilience and automated incident response capabilities

AIRBUS

Our Goals

We are already supporting in **the definition of use-cases and misuse-cases** based on risk assessments. Use-cases range from remote production monitoring to supply chain optimisation or predictive maintenance, whereas misuse-cases range from accidental malware insertion to Advanced Persistent Threat (APT) or offensive AI.

The modelling and simulation of cyber-physical systems which will populate the FoF will come in the second stage of the programme. They will utilise architecture validation, data generation, equipment testing and user training to support the adoption of smart secure manufacturing technologies.

In a third step, we will focus on capabilities that enhance the resilience and security of the FoF, particularly through resilient AI development (CAP52), human/machine behaviour monitoring (CAP53) and autonomous cyber-resilience mechanisms (CAP54).

These developments will finally be integrated and tested in pilot factories with application sectors ranging from aerospace to robotics or electronics. **A total of 8 Pilot factories will be involved** in the demonstration of project results with the deployment of modular system demonstrators integrating developments of the whole consortium.

Ultimately, this will help **identify not just security risks, but also risks targeting the safety of FoF**, enabling CyberSecurity#1 to focus on enabling solutions that address both safety and security.

FoF Characteristics

As a multifunctional production system, the FoF should be able to **deal efficiently with short production cycles, constantly changing production contents and strong customisation.** It should also be able to respond flexibly and adequately to deviations and disturbances.

The FoF is by nature flexible - and system associations are constantly adapting to changed boundary conditions and goals. This means that deviations from normal or desired behavior and hazards are much more difficult to detect than in traditional manufacturing systems.

In the FoF, people and machines work in close collaboration. To benefit from the augmentation of human and artificial intelligence, the cooperation of people with robots and other automats without explicit spatial separation must be enabled.

In the FoF, very large amounts of data are collected cumulatively. **The challenge is to analyse this huge amount of data in real time**, in order to recognise patterns and make decisions based on data output.

The FoF will use **AI methods** for monitoring and anomaly detection, decision support or automated control, self-optimisation and autonomic resilience.

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

ITEA 3

info@itea3.org
https://itea3.org/

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