Towards resilient Factories of Future
Defining required capabilities for a resilient Factory of Future[1]

Dipl.-Ing. **Matthias Glawe**, Airbus Cybersecurity GmbH, 82024 Taufkirchen, Matthias.glawe@airbus.com
Linda Feeken M.Sc., OFFIS e.V., 26121 Oldenburg, linda.feeken@offis.de
Björn Wudka M.Eng., HTW Berlin, 12459 Berlin, bjoern.wudka@htw-berlin.de
Ching-Yu Kao M. Sc., Department Cognitive Security Technologies, Fraunhofer Institute for Applied and Integrated Security AISEC, 85748 Garching, ching-yu.kao@aisec.fraunhofer.de
Elham Mirzaei M.Sc., InSystems Automation GmbH, 12489 Berlin, mirzaei@insystems.de
Torsten Weinhold, Bombardier Transportation GmbH, 02625 Bautzen, torsten.weinhold@rail.bombardier.com
Alexander Szanto, Brandenburg Institute for Society and Security, 14482 Potsdam, alexander.szanto@bigs-potsdam.org

Kurzfassung

Die Digitalisierung und fortschreitende Implementierung neuer Techniken für die Factory of the Future (FoF) bringen neue Möglichkeiten aber auch neue Bedrohungen mit sich, die beachtet werden müssen um die Optimierung der Produktion und die Bedürfnisse von Safety, Security und Resilienz zusammenzuführen. Das Projekt CyberFactory#1 adressiert diese Anforderungen in einem Framework möglicher Fähigkeiten für resiliente FoF Umgebungen. Um diese Fähigkeiten näher zu definieren wurde ein Ansatz basierend auf Use-Cases und Misuse-Cases gewählt, um Anforderungen und ein Implementierungsplanung ermitteln zu können.

Abstract

Ongoing digitalization and implementation of new techniques for the Factory of Future (FoF) brings up new opportunities as well new threats that must be concerned to **conciliate optimization** of the supply and manufacturing chain with the need for security, safety **and resilience**. The CyberFactory#1 project addresses these needs by providing a framework of possible capabilities for resilient FoF environments. To further define these capabilities an

[1] This paper was first presented at the conference AUTOMATION 2020 and is now available in: VDI-Berichte Nr. 2375, 2020, VDI Verlag; ISBN 978-3-18-092375-8.

approach was used to define requirements and implementation planning based on Use-Cases and Misuse-Cases to enable the development of needed capabilities for resilient FoF.

1. Motivation

Digitalization and automation are considered to be two of the key enablers for ensuring future profitability of factories [1]. An increasing degree of digitalization of procedures in the production process and of connection and interaction of systems within a factory are paving the way for the FoF: The FoF is no longer a collection of sporadically interacting individual systems, but becomes a multifunctional production system. It should be able to deal efficiently with short production cycles and dynamically changing production content. When facing disturbances like unexpected behavior of the logistic system or unusual interactions between human workers and systems, it should react flexibly and adequately. Consequently, new techniques are needed to improve the level of optimization and resilience of the FoF.

Those new techniques do not only imply new opportunities, but are also source of new threads to the FoF [2]: Digitalization of processes leads to increased reliance on vulnerable IT components. Enabling automated interaction of systems and the usage of data-based services does also mean to create interfaces between systems that can be used as entry points for blended attacks. Enabling the factory to react quickly to changes in the production process and disturbances increases the level of dynamicity in the FoF. This confuses the issue of the detection and retracement of anomalies in the FoF like unexpected delays in the logistic system. Those anomalies can be induced by security and safety threads. Hence, one key problem that must be addressed in the context of the FoF is the need to conciliate optimization of the supply and manufacturing chain of FoF with the need for security, safety and resilience against cyber and cyber-physical threats.

The transnational research project *CyberFactory#1* [3] focuses on tackling this problem. The project is shortly introduced in Section 2. The following two sections present the used approach for the identification of key capabilities of the FoF for optimization and resilience in *CyberFactory#1*. The approach is based on Use-Cases (Section 3) and Misuse-Cases (Section 4). Both Use-Cases and Misuse-Cases are basis for a systematic derivation of requirements on FoF capabilities. Section 5 gives insights on those requirements and on planned development and demonstration architecture for those requirements and sketches the realization of the development plan for the following project runtime.

2. The CyberFactory#1 Project

The CyberFactory#1[4] project consortium comprises nearly 30 partners from eight countries, involving industrial and research partners. In this paper we present works performed by the German consortium partners inside the CyberFactory#1 project. The German part of the research consortium is currently including 7 partners and started working on June 2019.

CyberFactory#1 aims at designing, developing, integrating and demonstrating a set of key enabling capabilities to foster optimization and resilience of the FoF. It will address the needs of pilots from different industries around Use-Cases such as collaborative product design, autonomous reconfiguration, continuous product improvement, distributed manufacturing and real time situational awareness. It will also propose preventive and reactive capabilities to address cyber and cyber-physical threats and safety concerns to the FoF. In comparison with other Industry 4.0 related projects, the differentiating factors of our approach are threefold. First, the system considered is not a simple manufacturing asset, nor a sum of isolated assets, but a network of factories, which is considered in a System of Systems (SoS) approach. The challenge is to propose novel architectures, technologies and methodologies to optimize the level of efficiency and security of this SoS in a context where every step towards digitization exposes the manufacturing process to widening cyber-threats. Last but not least, we intend to solve more than the technological challenges of Industry 4.0 in this project. Many studies have shown that demonstrating technical feasibility would not be sufficient to get the buy-in from workers, managers, entrepreneurs, decision-makers and customers about novel manufacturing approaches. CyberFactory#1 will therefore embrace technical, economic, human and societal dimensions at once shown in the capability framework of possible capabilities for resilient FoF environments in Figure 1.

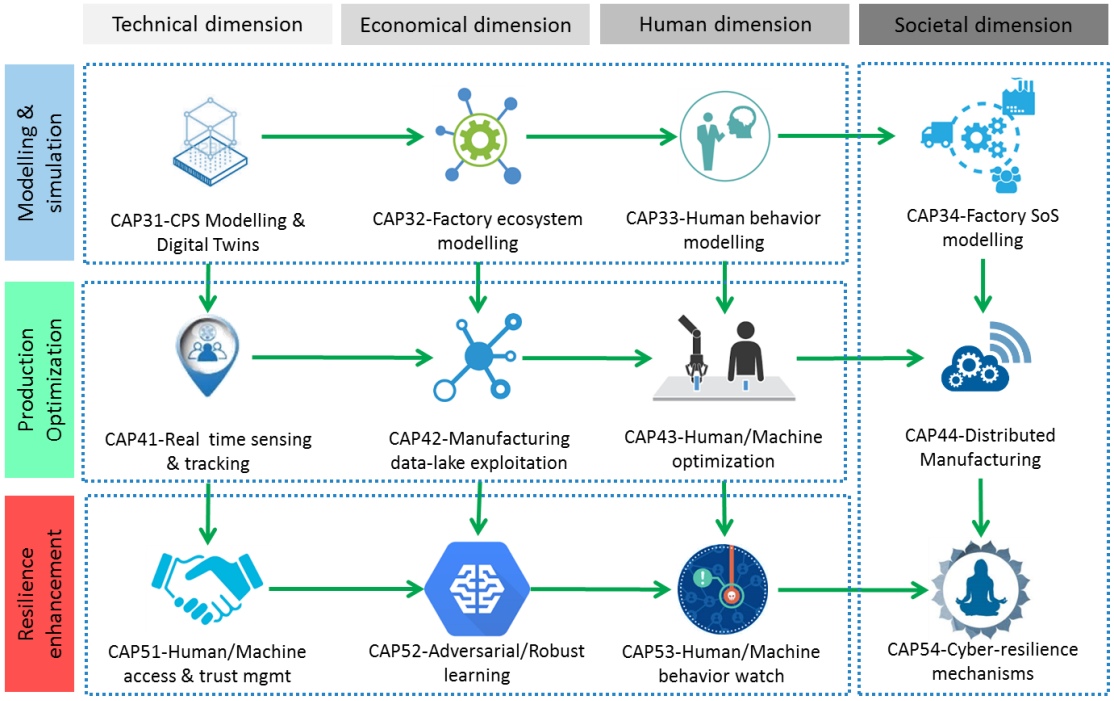

Figure 1: CyberFactory#1 Capability Framework

This capability framework addresses capabilities on modelling and simulation, production optimization and resilience enhancement. Each capability category is reflected on technical, economical human and societal dimension. This framework provides a first idea on necessary capabilities. Nevertheless the level of detail is far too low to start developing capabilities. To further identify the necessary and required capabilities for a resilient FoF, an approach based on the definition of Use- and Misuse-Cases was applied to focus on capabilities necessary to realize and protect existing Use-Cases.

3. Use-Case Definition

In the CyberFactory#1 project ten Use-Cases were described in total, focusing on different areas of the FoF, e.g. quality control, safety in human-machine interaction and security in the communication between FoF components. As part of these challenges two of those Use-Cases were defined by the German consortium in the area of production automation using flexible autonomous transport systems and hence supporting the logistic system of the FoF:

(1) a complex transportation system with automated guided vehicles (AGV) inside a production facility, and

(2) a fleet of robots capable of performing transportation jobs without central management.

Use-Case (1) focuses on a production hall of Bombardier in which the final assembly of various types of rail vehicles is done. The assembly process is distributed among several working stations on three levels. The provision of small parts and large components on the various

levels of the production lines is currently carried out exclusively manually and uses huge material buffer zones. This provision shall now be automated by using AGVs. A key challenge is the high rate of interactions between humans and AGVs, since human workers are involved in all steps of the assembly process. The overall goal of this Use-Case is to develop an automated material provision system that is safe not only for human workers, but also ensures safety of supply for the working stations. Additional objectives include the reduction of the material buffer, reduction of manual handling effort in the logistic system and a reduction in the error rate in the supply of material.

Use Case (2) focuses on a fleet of automated transport robots that perform factory internal logistics tasks independently and autonomously as developed by InSystems. The robots do not require special infrastructure elements such as rails, reflectors or beacons but localize themselves within a pre-scanned map of the factory using live sensor data from a laser scanner. In the current development status, the robots are safe for deployment in environments with humans, drive around obstacles and are able to adjust their planned path. The fleet receives transport requests from machines of the factory via wireless network. The robots are communicating with each other to distribute these orders among the fleet without requiring a central fleet management unit. The basic communication is sketched in Figure 2.

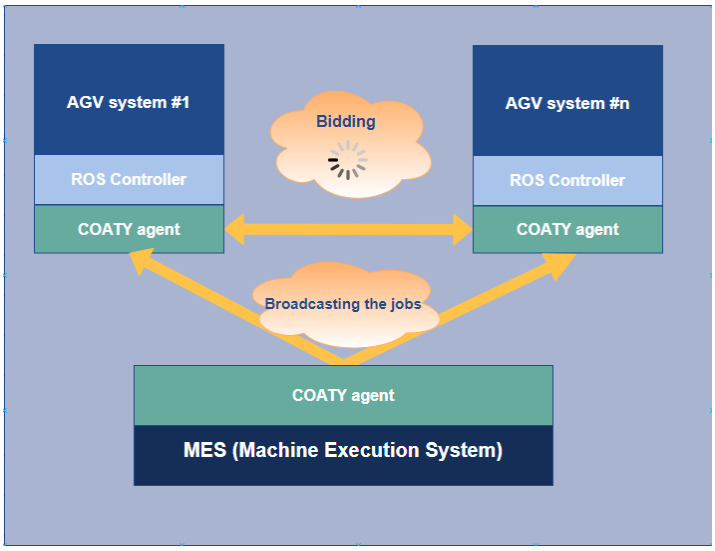

Figure 2: Basic architecture and interaction in the transport robot Use-Case

To become a valuable part of the FoF, the fleet of robots shall achieve several goals, including the following exemplary goals:

- The production shall never stop: The fleet must fulfill all incoming job requests in time.
- Green efficiency: The robots shall operate as energy efficient as possible.
- Equal wear and tear: The robots shall operate in such a way that all agents of the same age show approximately the same usage.

- Battery health and safety: Robots shall prevent their battery depleting or overcharging.

Currently, the robots can only use information on the actual state of the fleet for deciding on their next actions (e.g. taking over a transport task, charging the battery, driving to a storage or a machine). In the CyberFactory#1 project, the robots shall become smarter by increasing their level of context awareness: During normal operation of a transport robot fleet, large amounts of process data can be collected. This data can be utilized to optimize the workflow and performance of the fleet by adapting to recurring patterns in the work cycle of the factory. Usually, processes in factories are relatively repetitive and can be predicted with a good amount of certainty. Most changes in the logistic needs are reoccurring, e.g. a peak in the number of transport tasks each morning at 8am, when all machines in the factory are turned on simultaneously. If robots are able to identify such reoccurring patterns, they can react to them proactively, e.g. charging their battery before the machines are turned on at 8am. Additionally, comparing observed FoF behavior with precise predictions based on patterns allows detecting anomalies. An anomaly can indicate threats on safety and security in the FoF. A transport robot fleet that recognizes production patterns and anomalies and adapts dynamically to changes is a competitive advantage for transport robot developers as well as for factory operators. Such dynamic adaption shall be robust against new types of adversarial attacks which will be considered in this project. Adversarial attack means slightly changes of inputs to the sensors leading to wrong decisions.

Based on the Use-Case description, the following required FoF capabilities can be derived:

- It shall not only be possible to collect huge amount of data on observed FoF behavior in a data lake, but also to identify reoccurring patterns as basis for predictions.
- Robots shall be able to perform automated real time reconfigurations for reacting proactive to predictable FoF behavior in order to optimize the fleet performance.
- It shall be possible to detect significant deviations of predicted and observed FoF behavior. Robots shall be able to react to detected anomalies in such a way that the robot goals are still fulfilled as good as possible (increasing resilience).

The second Use-Case will be presented in the following chapters to provide examples on the next steps towards the development and validation plan.

4. Misuse-Case Definition

As the definition of Use-Cases provided information mainly on capabilities to optimize the FoF, an approach was needed to determine the necessary capabilities to enhance the resilience of FoF environment. To identify these capabilities, Misuse-Cases were created: “A misuse case is simply a use case from the point of view of an actor hostile to the system under design.” [5]

To create such Misuse-Cases basing on the Use-Case descriptions, risk assessments were performed to identify vulnerabilities of the FoF originating from the functional, safety, and security domains. These risks were aggregated into Misuse-Cases describing scenarios of damage to the FoF. Subsequently, mitigation means were identified to master the identified risk, thereby revealing gaps which cannot be mitigated by state-of-the-art measures. This process is shown below in Figure 3 and will be explained in further details in the following paragraphs and will be reflected focusing on the robot fleet Use-Case.

Figure 3: Misuse-Case analyzation process

The main input on the Misuse-Case definition was generated by risk assessments performed together with the Use-Case owners. The goal of the risk assessment was to look at functional, safety and security risks in a combined session to get an overall view of the risk structure. To perform the risk assessment an adapted approach based on IEC62443 [6] was used, since ICE62443 focuses only on security issues for existing control systems. For our Use-Cases safety and functional risks are also relevant and some of the involved components are not yet defined in detail.

As a first step of the risk assessment a high-level risk assessment was performed based on the Use-Case description and in cooperation with the Use-Case owner to identify first ideas of possible risks to the Use-Case considering at the Use-Case in whole. The high-level risks were described using a risk name, a risk description and a first description of the risk result. Having the high-level risk in mind, the known parts of the Use-Cases were discussed and structure to gain a better understanding of Use-Case functionalities as a basis to the following detailed-level risk assessment. As part of the detailed-level risk assessment, the high-level risks were split down into more precise risks and information regarding the possible impact, the expected probability and the source of the risk were added. As an example Table 1 shows one high-level risk (in bold) with two assigned detailed-level risks addressing the same risk with different sources and outcome.

Table 1: Risk Example

Name	Description	Impact	Prob.	Result

Wrong data communication between robots	**Wrong data (e.g. obstacle information, transport order) is exchanged between robots**	**-**	**-**	**Misinformation is spread to the robot fleet leading to misbehavior**
Wrong obstacle existence notification	Robot notified that there is an obstacle but it doesn't exist due to a sensor failure	Medium	Low	Wrong obstacle knowledge leads to delay on performing transport jobs
Wrong obstacle existence notification	Robot notified that there is an obstacle but it doesn't exist due to the manipulation of the robot	High	Low	Incorrect knowledge of obstacle leads to delays on performing transport jobs up to complete failure of the transport system

The addressed risks relate to the systems' planned ability to exchange obstacle information between robots. An exchange of wrong information leads to delays on transport jobs were impact and probability are depending on whether the risk is originating by a failure or generated by intent. In the example two risks were introduced concerning incorrect notification of existing obstacles as a result of a sensor failure and a cyber security attack. A cyber-attack is assumed to have high impact as an attacker can be expected to achieve the highest possible impact by placing obstacles at critical positions, while a sensor failure will place false obstacles randomly. For the two German Use-Cases previously described 93 detailed-level risks were identified including 23 risks resulting from the Use-Case surrounding legacy infrastructure and 70 risks resulting from the planned Use-Case design. As lessons learned from this risk assessment process it should be noted that an adaption of the normative risk assessment approaches to FoF Use-Cases under development is reasonable. Also changes to the risk assessment should be expected in the upcoming development with more Use-Case details been known. Nevertheless an early knowledge and documentation of risks supports resilience by design, which should be included in the Use-Cases. The aim of the risk assessment was to provide input to Misuse-Cases and to the development of capabilities in subsequent work packages. Thus, the results of the risk assessment do not represent a full risk assessment on all safety and security aspects ignoring many aspects identified as legacy or solved by state of the art. For example, safety aspects of transport robots, which are independent from the development of the Use-Case were not concerned.

Starting from the results of the risk assessments, Misuse-Case were derived aggregating risk to an attack story or damage scenario. The description of Misuse-Cases included a description, assumptions made on the execution of the Misuse-Case, an identification of the Misuse-Case source and a staging with references to risks from the risk assessment. The Misuse-Cases were concluded by possible state-of-the-art mitigations measures and an analyzation of mitigation gaps, which need to be addressed in the upcoming work packages of CyberFactory#1. On the robot fleet Use-Case, five Misuse-Cases were identified:

MUC1 – Misbehaving Robot

MUC2 – Increasing number of transport tasks

MUC3 – Machine breakdown & involvement of humans

MUC4 – Robot breakdown & insufficient strategy choice

MUC5 – Machine learning related Misuse-Case

As an Example some aspects of MUC1 should be discussed in the following paragraphs. This Misuse-Case focuses on the vulnerability of wireless communication between robots, which acts as a gateway to the wider backend. In a staged attack, the wireless communication will be intercept and malicious messages will be inserted into the communication between the robots. For this purpose a rogue simulated robot will be created. Once the rogue robot has become part of the fleet, the Use-Case can be sabotaged by inserting false data. To perform this Misuse-Case it is assumed the wireless network security can be compromised e.g. by a dictionary attack. Figure 4 shows the situation once the attacker entered the network as a rogue robot.

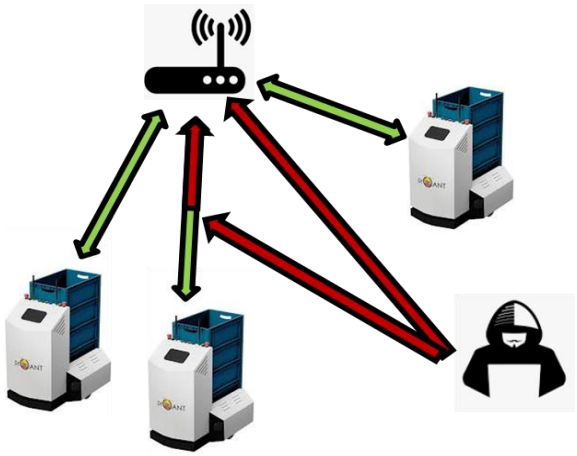

Figure 4: Attacker accessed robot network

The attackers' goal could include disruption of the production environment, financial gain, causing damage as well as proof of own skills. The observed attacker in this Misuse-Case has knowledge about the used communication protocol as well as the industrial environment. Furthermore he has knowledge about networks specifically wireless networks and uses open

source software to reach his goals. Involving the aforementioned skills and in relation to the IEC62443, the attacker is classified as Level 3 attacker. The Level 3 attacker drives intentional attacks, with sophisticated means and moderate resources. He has Industrial Control System specific skills and moderate motivation. Once connected to the robot fleet as a rogue robot the attacker can undermine the robot network by e.g. disconnecting other robots, sending false information about obstacles or corrupting the task bid process. At fleet level, one of the robots is now misbehaving, leading to at least reduced performance of the robot network, or even to a complete stop of the logistics system.

The described attack can be partially mitigated by state-of-the-art security measures such as implementing signature-based authentication for robots, securing the network hardware configuration or disabling unneeded network services. Even though these mitigations measures will result in a more resilient system that makes it more difficult to perform such a Misuse-Case, it must always be expected that new or unknown vulnerabilities in the robot or wireless network could result in such Misuse-Case scenario. To detect the abnormal behaviour, capabilities are needed to monitor the behaviour of the transportation system and the robots. One way to detect abnormal behaviour based on the monitored behaviour could be a comparison of the monitored behaviour with a simulation/model of expected or normal behaviour. This requires the development of capabilities to apply digital twin models as a basis for behaviour watch techniques.

5. Requirements derivation, demonstration architecture and the way ahead

Based on the given Use-Cases and the Misuse-Cases, an architecture design was developed to meet the given requirements. The developing architecture is shown in the Figure 5. Based on the frequently used industrial internet reference architecture of Lin [7] our factory architecture is designed. The factory architecture is constructed as three tier architecture: edge tier, platform tier and enterprise tier. All three tiers are parts of an overall factory structure which are connected to each other by dependencies. The edge tier describes all facilities and autonomous working devices that can be located in the factory hall. The platform tier is superordinate to the edge tier, which monitors all systems contained in the edge tier and platform-tier. The enterprise tier monitors all distributed platform-tier within a company to monitor and reconfigure the overall system.

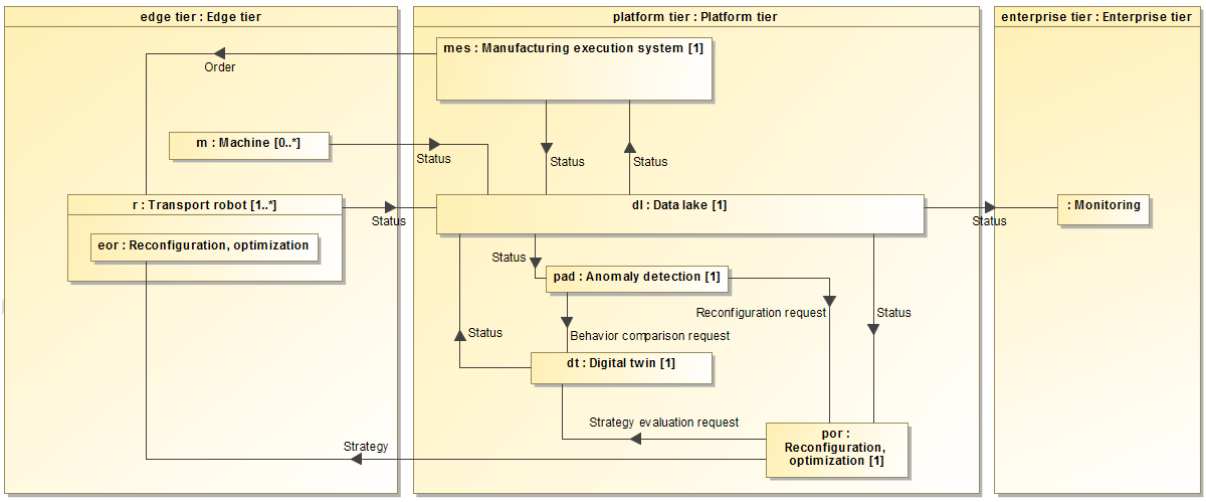

Figure 5: Demonstrator Architecture for the FoF

In the three tiers nodes are integrated which will be described in the following. Since certain nodes, such as reconfiguration/optimization, can exist in different forms in each of the three tiers, and since we are focusing on basic functions and principles, we need only one element at a time and do not consider similar elements on the other tiers. Therefore, in the first development step, the architecture is focused on the edge-tier and platform-tier. Usage of components on an enterprise tier is addressed in international cooperation.

For the robot fleet Use-Case, the robots and machines of a factory building are embedded into the edge-tier. The robots are used to deliver material to machines and pick up finished goods to a storage location or to the next production step. Within the platform-tier there is the manufacturing-execution-system (MES) which is responsible for providing transport orders to the robot fleet, the data-lake which consists of historical and real time data, the digital-twin which simulates the architecture, the anomaly detection to detect failures of the architecture and the reconfiguration/optimization to select new strategies. For the Use-Case the developed architecture model will now be described. In the factory of the robot fleet Use-Case, distributed machines generate orders that are executed by the transport robots. The goal of the system is to optimize the transportation needs of the plant according to given optimization criteria. The transport robots can bid on every order to take over the task. The amount of the respective bid depends on the feasibility of an order for the respective transport robot. The order is taken by the robot having the lowest bid. To monitor the architecture the status data of the machines and transport robots from the edge tier, generated status data from the digital-twin and status data from the MES are stored in the data lake. Anomaly detection can compare and analyse the collected real-time data and the historical data consisting of past successful orders. An anomaly is the deviation of the overall system or system parts from prediction from the digital twin, historical data or common behaviour. In case of anomaly a reconfiguration/optimization

of robots is initiated. For reconfiguration/optimization two approaches are being pursued the centralized and decentralized approach. In the centralized approach, reconfiguration within the platform tier is performed simultaneously for all robots. The decentralized approach, on the other hand, embeds the reconfiguration/optimization within each individual transport robot in edge tier. In the reconfiguration/optimization process, suitable strategies are now selected based on the anomaly, states within the data lake and the system goals. The highest goal to be achieved is to fulfil the orders as soon as possible. After selecting a strategy from a pre-defined strategy catalogue, it is tested by the digital-twin. If the test is successful, the selected strategy is passed on to the transport robots, which then execute it. For example by changing the transport robots by functional goals such as changing the minimum battery level, this will then have an effect on the bidding process.

For the development of the described architecture some components will be newly developed others are provided by project partners. The focus of the development is on the platform tier. In the course of the project the digital-twin, the anomaly detection and both approaches of reconfiguration/optimization will be developed. It is also necessary to identify strategies that can be used for reacting to detected anomalies. At the end we want to develop and implement a demonstrator which fulfils all capabilities required by the German Use-Cases as part of the CyberFactory#1 project. In this case we need to interact with the other European project partners for applying their solution and supporting them on their Use-Cases and Misuse-Case with the capabilities developed inside the German consortium. Such development tasks will also include cooperation with other international project partners. Through the successful implementation of such architecture it is possible to increase the resilience on safety and security issues within the FoF significantly.

In conclusion it could be stated that the described approach based on Use- and Misuse-Cases lead to the requirements and architecture which needs to be fulfilled to ensure resilient FoF. The described approach was afterwards reused by some project partners in other research projects and FoF development activities.

6. Acknowledgment

The research project was carried out in the framework of the industrial collective research programme as part of ITEA framework. It was supported by the Federal Ministry of Education and Research (BMBF, Germany, funding no. 01IS18061A).

References

[1] Kagermann, Henning (2015). Change Through Digitization—Value Creation in the Age of Industry 4.0. In: Albach H., Meffert H., Pinkwart A., Reichwald R. (eds) Management of Permanent Change. Springer Gabler, Wiesbaden

[2] Luthra, Sunil & Mangla, Sachin Kumar (2018). Evaluating challenges to Industry 4.0 initiatives for supply chain sustainability in emerging economies. In: Process Safety and Environmental Protection, volume 117, p. 168-179

[3] Becue, Adrien & Fourastier, Yannick & Praça, Isabel & Savarit, Alexandre & Baron, Claude & Gradussofs, Baptiste & Pouille, Etienne & Thomas, Carsten (2018). CyberFactory#1 — Securing the industry 4.0 with cyber-ranges and digital twins. 14th IEEE International Workshop on Factory Communication Systems (WFCS). DOI 10.1109/WFCS.2018.8402377.

[4] https://www.cyberfactory-1.org/

[5] Alexander, Ian (2003). Misuse cases: use cases with hostile intent. In IEEE Software (Volume: 20, Issue: 1, Jan.-Feb. 2003). DOI: 10.1109/MS.2003.1159030

[6] IEC/TS IEC/TS 62443-3-2 – Industrial communication networks – Network and system security – Part 3-2: Security risk assessment and system design, International Electrotechnical Commission;

[7] Lin, Shi-Wan & Mellor, Stephen & Miller, Bradford & Durand, Jacques & Joshi, Rajive & Didier, Paul, eds. (2015). Industrial Internet Reference Architecture. In Industrial Internet Consortium. Version 1.7, p: 37-39