CyberFactory#1

Addressing opportunities and threats for the Factory of the Future

Success story

The digital transformation in production is expected to bring huge benefits to industrial manufacturing but can also create new threats and risks to the Factory of the Future (FoF). Cyber risks for future factories include malware, data leakage or confiscation, adversarial machine learning and 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.

This global challenge was picked up by the ITEA project CyberFactory#1, gathering 29 partners from seven countries – Canada, Finland, France, Germany, Portugal, Spain and Türkiye. 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.

Creating simulation, optimisation and resilience

Their 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.

Digital twins simulating manufacturing chain operations and communication processes

The project's use-case owners were predominantly factories, which have tested and demonstrated these technologies in a mix of real and simulated environments.

Project start
December 2018

Project end
June 2022

Project leader
Adrien Philippe Bécue
Airbus CyberSecurity SAS, France

More information
https://itea4.org/project/cyberfactory-1.html

In an Airbus factory in Spain, the robotic system Roboshave has been successfully demonstrated for automatic jo-bolt rivet shaving in aircraft rudders, which control an aircraft's rotation on its vertical axis. Initially a standalone piece of equipment, Roboshave was integrated into a distributed IoT platform designed to support real-time monitoring, process optimisation, and quality control. The CyberFactory#1 project has significantly enhanced Roboshave by developing its digital twin, connecting it to a secure IIoT platform and protecting it against a wide range of cyber-attacks through simulated security measures.

These advancements have led to reduced lead times, lower production and maintenance costs, decreased product defects, and mitigated security risks. The digital twin enables the simulation of numerous attacks, ensuring that robust security measures are in place. Roboshave now achieves 100% traceability of processes and products from the shop floor and provides 100% accuracy in near real-time information on dashboards - features that were not available before the project. Additionally, automating communication between machines and the manufacturing execution system has eliminated the need for manual machine data collection by human operators, thus reducing human error and improving worker satisfaction by allowing them to focus on more engaging tasks.

Roboshave has contributed to significant cost savings by preventing quality failures, with estimated annual savings of 25,000 euros. Data analysis has pinpointed areas of quality failures in Roboshave's operations, facilitating root cause identification and problem resolution. In terms of predictive maintenance, the project has leveraged historical data to analyse the behaviour of tools in the rivet shaving operation, specifically the End-Effector, resulting in reduced tool failures.

Much of CyberFactory#1'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. Complex industrial automation like Roboshave can be designed, upgraded and tested without any negative impact on the real assets.

RF technology increasing security

The Turkish project partner GOHM Electronics applied another technology in the CyberFactory#1 project – radio frequency (RF) fingerprinting – to increase security in wireless communication. Following further progress on these developments, they have successfully completed an RF sniffer system for use in the defence industry. Utilising the same technology, they created a follow-up project which pioneers the development of data-driven, AI/ML-based security solutions to address the evolving challenges of 6G services and networks within the future cyber-physical continuum. Currently, they are in discussions with one of the largest cellular operators in Türkiye to co-develop spectrum sensing devices that can detect potential threats and address false base station issues. They are constantly investing in this technology and see significant potential for its future applications.

Reducing manufacturing costs, waste, efforts and lead time and enriching portfolios

For factories, the impact of CyberFactory#1's results generally consists of internal exploitation to reduce manufacturing costs, waste, efforts and lead time.

For security and technology vendors, exploitation is primarily focused on enriching their portfolios with new products and services. For example, Airbus in France collaborated with Bittium in Finland using Airbus' CyberRange system to simulate the cybersecurity of Bittium's distributed virtual manufacturing solution. The outcomes of these simulations are taken into practice and, as a consequence, the cybersecurity of Bittium's solution is improved. These virtual manufacturing solutions are used in all manufacturing events of Bittium to control the manufacturing process, product quality and all production phases of the

The project has been recognised as a pioneer of Industry 5.0

distributed manufacturing network. Bittium's manufacturing needs vary from very small batches up to mass market deliveries in medical products.

Vestel has built a new Manufacturing Execution System (MES/MOM) in order to leverage new capabilities such as real-time tracking and traceability tools. Scrapped electronics components from SMT machines in production lines could not be estimated correctly in previous versions of MES. Due to these new tools, scraped material quantities are now tracked in a much better way. With the help of this new MES, easier material logistics, improved efficiency and process resilience can be achieved. Vestel is employing both development and maintenance engineers to improve the newly built MES traceability, maintenance and real-time tracking tools.

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 eight million euros and more than 80 new jobs in the digital twin domain, 28 million euros and over 100 jobs in Industry 4.0 and 114 million euros and more than 250 jobs in IIoT security. This total impact equals 150 million euros and >450 jobs across the consortium.

Paving the way to the next industrial revolution

Meanwhile, dissemination of this vital technology is ongoing. Alongside many presentations at conferences and contributions to a book, the University of Applied Sciences of 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.