# ITEA Press release

CyberFactory#1 fosters the optimisation and resilience of the Factory of the Future

*15 September, Helsinki – To enable the Factory of the Future, optimisation must be reconciled with security. The growing integration of Information Technology (IT) into Operational Technology (OT) exposes manufacturing systems to a growing number and diversity of threats. The ITEA project CyberFactory#1 has designed, developed, integrated and demonstrated a set of key enabling capabilities to foster the optimisation and resilience of the Factory of the Future (FoF).* *For these achievements, the CyberFactory#1 consortium was awarded the ITEA Award of Excellence 2022 for Business Impact!*

The CyberFactory#1 project, led by Airbus Protect in France, consisted of 28 partners from Canada, Finland, France, Germany, Portugal, Spain and Turkey. The project addressed the needs of pilot factories across the aerospace, transportation, machine fabrication, textile and consumer electronics industries in a total of 10 use-cases. Depending on the use-case, different aspects of FoF were developed and tested, such as collaborative robotics, process optimisation, real-time quality control, distributed manufacturing and predictive maintenance. The project also proposed preventive and reactive capabilities to address cyber and physical threats and safety concerns for FoF.

Applicable from rivet shaving to cheese manufacturing

The key capabilities were demonstrated in real and hybrid environments, reflecting the variety of possible new factory types like hyper-automated plants, distributed shopfloors or learning factories.

For example, an industrial IoT system has been deployed in Airbus factories in Tablada, San Pablo Sur, and Cadiz in Spain to support the remote monitoring and optimisation of rivet shaving, forming and curing and the visual inspection of critical aeronautical parts. Digital twins of the monitored industrial assets have been modelled to support a large set of penetration tests and security trainings. A Security Operation Centre dedicated to Operational Technology has been assigned, which supports attack detection and real-time response based on advanced machine learning techniques. This system has been adopted as a standard and will be replicated for implementation in more than 20 factories within the Airbus group.

Another use-case was led by the Finnish partner High Metal and covered an integrated platform-based concept for cheese manufacturing. One scenario dealt with a potential attacker who could get access to the configuration of the platform and could modify the cheese-making process. A resulting change in the quality of the cheese might only be detected much later in the process and could lead to significant losses for the producer, if not consumer health issues. The partners involved in this use-case were able to demonstrate that a strong authentication and network behaviour monitoring system could prevent the attacker from gaining access to the platform.

€150 M additional revenues and 450 extra jobs by 2025  
Acceptance and adoption by industrial users are boosted by the human-centricity and high-grade security which this project’s results offer. The business impacts represent three fast-growing markets: the digital twin market, the Industry 4.0 market, and the IIoT security market. The partners intend to generate around €150 M additional revenues and 450 extra jobs by 2025.

CyberFactory#1, a project born within Industry 4.0, has been recognised as a pioneer of Industry 5.0 for its contributions to a more sustainable, human-centric and resilient industry.

*“Cyberfactory#1 was an excellent project as it created a solid foundation for cybersecurity and cyber-resilience capabilities in the context of the Factory of the Future and Industry 4.0. The approach taken for the development of cyber-resilience capabilities goes beyond risk management and tactical technical solutions, requiring a holistic view of systems and processes to prepare for the reality of cyber-incidents. These were conducted in e.g. the Bittium case by modelling digital twins and performing true simulation and testing with hundreds of test scenarios with available cyber-frameworks in excellent collaboration with Airbus Cybersecurity FR. The outcome was that the cybersecure architecture for the use-case could be practically taken into use and can be adopted in alternative use-cases the future.”*

* Jari Partanen, Head of Quality, Environment and Technology Management at Bittium

This project has received funding from:

Logo

Description automatically generatedText, timeline

Description automatically generated with medium confidence*Text

Description automatically generated*

Logo, company name

Description automatically generatedLogo

Description automatically generatedA picture containing logo

Description automatically generatedIcon

Description automatically generated with low confidence

## *Note for editors, not for publication*

## For interview requests, questions and additional information about CyberFactory#1 and ITEA, please contact:

CyberFactory#1 Contact person ITEA Contact person  
Adrien Bécue Linda van den Borne-Toupet   
[adrien.becue@airbus.com](mailto:adrien.becue@airbus.com) [linda.van.den.borne@itea4.org](mailto:linda.van.den.borne@itea4.org)

#### CyberFactory#1 project partners and websites <https://itea4.org/project/cyberfactory-1.html>

<https://www.cyberfactory-1.org/home/>

#### About ITEA

ITEA is the Eureka Cluster on software innovation, enabling a large international community to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. <https://itea4.org>