Airbus CyberSecurity look to the future with collaborative international CyberFactory#1 research project

by Matthias Glawe, Security Engineer ICS

Munich/Ottobrunn, 12 September 2019 – 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). To address these new threats and risks, Airbus CyberSecurity joined the international research project **CyberFactory#1**, which is part of the ITEA cluster of the EUREKA program bringing together 35 industrial and research partners from 8 countries.

The CyberFactory#1 project

CyberFactory#1 aims to design, develop, integrate and demonstrate a set of key enabling capabilities to foster optimisation and resilience of FoF. It will address the need of pilot projects across aerospace, automotive and electronics industries around use cases such as collaborative product design, autonomous machine reconfiguration, continuous product improvement, distributed manufacturing and real time situational awareness. It will also propose preventive and reactive capabilities to address cyber and physical threats and safety concerns to FoF.

The CyberFactory#1 approach

1. As a first step, **realistic digital models of FoF and their ecosystem**, enabling to perform simulation-aided design, testing and validation of optimisation and resilience components will be developed.

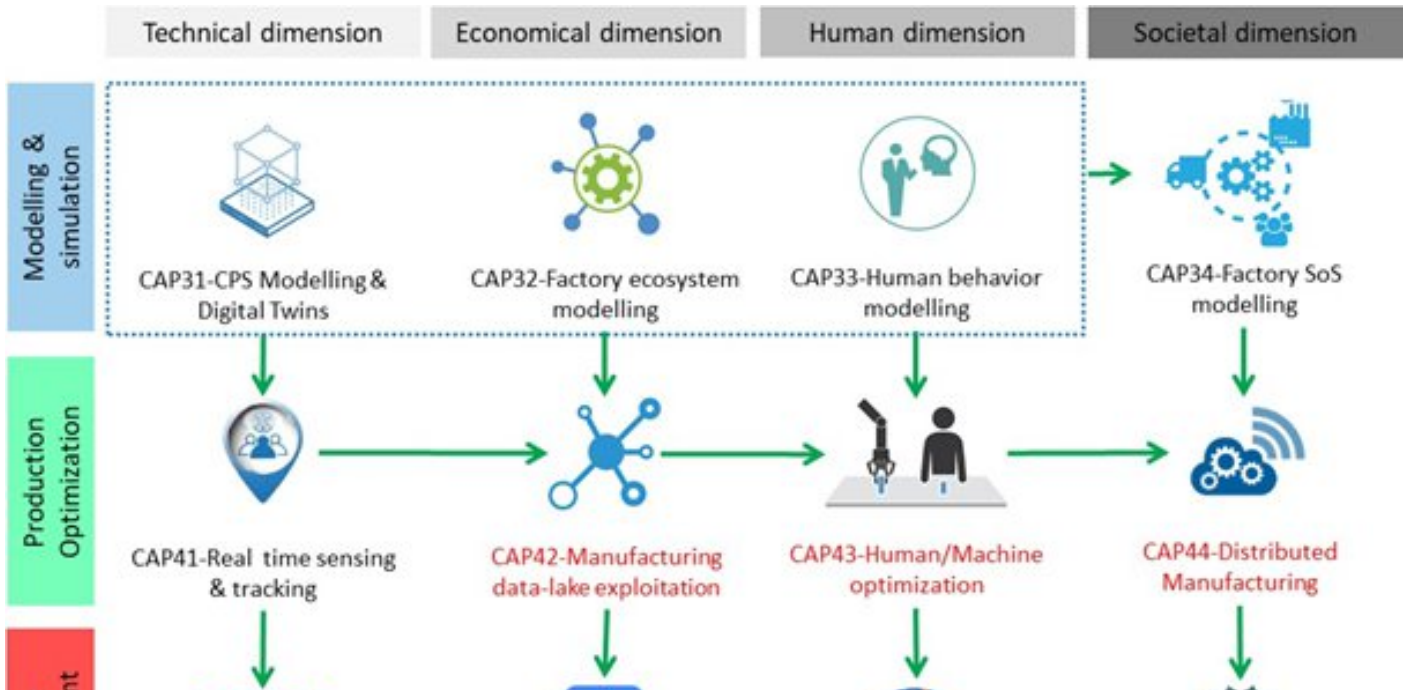
2. A second output will be the **development of key technology bricks for the optimisation of the FoF**. This includes enabling real-time sensing and tracking of materials, humans and machines on the shop floor, optimisation of human/machine collaboration, distributed manufacturing scenarios, data lake exploitation for process improvement and data-centric business creation.

3. A third output will be to **address the need for enhanced resilience of FoF**, starting with human/machine access & trust management, human/machine behaviour watch, robust machine learning and self-healing mechanisms.

The key capabilities will be demonstrated in realistic environments reflecting the variety of possible new factory types like user-centric plants or learning factories and take into account business model shifts like turning products into services or developing data services on top of manufacturing activities.

Project structure & Airbus CyberSecurity goals

The CyberFactory#1 project is structured into seven work packages (WP). WP1 and WP7 are focusing on project management and dissemination. WP2 as starting point to the project work, focuses on the definition of new business models, Use-Cases, Misuse-Cases and System-of-System Architectures for the Factory of Future. Based on these results, WP3, WP4 and WP5 are working on providing the key capabilities shown below. WP6 provides an environment to implement, test and present the developed key capabilities in an integrated way.



Key capabilities in Cyberfactory#1 focus

In this context, Airbus CyberSecurity is focusing on capabilities **to enhance the resilience for FoF to be able to provide and monitor security in FoF.**

This focus is addressed by the capabilities CAP53 and CAP54. As a prerequisite to these capabilities Airbus CyberSecurity will also work on the creation of CPS Modelling (CAP31) to be able to provide virtual CPS models as an enabler for training and testing on security solutions. These models are based on Misuse-Cases defined as part of WP2. By defining Misuse-Cases in cooperation with CyberFactory#1 partners, Airbus CyberSecurity is looking forward to **identifying the needs and requirements of future security environments in FoF**.

As part of CyberFactory#1 demonstrator, Airbus CyberSecurity is planning to demonstrate the developed capabilities to illustrate the possibility of a resilient FoF by performing the earlier identified Misuse-Cases.

Airbus CyberSecurity GmbH as country lead

In addition to the work on the capabilities Airbus CyberSecurity GmbH acts as **country lead** to coordinate the work between the eight German partners inside the whole research project. The German partners are HTW Berlin, Fraunhofer AISEC, OFFIS e.V., Bombardier Transportation GmbH, Aviawerks International GmbH, InSystems Automation GmbH and the Brandenburg Institute for Society and Security (BIGS).

Further Steps

In a first step Airbus CyberSecurity supports in the definition of Use-Cases and will soon start, with its research partners, the definition of Misuse-Cases by executing risk assessments to find risks to the FoF and later identify Misuse-Cases to the FoF which need to be addressed by new or additional security solutions. In cooperation with our partners, not only security risks but also risks targeting the safety of FoF are in focus to enable future solutions addressing security as well as safety.

Acknowledgment

Airbus CyberSecurity GmbH acknowledges the funding for the CyberFactory#1 project by the German Federal Ministry of Education and Research (funding number 01IS18061A).

Find out more here

Back to News