Project Results

CyberFactory#1

Addressing opportunities and threats for the Factory of the Future

The ITEA project CyberFactory#1 has combined simulation, optimisation and resilience enhancements to secure the manufacturing transition to Industry 4.0 with a System of Systems (SoS) approach. This will enable the Factory of the Future (FoF), a permanently connected production unit involving disruptive technologies like digital twins, edge computing and collaborative robotics.

Project origins

Cyber-risks for the FoF include malware, data leakage or confiscation, adversarial machine learning or rogue devices. These attacks can disrupt industrial processes and damage products, reducing competitiveness or even threatening safety. As product and asset connectivity increase, optimisation must be reconciled with cybersecurity and addressed from an early design stage throughout the production lifecycle.

Addressing ten use-cases in transportation, automotive, electronics and machine manufacturing, CyberFactory#1 has created tools and methodologies to ensure that factories can safely adopt Industrial Internet of Things (IIoT), advanced AI analytics and collaborative robotics. The work has been structured in three layers: (1) modelling and simulation, (2) production optimisation, and (3) resilience enhancement. The modelling and simulation layer provides digital twins of the FoF, enabling testing-based design and validation of the other layers. The optimisation layer provides shop floor connectivity and AI-based process control for improved productivity. The resilience layer ensures protection, detection and response regarding advanced cyber and physical threats to the FoF. These interlinked tools can help companies take a step beyond Industry 4.0.

Technology applied

CyberFactory#1's technology is a synthesis of 12 enabling capabilities for the FoF, which are divided not only across the three layers but also across four dimensions. The technical dimension focuses on cyber-physical systems (CPS) in general, dealing with architecture, crypto, data collection and analysis using CPS modelling and digital twins, real-time sensing and tracking, and human-machine access and trust management. The economic dimension utilises factory ecosystem modelling, manufacturing data lake exploitation and adversarial/robust learning to deal with multiple interacting factories, protecting transactions between actors in the supply chain. As safety in human-machine collaboration is central to the FoF, the human dimension uses human behaviour modelling, human-machine optimisation and human-machine behaviour monitoring to promote more human-centric manufacturing. Finally, the societal dimension aggregates the prior aspects into factory SoS modelling, distributed manufacturing and cyber-resilience mechanisms, scaling them up to the full production ecosystem.

^ CyberFactory#1: Securing Human-Robot collaboration in Factories of the Future

The project's use-case owners are predominantly factories, which have tested and demonstrated these technologies in a mix of real and simulated environments. In an Airbus factory in Spain, for example, the robotic system RoboShave has been demonstrated for automatic jo-bolt rivet shaving in aircraft rudders. The project has contributed to RoboShave's improvement through the elaboration of its digital twin, its connection to a secure IIoT platform and its protection against a large set of cyber-attacks. These developments will reduce lead time, production/maintenance costs, product defects and security risks. Much of CyberFactory's digital twin technology is based on an environment developed by Airbus (CyberRange), which simulates both manufacturing chain operations and communication processes to examine different attack scenarios.

Making the difference

Having worked on almost 200 KPIs across the use-cases, CyberFactory#1 partners are now pursuing exploitation individually and collaboratively. For factories, this generally consists of internal exploitation to reduce manufacturing costs, waste, efforts and lead time. RoboShave, for instance, has achieved 100% traceability of processes and products from the shop floor and 100% accuracy of (near) real-time information on dashboards, both of which started at zero. By automating machine and manufacturing execution system communication, it has also seen a 100% reduction in the time spent by human operators on manual machine data collection. In turn, this reduces human error while improving worker satisfaction by allowing them to focus on more stimulating tasks.

For security and technology vendors, exploitation is primarily focused on enriching their portfolios with new products and services. For example, Airbus in France is collaborating with Bittium in Finland to deploy CyberRange to simulate and monitor their distributed manufacturing environment. Airbus is also offering Security Operation Centre (SOC) services that monitor a factory's traffic, raise alarms and respond to anomalies. Across the project, commercialisation will target the digital twin, Industry 4.0 and IIoT security markets, with impressive results expected in each: by 2025, partners can expect revenues of EUR 8 million and 82 new jobs in the digital twin domain, EUR 28 million and 114 jobs in Industry 4.0 and EUR 114 million and 256 jobs in IIoT security. This total impact equals EUR 150 million and 452 jobs across the consortium.

Meanwhile, dissemination is ongoing and has so far seen eight journal publications, 37 conference appearances, one contribution to a book and 26 other types of dissemination achievement. For example, HTW Berlin has launched PhDs on topics like the formalisation of collaborative objectives in heterogeneous systems of systems and the safety and certifiability of safety-critical systems based on machine learning. Crucially, the project has been recognised as a pioneer of Industry 5.0, which goes beyond efficiency and productivity and reinforces industry's contribution to societal goals. With its focus on a sustainable, human-centric and resilient industry, CyberFactory#1 has paved the way to the next industrial revolution.

Major project outcomes

Dissemination

- 8 Journal Articles published, 37 Conference Papers, 28 Other Dissemination Achievements

Exploitation (so far)

- **20 new products:** OT CyberRange, OT Security Operation Center, IoT Fingerprint *(AIRBUS)*; Collaborative AGV Controller, AGV data analysis tool *(ASTI)*; Network Analyser, Correlation Engine *(ISEP)*; SQL Trigger Software, Windows Service Software, Predictive Maintenance Tool *(VESTEL)*; Wireless Intrusion Detection System *(GOHM)*; AGV Fleet Optimisation Algorithm *(OFFIS)*; Smart UX Interface, Intelligent Role Management System, Virtual Assistant Agent, Production Scheduling Optimisation *(SISTRADE)*; Geofencing Software, Authorisation Server, Network Analyser, Anomaly Detector *(S21SEC)*
- **6 new services:** Collaborative OT Security Training, Collaborative OT SOC Services *(AIRBUS)*; Functional Safety Testing *(Rugged Tooling)*; Energy Forecasting as a Service *(ISEP)*; MITRE/OWASP Attack scenarios *(BITTIUM)*; Supply Chain Attack Impact Modelling *(BIGS)*
- **10 new systems:** 3 Aerospace Manufacturing IIoT Systems *(AIRBUS)*; 1 Automotive Manufacturing CPS *(TRIMEK)*; 1 Distributed Manufacturing Supply Chain *(BITTIUM)*; 1 Intelligent Cheese Making Machine *(HIGH METAL)*; 1 Consumer Electronics Real Time Asset Tracking *(VESTEL)*; 1 Optimisation System for Rail Vehicle production *(ALSTOM)*; 1 Autonomous Mobile Robots Fleet *(ASTI MOBILE ROBOTICS)*

Standardisation

- **Industrial standards:** IEC 61508, DID DI-MGMT-82141, EUROCAE ED 204, SAE J3061_201601, ISO/SAE 21434, ISO 26262, ISO 10218 Series, ISO 15066, ISO 14539:2000
- **Security standards:** IEC 61158, ISO/IEC 27000:2018, ETSI TR 102 893, ISO/TR 22100-4, ISO/IEC 19778, ISO/IEC 15408 Series, ISO/IEC 20546:2019, IEC 62443, ISO 13849-1:2015, ISO/IEC 15408, IEC 62714 Series

Patents & Spin-offs

- 1 patent filed: IoT Fingerprint by AIRBUS
- 1 spin-off: LISA GmbH

CyberFactory#1

17032

Partners

Canada

- Bluewrist Inc.

Finland

- Bittium Wireless Ltd.
- High Metal Oy
- Houston Analytics Oy
- Netox Oy
- Rugged Tooling
- VTT

France

- Airbus Protect SAS
- IRT SystemX

Germany

- Airbus Protect GmbH
- Aviawerks International GmbH
- BIGS
- Bombardier
- Fraunhofer AISEC Institute
- HTW Berlin University of Applied Sciences
- InSystems Automation GmbH
- LISA Deutschland GmbH
- OFFIS

Portugal

- IDEPA
- ISEP
- SisTrade Software Consulting S.A.

Spain

- Airbus Defence & Space
- ENEO Technologia S.L.
- Grupo S21sec Gestion S.A.U.
- PAL Robotics
- Trimek

Türkiye

- GOHM
- Lostar Information Security
- Vestel

Project start
December 2018

Project end
June 2022

Project leader
Adrien Bécue, Airbus Protect SAS

Project email
adrien.becue@airbus.com

Project website
https://www.cyberfactory-1.org/