Lecture Notes in Networks and Systems 849

Erik Puik
David S. Cochran
Joseph Timothy Foley
Petra Foith-Förster *Editors*

Proceedings of the 15th International Conference on Axiomatic Design 2023

Springer

Lecture Notes in Networks and Systems 849

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Erik Puik · David S. Cochran ·
Joseph Timothy Foley · Petra Foith-Förster
Editors

Proceedings of the 15th International Conference on Axiomatic Design 2023

Springer

Editors
Erik Puik
Professor of Smart Manufacturing
Fontys University of Applied Sciences
Eindhoven
Eindhoven, The Netherlands

Joseph Timothy Foley
Reykjavík University
Reykjavík, Iceland

David S. Cochran
Professor of Systems Engineering,
and Director
Purdue University Fort Wayne
Fort Wayne, IN, USA

Petra Foith-Förster
Stuttgart, Germany

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-49919-7 ISBN 978-3-031-49920-3 (eBook)
https://doi.org/10.1007/978-3-031-49920-3

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

In modern engineering, the ever-accelerating pace of technological innovation is matched only by the increasingly complex challenges we face. From manufacturing systems and smart robotics to healthcare technologies and aerospace designs, our efforts to innovate are set against a backdrop of intricate, interconnected systems. It is within this context that we gather for the International Conference on Axiomatic Design 2023. The Axiomatic Design community has advanced the field of more and more complex systems through research on methods for systems engineering, particularly on applications of design axioms and associated methodologies. AD has been applied by and for organizations to gain added value but also by universities to teach novice designers to produce better systems. AD has proven to be a logical and rational scientific framework for making the best decisions during the synthesis of a broad range of systems.

The aim of the ICAD is to unite scholars, practitioners, industry experts, and future leaders of the field to share research findings, best practices, and new applications of AD. Our focus is not merely to dissect individual components of systems but to understand how these components interact and coalesce to form integrated wholes. This holistic perspective is fundamental for tackling the multi-dimensional challenges of our near future and beyond, from sustainable development and cybersecurity to automation and data analytics.

We are grateful to our keynote speakers who have provided thought-provoking insights into their respective domains presented in original ways, for example, by comparing the turnover of ASML semiconductor processing systems with selling quite a few bunches of tulips. Special thanks goes to our sponsors Dr. and Mrs. Park for financially supporting the Axiomatic Design Research Foundation, without which this conference would not have been possible. I must also express gratitude to the members of the Program Committee and our dedicated team at Fontys Applied University of Sciences Eindhoven for their hard work in ensuring the success of the event.

Best wishes for an intellectually rewarding experience when reading (parts of) these proceedings. Our aspiration is that they serve as a valuable resource for further research and real-world applications of AD. The perspectives and approaches described herein are also a call to action to pass on the legacy of AD to a wider audience and future generations. And obviously, we encourage readers to engage with these contributions, collaboratively, constructively, and as always critically.

Erik Puik
Conference Chair,
ICAD2023

Contents

Axiomatic Design and Product Design

Conceptual Design and Learning Axiomatic Design

Axiomatic Design and Health

Axiomatic Design and Manufacturing

Design Decomposition for Cyber Resiliency in Cyber-Physical Production Systems

Tanel Aruväli[1](✉), Matteo De Marchi[1], Erwin Rauch[1], and Dominik Matt[1,2]

[1] Free University of Bozen-Bolzano, Piazzetta del Università 1, 39100 Bolzano, Italy
tanel.aruvaeli@unibz.it
[2] Fraunhofer Italia Research, Via A. Volta 13/a, 39100 Bolzano, Italy

Abstract. Digitalization and related networked systems integration and automation have increased the performance of manufacturing. At the same time, the vulnerability of the systems has increased significantly as networks are potential targets for attacks to compromise companies. Therefore, the study focuses on the functional design of cyber resiliency in cyber-physical production systems. To support functionality while emphasizing the resilience of manufacturing systems, Axiomatic Design is used as a design methodology for the concept design of a cyber resiliency module. Based on functional requirements, design parameters were decomposed and design guidelines for preparedness for cyberattacks were provided. The guidelines were applied to a cyber-physical demonstrator that realizes the Industrial Internet of Things with a digital twin. As a result, physical/virtual solutions for the system were found. Such an axiomatic design-based approach allowed for studying solution-neutral functional requirements that resulted in functional cyber resiliency solutions. The provided guidelines have practical value in the planning phase of manufacturing system networks to increase their long-term resiliency. This study fills the gap in the solution-neutral design of cyber resiliency in manufacturing companies.

Keywords: Axiomatic Design · Cybersecurity · Resilience · Sustainable Manufacturing · Industry 4.0

1 Introduction

In Cyber-Physical Production Systems (CPPS), cybersecurity is essentially important as the machinery and its processes are vulnerable due to network integrations. In traditional manufacturing, the link between machinery is a human. In the age of the internet of things, connectivity, remote control, and unidirectional data flow are enabled by virtual networks. Compared with physical access, digital access and intrusion to the shopfloor can be hidden, although the consequences may be even more harmful. In recent years, many companies have been attacked by threat actors and suffered while losing control over their digitally generated processes, workflow, sensitive customer data, or trade secret data. Often cyberattacks are targeted at companies that in addition to performance and credibility loss, must consider environmental impact [1].

E. Puik et al. (Eds.): ICAD 2023, LNNS 849, pp. 3–14, 2024.
https://doi.org/10.1007/978-3-031-49920-3_1

The research aims to derive design guidelines for today's intelligent manufacturing systems by decomposing and decoupling functional requirements (FRs) to derive the most inevitable design parameters (DPs) for cybersecurity purposes. More specifically, to find the concept DPs for CPPS to increase the level of resilience by applying an Axiomatic Design (AD) [2] approach. The work is limited to cybersecurity functions for preparedness for potential cyberattacks. It does not cover the avoidance of cyberattacks.

The paper is organized as follows. Section 2 explains the theoretical background of resilience, cybersecurity, and relevant AD studies. Thereafter, in Sect. 3 the research methodology AD decomposition and decoupling process is presented to derive design guidelines for resilient CPPS on cybersecurity. Section 4 presents the decomposition results used in the cyber-physical demonstrator. Finally, in Sect. 5 the results are further discussed, future perspectives found, and further research recommended.

2 Theoretical Background

2.1 Resilience and Disruptions

According to Gu et al. [3] resilience is the ability of a system to withstand potentially high-impact disruptions, and it is characterized by the capability of the system to mitigate or absorb the impact of disruptions, and quickly recover to normal conditions. In resilience, three main features and phases can be distinguished: absorption, adaptation, and restoration [4]. In the absorption phase, disruptions or the impact of disruptions is eliminated without loss in productivity. In the adaptation phase, the disruption has influenced production performance and adaptive changes are needed to restore productivity. According to the multi-criteria decision-making Analytic Hierarchy Process analysis [5], the Penalty of Change (POC), proposed by Alexopoulos et al. [6], was selected as the most practically usable resilience metric. It divides resilience into two main components: the probability of changes and the cost of changes. The method of POC originates from Chryssolouris and is calculated as follows [7, 8]:

$$\mathrm{POC} = \sum_{i=1}^{D} \mathrm{Pn}(X_i)\mathrm{Pr}(X_i) \tag{1}$$

where D is the number of potential changes, $\mathrm{Pn}(X_i)$ is the penalty (cost) of the i-th potential change and, $\mathrm{Pr}(X_i)$ is the probability of the i-th potential change to occur.

On a shop floor, disruptions can be internal such as product quality flaws or machine failures [9], or external such as pandemics, natural disasters, shortage of materials, cyberattacks, etc. [10, 11].

2.2 Cyber Resiliency

Cyberattacks are up-trending disruption sources. In addition to cyberattacks' probability to occur, also their influence has increased significantly. In the year 2022, the average ransom payment for cyber criminals to decrypt the hijacked data increased by nearly to 1 million $ [12]. Ransomware is just one type of malware. The other three most common types of malwares are viruses, worms, and Trojan horses. Malware's main goal is to get the payload delivered and installed in the victim's system. This enables a variety of network-related remote attacks to be taken.

In addition to overall resilience in manufacturing, CPPS are focusing on cyber resiliency. Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources [13]. For cyber physical systems' cyber resiliency, Haque et al. [14] proposed a metric and related simulation method to automate the resilience assessment process. From a cyber resiliency perspective at the industry level, critical infrastructure-related industries have been in research focus such as the oil and gas industry [15] and power plants [16]. In the manufacturing field, cyber resiliency is mainly studied regarding additive manufacturing. Medwed et al. [17] describe the system to provide self-monitoring for IoT devices to increase their cyber resilience. Rahman et al. [18] developed an index of cyber resilience for the additive manufacturing supply chain, while Durling et al. [19] analyzed the cyber threats to additive manufacturing system security.

2.3 AD for Systems Design in Manufacturing

AD is a methodology used for systems engineering and the design of complex systems. The main pillars of AD are Suh's axioms [2]: (i) maintain the independence of the FRs and (ii) minimize the information content. The central idea of the AD is to concentrate on FRs and remain solution neutral, meaning openness for all possible solutions and technologies, rather than proposing modifications for existing solutions. The main problem (customer need) is translated in a technical language in form of a functional requirement and decomposed into multi-level FRs and corresponding design guidelines as DPs are found. The design matrix connects FR vectors with associated DP vectors (Eq. 2) [20]. Whereby, FRs must be collectively exhaustive with respect to a higher level and mutually exclusive at the same level (having no overlapping nor redundancy). The goal is to reach uncoupled or at least decoupled design matrixes. In the uncoupled matrix, the DPs are independent of each other and provide more freedom. Coupled matrixes must be avoided. Decoupled matrixes are allowed, but the implementation of design guidelines needs to follow a certain sequence in this case. The design matrix can be described as follows:

$$\{FRs\} = [A]\{DPs\} \tag{2}$$

where FRs are functional requirements, DPs are design parameters and A indicates the effect of changes of the DPs on the FRs.

Cochran et al. [21] used AD and a lean approach in manufacturing system design decomposition and provided design guidelines that are suitable for a wide variety of manufacturing systems. Later, the lean approach was extended with a sustainability view [22]. Matt et al. [23] proposed DPs for the design of scalable modular manufacturing systems. In addition, the specific parts of manufacturing systems have been studied more deeply using AD approach. Vickery et al. [24] focused on smart data analytics in manufacturing SMEs. Manufacturing systems design studies in AD approach mainly consider productivity and neglect the importance of long-term resilience. No AD approach for resilience and especially for cybersecurity requirements decomposition in manufacturing was found in the literature.

3 Resilient CPPS Design Decomposition for Cybersecurity

To increase resilience in manufacturing, the AD methodology was used to derive conceptual DPs for CPPS planning. FRs, FRs metrics and corresponding DPs were mapped. Design matrices were used to check DPs independency. POC resilience metric was used as a support for the highest-level DP decomposition. The decomposition was finalized in three upper levels. From the fourth level, only minimizing the cost caused by cyberattacks was investigated in this work.

3.1 First Three Levels Decomposition of Resilient CPPS

As during last years, manufacturing companies have suffered due to the hectic external environment, the long-term performance measure resilience was taken into focus as a customer need. According to customer need, FR0 as the highest-level functional requirement was defined as “Increase the resilience in CPPS” (Fig. 1). The metric POC was selected for measuring the goal as it considers the strong booster - economic impact of disruptions and related changes. The second reason was the practical usability of the metric. DP0 as the highest-level DP was thus defined “Resilient manufacturing system”.

Considering the POC components (probability of the potential change to occur and penalty/cost of the potential change), the first level FRs were defined similarly (minimize the need for changes and minimize the cost of change caused by disruptions). From a manufacturing perspective, the cost (time) of change is influenced by preparedness for potential changes and their on-time discovery. Preparation means the ability for rapid and anticipated changes. The probability component is related to minimizing the occurrence of disruptions or even avoidance of them. Therefore, the first level parameters were found avoidance (DP1) and preparedness (DP2) for disruptions and their caused changes. In theory, if bringing one of these two components to zero, the other component could be neglected to observe. In practice, it is not possible to completely control the inputs to the system nor be aware of all possible changes a disruption can cause.

In the second level, both branches were divided between internal and external disruptions as they have different behavior. Internal disruptions are more predictable, and their occurrence is highly influenceable, while the causes of external disruptions are often out of manufacturers’ reach. Thus, to avoidance of disruptions occurrence, there is a need for responsible (DP1.1) and quality manufacturing (DP1.2). For preparedness, the most influenceable external (DP2.1) and most influenceable internal disruptions (machine faults) (DP2.2) must be considered. As the range of possible disruptions is not limited, focusing on the most influenceable ones provides the best results.

In the third level, focusing on the specific system modules takes place. From this level, we continue only with FR to minimize the cost caused by cyberattacks.

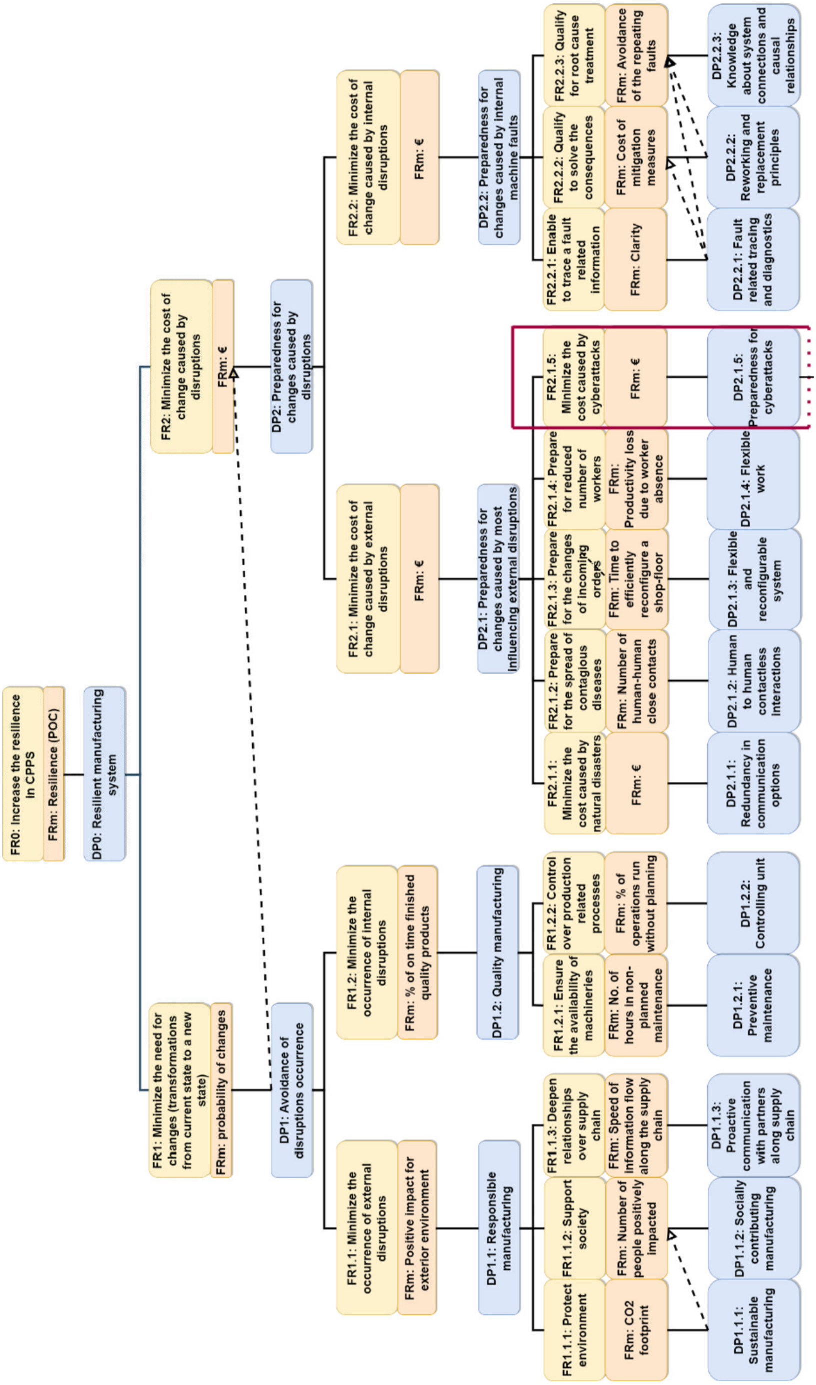


Fig. 1. Main branches of the design decomposition of resilient manufacturing systems.

3.2 Cybersecurity Decomposition

Recently, virtual networks have become one of the most vulnerable systems of the company. Protecting them against external disruptions (attacks) is more complex compared with physical resources. To minimize the cost caused by potential cyberattacks, preparation is essential. Most of the cybersecurity mitigation measures must be executed before the attack to minimize the spatial and temporal reach of the attack. This allows for minimizing the cost of changes for virtual networks and entities in these networks. Cybersecurity branch decomposition provides DPs to execute the preparation measures for virtual networks (Fig. 2).

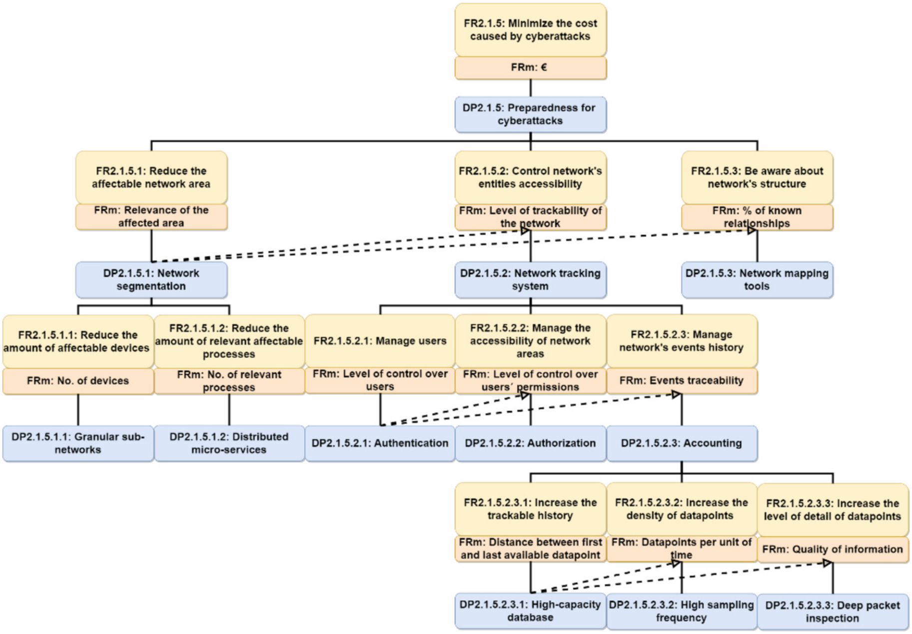


Fig. 2. Decomposition of the cybersecurity branch.

Preparedness for Cyberattacks. Preparedness and mitigation measures for cyberattacks consist of three main components: minimizing the reach of an attack, controlling the accessibility to the network, and maintaining the knowledge of the Full network structure. Network Segmentation (DP2.1.5.1) stands for dividing the network into smaller parts to limit the dimension of consequences of unauthorized access. The network tracking system (DP2.1.5.2) enables tracking suspicious events, related parties, and data packages sent and received. Network mapping tools (DP2.1.5.3) help to remain an awareness of large network structures and their relationships. Network segmentation is the prior activity for network mapping and enabling Full network control as it defines the structure of the network. Therefore, the DPs are partly decoupled (Eq. 3).

$$\begin{Bmatrix} \text{FR2.1.5.1} \\ \text{FR2.1.5.2} \\ \text{FR2.1.5.3} \end{Bmatrix} = \begin{vmatrix} \text{X} & 0 & 0 \\ \text{X} & \text{X} & 0 \\ \text{X} & 0 & \text{X} \end{vmatrix} \begin{Bmatrix} \text{DP2.1.5.1} \\ \text{DP2.1.5.2} \\ \text{DP2.1.5.3} \end{Bmatrix} \tag{3}$$

Network Segmentation. Segmentation can be realized for network entities (devices and machinery) and processes executed in the network. The network segmentation for its entities forms password-protected granular sub-networks (DP2.1.5.1.1) to reduce affectable devices in case of cyberattacks. It enables continued manufacturing of devices in other segments. Segmentation areas can be compared with physical spaces (shop floors). If one of the spaces is physically attacked, it does not affect the condition of the other spaces. In the same way for processes, distributed micro-services (DP2.1.5.1.2) allow controlling only small particles of the operations. In this way, unauthorized access can only receive limited control over the process. Granular sub-networks and distributed micro-services design matrix is uncoupled (Eq. 4).

$$\begin{Bmatrix} FR2.1.5.1.1 \\ FR2.1.5.1.2 \end{Bmatrix} = \begin{vmatrix} X & 0 \\ 0 & X \end{vmatrix} \begin{Bmatrix} DP2.1.5.1.1 \\ DP2.1.5.1.2 \end{Bmatrix} \tag{4}$$

Network Tracking System. The network tracking system's purpose is to control user rights and monitor network traffic. The users can be managed through the authentication process that controls access to the network. Authentication can be realized by using methods such as username and password combination checks, token cards, and challenges with response questions. Authorization services determine which network resources the user can access and which operations the user is allowed to perform. Accounting stands for monitoring of network traffic. Thus, it tracks who and how the network resources are used. It Records the access time and changes made in the network. The prior process is the user's authentication to enable authorization and accounting, therefore the DPs are partly decoupled (Eq. 5).

$$\begin{Bmatrix} FR2.1.5.2.1 \\ FR2.1.5.2.2 \\ FR2.1.5.2.3 \end{Bmatrix} = \begin{vmatrix} X & O & 0 \\ X & X & 0 \\ X & 0 & X \end{vmatrix} \begin{Bmatrix} DP2.1.5.2.1 \\ DP2.1.5.2.2 \\ DP2.1.5.2.3 \end{Bmatrix} \tag{5}$$

Accounting. From the network traffic monitoring perspective, the characteristics are the length of historical traffic data (DP2.1.5.2.3.1), the density of data points (DP2.1.5.2.3.2), and the completeness of the data that is recorded (DP2.1.5.2.3.3). Historical data of the traffic is beneficial to preserve as a new more advanced type of scanning method may disclose old attacks that were undiscovered. In the first phase, the threat actor establishes access to the system, gathers the data and may search for options for expanding its access area. The culmination of any attacks often arrives in later phases such as encryption of the data to request a ransom. Therefore, a high-capacity database is a prerequisite for high sampling frequency and deep packet inspection, which outcomes in the partly decoupled relationship between sixth-level DPs (Eq. 6). Sampling frequency becomes important if the collected data is not event log based, but real-time monitored. Different network monitoring tools provide packet inspection at various scales. Some tools provide only access time, the accessed user, visitors' IP address, and the type of transferred data. In a network monitoring system, there could be distinguished various data modules such as network traffic, network flows, system logs, endpoint data, threat intelligence feed, security events, etc. Deep packet inspection enables the identification of exact data packets that were transferred and provides access to their content.

$$\begin{Bmatrix} FR2.1.5.2.3.1 \\ FR2.1.5.2.3.2 \\ FR2.1.5.2.3.3 \end{Bmatrix} = \begin{vmatrix} X & 0 & 0 \\ X & X & 0 \\ X & 0 & X \end{vmatrix} \begin{Bmatrix} DP2.1.5.2.3.1 \\ DP2.1.5.2.3.2 \\ DP2.1.5.2.3.3 \end{Bmatrix} \tag{6}$$

4 Application Use Case: Cyberattacks Prevention Solutions for Cyber-Physical Demonstrator

According to AD-based decomposition of minimizing the cost caused by cyberattacks in resilient CPPS, the conceptual DPs were found in Sect. 3. Based on the conceptual DPs the physical and virtual solutions (Table 1) were found for the cyber-physical demonstrator in the learning factory 'Smart Mini Factory' at the Free University of Bozen-Bolzano.

The demonstrator consists of the following physical entities (see Fig. 3): a Montrac transfer line with three shuttles for transportation; a warehouse rack; a Universal Robot UR10 collaborative robotic arm for loading components and products from the warehouse to shuttles and manual workstation; a 3D-printer; a manual workstation with digital assistance system; and an Omron Adept Quattro fixed robot for servicing the 3D-printer. All the entities have IoT functionality which allows them to communicate with each other through the uniform communication system. Input for decision support system is provided by other virtual network entities: enterprise resource planning system, database, analytics, and simulation. The human worker in the manual workstation is in the loop of a production process. Nevertheless, manual workstation servicing processes will be executed automatically (servicing with physical components and providing step-by-step digital work instructions). The transfer line allows to the addition of up to seven workstations, which makes the demonstrator extendable.

4.1 Network Segmentation

Network segmentation's aim is to limit the potentially harmed area in the network if a threat actor should get access to the system. It can be limited by separating connected devices by the creation of multiple access-protected networks. One option to establish it is to use several gateways to physically separate the networks. Virtual segmentation allows using a single gateway that separates the gateway-connected devices into separate networks. For the demonstrator, the Endian 4i Edge X gateway was selected that supports virtual segmentation.

The second option for limiting the access area is limiting the reach of the machine-related processes. It could be implemented by dividing the services that field level entities provide into smaller parts. In this way, a threat actor cannot take over the full macro-services. For instance, the macro-service "Bring the finished products from the work

Table 1. The physical and virtual solutions for minimizing the cost caused by cyberattacks.

Design parameters area	Conceptual design parameter	Physical/virtual solution
Network segmentation	Granular subnetworks	Endian 4i Edge X gateway network segmentation module
	Distributed microservices	Recognized functions of field level entities
Network tracking	Authentication	Endian server Switchboard (multi-factor authentication and authorization)
	Authorization	
	High-capacity database	Relational SQL database
	High sampling frequency	Endian intrusion detection system
	Deep packet inspection	
Network mapping	Network mapping tool	Endian Network Awareness application

station (WS) to the warehouse" can be divided into multiple micro-services such as "Check available bins in the warehouse", "Select and book the bin in the warehouse", "Choose the optimal transportation unit", "Bring the transportation unit to the WS", "Pick the finished products from the WS", "Place the products on the transportation unit", "Choose the optimal path to the warehouse", etc. Micro-services can be realized due to frequent communication between Python script supported IoT devices and decision support system.

4.2 Network Tracking System

Remote access to the network, provided by Endian switchboard (server), is authenticated by username and password. Additionally, device type recognition can be added for authorization. The switchboard also provides permission management based on users and device types. Therefore, different users can access previously defined areas only. It provides access to the network, data aggregation and customizable dashboards for data visualization.

High-capacity database, high sampling frequency, and deep packet inspection provide additional functionality to support network tracking and accounting. A relational SQL database will be used to store network tracking data. Traditional hard drive or solid-state drive hosted databases such as PostgreSQL and SQLite are preferred over "in-cache" database such as Redis.

Zero-trust architecture for remote networks is complemented with intrusion detection system. Intrusion detection system is seen as a sensor, that detects abnormal activities in network. It works based on rules that trigger security alerts. It covers the function deep packet inspection in real-time traffic monitoring and inspection. The data acquisition frequency is based on events occurrence frequency in the network. Therefore, in this case, intrusion detection system also covers high sampling frequency function. The selected solution is Endian intrusion detection system as it connects smoothly with the system. For instance, the system provides transmission control protocol window scaling, support for untagged virtual local area network traffic, bonding mode configuration in the web user interface, and support for dynamic host configuration protocol relay. Alternative software options for deep packet inspection are network protocol analyzer Wireshark and data-network packet analyzer tcpdump.

4.3 Network Mapping

Network mapping is the visual representation of the connectivity between interconnected devices. It facilitates network connectivity management and enables to detection of all connected devices. It provides maintenance for IT infrastructure.

For network mapping, the Endian Network Awareness application with graphical user interface was selected. It provides real-time network bandwidth information with top applications in use on the network, identification of top network activities and flows (for eliminate devices or applications creating bottlenecks and enables to see historical network mapping history. The alternative non-Endian options could be Nmap, Libre NMS and NetworkMaps.

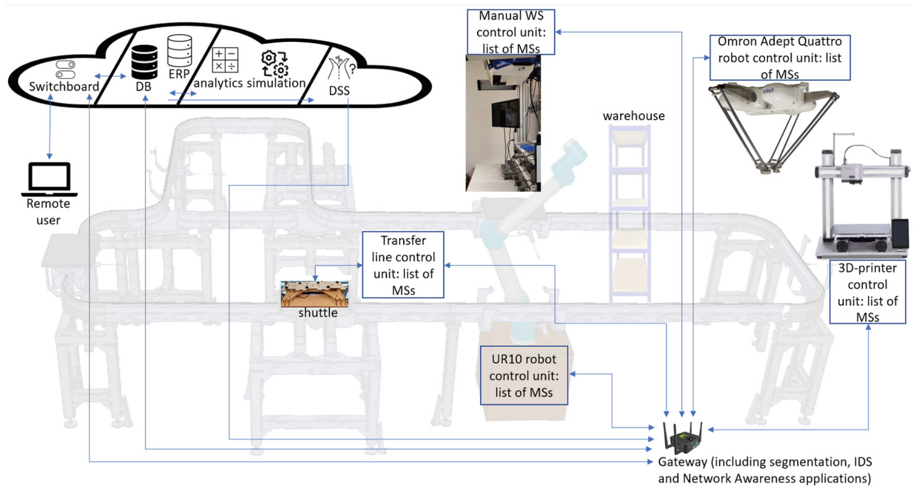


Fig. 3. Application of design guidelines in a cyber-physical demonstrator. DB – database, ERP – enterprise resource planning, DSS – decision support system, WS – workstation, UR – Universal Robot, MSs – microservices, IDS – intrusion detection system.

5 Discussion

AD theory was applied to increase the level of resilience in CPPS. The conceptual DPs of cybersecurity functions for preparedness for potential cyberattacks were derived. The DPs were applied to the Industrial Internet of Things and digital twin supported cyber-physical demonstrator. Based on this, physical and virtual solutions for the demonstrator were found.

The provided concept DPs have practical value not only for CPPS but also for traditional manufacturing systems that use virtual networks in their processes. The derived parameters facilitate in the planning phase of manufacturing system networks to increase their long-term resiliency. This study filled the gap in the solution-neutral design of cyber resiliency in manufacturing companies.

The current research focused on preparedness for disruptions in cyberattacks aspect. The other side of cyber resiliency is minimization and avoidance of the occurrence of the attack which needs further research. Additionally, the other branches (Fig. 1) need further decomposition to derive specific concept DPs from the CPPS resilience perspective.

Acknowledgment. This project has received funding from the Autonomous Province of Bozen/Bolzano, Department Innovation, research, universities and museums (ASSIST4RESILIENCE: Increasing Resilience in Manufacturing - Development of a Digital Twin Based Worker Assistance).

References

1. Mohammed, A.S., Reinecke, P., Burnap, P., Rana, O., Anthi, E.: Cybersecurity challenges in the offshore oil and gas industry: an industrial cyber-physical systems (ICPS) perspective. ACM Trans. Cyber-Phys. Syst. **6**(3), 1–27 (2022)
2. Suh, N.P.: The principles of design. Oxford Univ. Press, New York (1990)
3. Gu, X., Jin, X., Ni, J., Koren, Y.: Manufacturing system design for resilience. Procedia CIRP **36**, 135–140 (2015)
4. Tran, H.T., Balchanos, M., Domerçant, J.C., Mavris, D.N.: A framework for the quantitative assessment of performance-based system resilience. Reliab. Eng. Syst. Saf. **158**, 73–84 (2017)
5. Aruväli, T., De Marchi, M., Rauch, E.: Analysis of quantitative metrics for assessing resilience of human-centered CPPS workstations. Sci. Rep. **13**(1), 2914 (2023)
6. Alexopoulos, K., Anagiannis, I., Nikolakis, N., Chryssolouris, G.: A quantitative approach to resilience in manufacturing systems. Int. J. Prod. Res. **60**(24), 7178–7193 (2022)
7. Chryssolouris, G.: Manufacturing Systems Theory and Practice, 2nd edn. Springer-Verlag, New York (2006)
8. Chryssolouris, G., Lee, M.: An assessment of flexibility in manufacturing systems. Manuf. Rev. **5**(2), 105–116 (1992)
9. Jin, X., Gu, X.: Option-based design for resilient manufacturing systems. IFAC-PapersOnLine **49**, 1602–1607 (2016)
10. Murino, G., Armando, A., Tacchella, A.: Resilience of cyber-physical systems: an experimental appraisal of quantitative measures. In: 2019 11th International Conference on Cyber Conflict (CyCon) vol. 900, pp. 1–19 (2019)
11. Okorie, O., et al.: Manufacturing in the time of covid-19: an assessment of barriers and enablers. IEEE Eng. Manage. Rev. **48**, 167–175 (2020)

12. Palo Alto Networks Blog https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/. Accessed 12 Jan 2023
13. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. & McQuaid, R.: Developing cyber-resilient systems: a systems security engineering approach. In: No. NIST Special Publication (SP) 800–160, vol. 2 (Draft), Natl. Inst. Stan Technol. (2021)
14. Haque, M. A., Shetty, S., Krishnappa, B.: Cyber-physical system resilience. In: Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy, p. 12301 (2019)
15. Beteto, A., et al.: Anomaly and cyber fraud detection in pipelines and supply chains for liquid fuels. Environ. Syst. Decisions **42**, 306–324 (2022)
16. Ghiasi, M. et al.: A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future. Electr. Power Syst. Res. 215, (2023)
17. Medwed, M., Nikov, V., Renes, J., Schneider, T., Veshchikov, N.: Cyber resilience for self-monitoring IoT devices. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 160–167 (2021)
18. Rahman, S., Hossain, N.U.I., Govindan, K., Nur, F., Bappy, M.: Assessing cyber resilience of additive manufacturing supply chain leveraging data fusion technique: a model to generate cyber resilience index of a supply chain. CIRP J. Manuf. Sci. Technol. **35**, 911–928 (2021)
19. Durling, M. R. et al.: Model-based security analysis in additive manufacturing systems. In: Proceedings of the 2022 ACM CCS Workshop on Additive Manufacturing (3D Printing) Security, pp. 3–13 (2022)
20. Cosmin, R., Stavarache, Ermolai, V., Irimia, A. & Etcu, M.: Using axiomatic design principles for the development of a device to measure the positioning error of an industrial robot. In: IOP Conference Series: Materials Science and Engineering. vol. 1174(1), p. 012018, IOP Publishing (2021)
21. Cochran, D.S., Arinez, J.F., Duda, J.W., Linck, J.: A decomposition approach for manufacturing system design. J. Manuf. Syst. **20**, 371–389 (2001)
22. Cochran, D. S., Hendricks, S., Barnes, J. & Bi, Z.: Extension of manufacturing system design decomposition to implement manufacturing systems that are sustainable. J Manufact. Sci. Eng. Trans. the ASME **138**(10), (2016)
23. Matt, D.T., Rauch, E.: Design of a network of scalable modular manufacturing systems to support geographically distributed production of mass customized goods. Procedia CIRP **12**, 438–443 (2013)
24. Vickery, A. R., Rauch, E., Rojas, R. A., Brown, C. A.: Smart data analytics in SME manufacturing – an axiomatic design based conceptual framework. In: MATEC Web Conferences, vol. 301, pp. 1–11 (2019)

Smart Mobile Factory Design Decomposition Using Model-Based Systems Engineering

Ali Asghar Bataleblu(✉), Erwin Rauch, Andrea Revolti, and Patrick Dallasega

Industrial Engineering and Automation (IEA), Faculty of Engineering, Free University of Bolzano-Bozen, Bolzano, Italy
Aliasghar.Bataleblu@unibz.it

Abstract. Nowadays, providing an automatic agile process in the design processes relying on Model-Based Systems Engineering (MBSE) to speed up innovation creation as much as possible is a progress key as well as a survival factor in the competitive industrial environment. Therefore, companies should make a cultural shift from traditional document-based information exchange and iterative time-consuming serial design procedures, to communicate the information based on visual modeling in a common language such as SysML, which is easier to follow. In this respect, although the capability of Axiomatic Design (AD) in product work breakdown structure has been proven, from stakeholders' needs to functional requirements and physical solutions, it seems that now is the time to automate and speed up this critical process in the product life cycle practically using developed MBSE tools. That means, when changes occur, updating a model is more straightforward than documents that require manual revisions of tables, glossaries, requirements, etc. To show the application of such a work, this paper proposes the AD of a smart mobile Hyperloop transportation factory through requirements modeling and analysis in the Cameo System Modeler software. As the main goal of the project is the decentralization of producing tube elements, and easily disassembling and building up again along the planned track/construction side, the AD is focused on the mobile factory than the Hyperloop system. Results illustrate how MBSE could alleviate difficulties in dealing with AD problems in real-world complex applications with lots of requirements.

Keywords: Model-Based Systems Engineering · Cameo System Modeler · Axiomatic Design · Smart Mobile Factory · Hyperloop Transport System

1 Introduction

The main idea of Smart Mobile Factories (SMFs) relied on industries that could operate in remote areas with limited logistical capabilities. Using SMFs and operating locally can gain competitive advantages by reducing logistics efforts and costs while improving operational efficiency. As SMFs can install, implement, and disassemble in nearby operational platforms, parts can be produced directly wherever the need arises without having to wait for them to arrive from a supplier or central storage. Overall, a wealth

E. Puik et al. (Eds.): ICAD 2023, LNNS 849, pp. 15–25, 2024.
https://doi.org/10.1007/978-3-031-49920-3_2

of potential applications considering sustainability factors can be provided through the SMFs. A systematic literature review on modular and mobile facility location problems is done by Eduardo and Udo in [1]. According to [1], to provide a more efficient response to today's markets, more flexible networks have to be proposed by addressing the inclusion of modular units to consider fully mobile units. As the situation of flexibility in factories' planning horizon shows (see Fig. 1), flexibility directly depends on the degree of mobility [2]. After the idea of "factory in a box" as a solution to move toward SMFs (i.e., manufacturing small-scale components in a container, see Fig. 2), now it is time for emerging concepts for the additive manufacturing of prefabricated parts made of concrete or other materials for real-world industrial applications [3, 4].

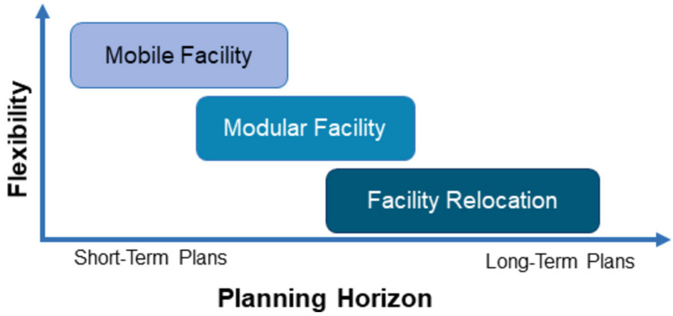


Fig. 1. Flexibility in factories' planning horizon [1]

Fig. 2. Factory in a box as a solution for SMFs [4]

In recent years, pandemic problems such as the COVID-19 crisis remarkably revealed supply chain vulnerabilities. The manufacturing industry strongly persists in promoting the expectations of previous years and a strong trend toward intelligent reindustrialization and local production can be seen these days. More and more companies are striving to alleviate supply chain difficulties due to geographically distant suppliers through SMFs [4]. At the same time, significant attention to the systems engineering field relying on a system thinking mindset will speed up systems design in a product lifecycle and it is expected to increase productivity through efficiency gains and thus gradually reduce the gap between design and manufacturing.

This research aims to illustrate how Model-Based Systems Engineering (MBSE) tools like Catia Magic can be used to decompose the functional requirements of complex systems. Therefore, producing infrastructure elements of the Hyperloop Transportation System (HTS) as an SMF is proposed.

In the following, first, a brief overview of the SMF of the HTS project at the Free University of Bozen-Bolzano is presented. Then, the problem definition and formulation as an Axiomatic Design (AD) are introduced in the next section. After that, the application of the Cameo Systems Modeler as part of Catia Magic in the automation of the AD process and related results are highlighted and proposed. The final section provides the conclusions of this research.

2 Mobile Smart Factory for Hyperloop Construction

The Hyperloop concept was born in 2013 when tech entrepreneur Elon Musk published a white paper on the subject [5] that focused on environmentally friendly goods and passenger transport. The Hyperloop's propulsion system is generated by a linear electric motor powered by renewable energy sources. Magnetic levitation is eco-friendly, consumes less energy, and causes no emissions. Eurotube Foundation [6] a non-profit research institution from Switzerland has developed a patent that envisages building the tube infrastructure using concrete instead of metal alloys. Within the joint research project Smart Mobile Factory for Infrastructure Projects (SMF4INFRA) between the Eidgenössische Technische Hochschule Zürich (ETH Zürich) and the Free University of Bozen-Bolzano, a prototype for a smart mobile factory to deliver material for the construction of hyperloop infrastructure is developed. Using a mobile factory in a linear construction site, with wide-ranging routes, allows for erecting the infrastructure sustainably. Moving the production factory of the individual pipe components while remaining close to the construction site's progression helps guarantee economic and ecological sustainability. Within the SMF4INFRA project, the physical mobile factory will be designed (Fig. 3) and its Digital Twin will be developed to ensure environmental sustainability during the construction of the hyperloop infrastructure project.

3 Axiomatic Design Decomposition

Axiomatic Design (AD) was developed by Nam P. Suh in the mid-1970s in the pursuit of developing a scientific, generalized, codified, and systematic procedure for design. AD uses the following four domains:

1) The customer domain where the customer wishes are described as so-called customer needs (CNs);
2) The functional domain where CNs are translated into functional requirements (FRs) as well as design constraints (Cs);
3) The physical domain where physical solutions (PSs) (or design parameters (DPs)) are derived that meet the previously defined functional requirements and

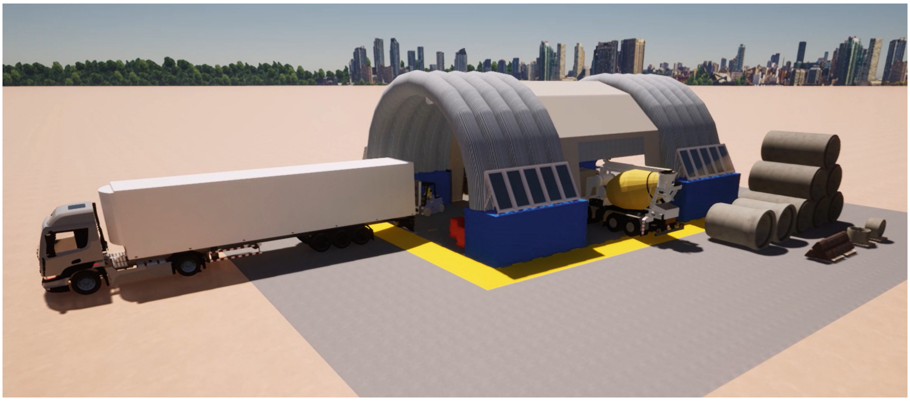


Fig. 3. First concept of the Smart Mobile Factory for Hyperloop construction

4) The process domain, where the DPs are transformed into real process variables (PVs).

The scientific theory gets its name from two axioms in AD that must be respected [7].

- The first is the Independence Axiom: Maintain the independence of the functional elements, i.e., avoid coupling in the system (e.g., avoiding dependencies between the DPs and other FRs).
- The second is the Information Axiom: Minimize the information content: select the solution with the least information content, i.e., that has the highest probability of success.

To apply these axioms, parallel functional and physical hierarchies are constructed, the latter containing the physical design solutions. The benefit of AD is that the designer learns how to construct large design hierarchies quickly that are more structured, thus freeing more time for mastering applications [8].

In the initial workshop on AD at Smart Mini Factory Lab. at Unibz, requirements and so-called CAs of the SMF4INFRA project were collected. Based on these inputs, FRs and Cs are defined and design parameters for a redesign were derived in an AD top-down decomposition and mapping process. The AD steps that have been carried out are as follows:

Step 1: Problem Formulation.
Step 2: Elaborate use cases into steps.
Step 3: Identify customer needs.
Step 4: Translate Needs and Use Case Steps to FRs and FRms.
Step 5: Generate Physical Solutions alternatives.
Step 6: Design decomposition – choose PS to achieve FR.

Figure 4 presents the result of these six steps for decomposing the design of a smart mobile factory for hyperloop infrastructure into 4 levels (Level 0 to Level 3). The design team has checked the independence axiom using the design matrix for each level to achieve an uncoupled or at least decoupled design.

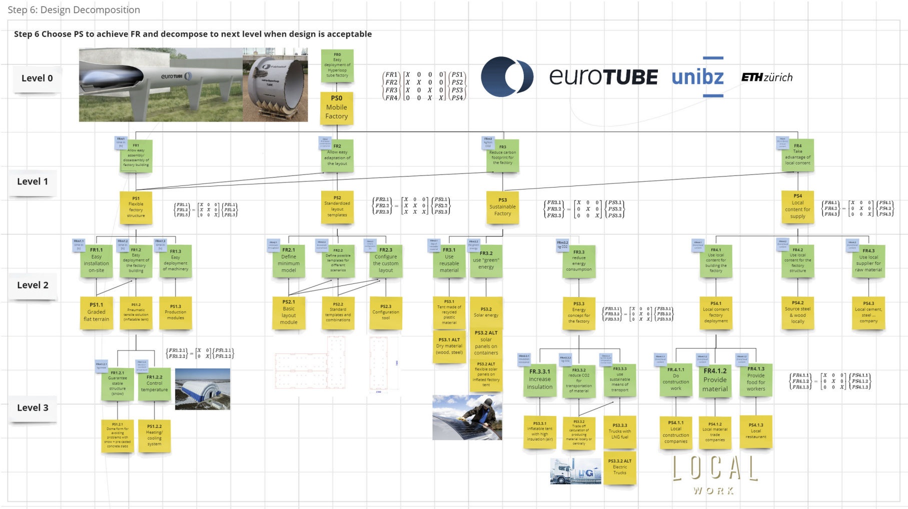


Fig. 4. Overview of the Axiomatic Design based decomposition of FR and PS

4 Model-Based Systems Engineering (MBSE) Using Catia Magic

Model-based systems engineering tools like Cameo System Modeler (developed by No Magic Inc. Which was purchased by Dassault Systems company in 2018 and is now part of Catia Magic) are suitable solutions for software architectures and operational processes. Requirement management is one of the features of this tool which provides capabilities as follows for users (see Fig. 5) [9]:

- Creating requirements
- Importing text-based requirements
- Requirements decomposition
- Requirements numbering
- Requirements gap and coverage analysis
- Tracing requirement changes in Teamwork Cloud
- Requirements verification
- Visualize and analyze.

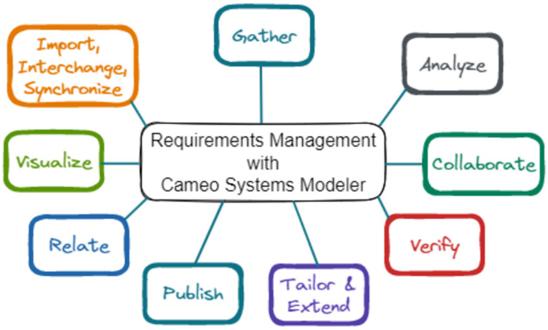


Fig. 5. The main features of Cameo Requirements Management [9]

Requirements can easily be visualized through the Requirement Diagram and Requirements Table by creating and importing them into the modeling tool. But before diving into the requirements, the structure of the problem can be modeled with blocks which here SysML Block Definition Diagram (BDD) plays an important role in this software. Using this part, you can see the problem's overall work breakdown structure and decide on decomposition and interaction between different blocks. In other words, system hierarchy from system to sub-systems and the specification of software, hardware, or human elements can be represented by blocks [9]. Figure 6 illustrates the SMF structure of the Hyperloop system using BDD, which comprises two Work Packages (WPs): the physical factory and its Digital Twin (DT).

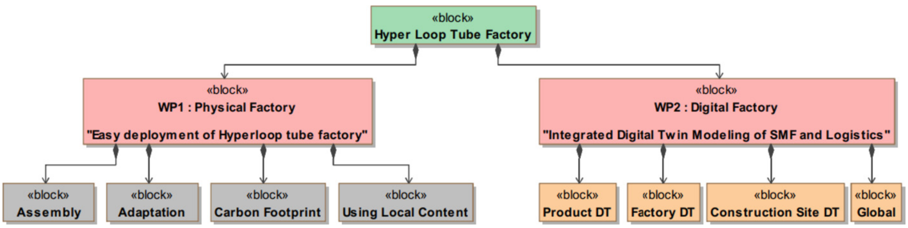
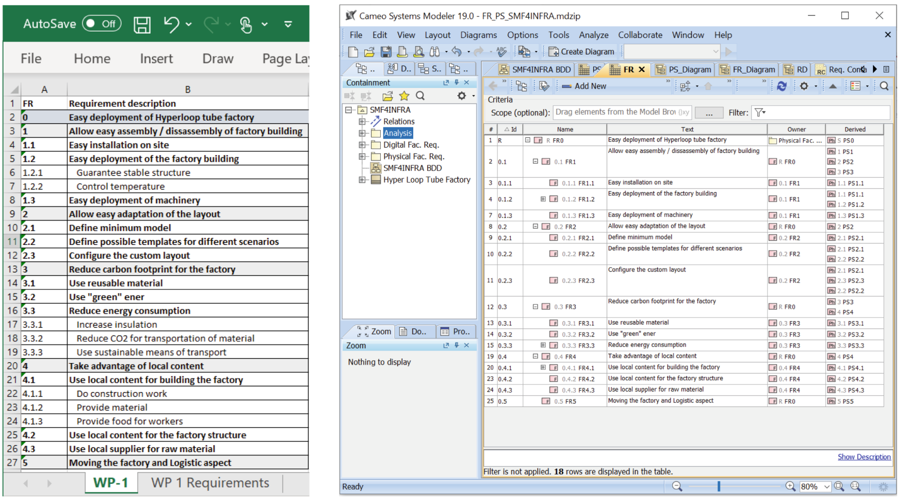


Fig. 6. The structure of the SMF of the Hyperloop project in the BDD

After creating the work breakdown structure of the problem from the system to the subsystem level, it is time to import predetermined FRs and PSs from Excel sheets to the Cameo software. This process can be done from the beginning in the software. However, importing and exporting requirements with different text-related software using Cameo is an advantage. All requirements can be easily updated in tables and diagrams just by copying and pasting them into the requirements table by a predetermined template. Figure 7 illustrates the FRs table based on related Excel sheet requirements. The requirement Diagrams are a valuable tool to provide a bridge between traditional requirement management tools and other SysML models. They are for demonstrating traceability from the requirements to the elements that are dependent on them. The FRs and PSs diagrams are represented in Fig. 8.

Such modeling can be done for PSs and finally, the relation between FRs and PSs can be shown and checked by providing a diagram including both (Fig. 9). One of the advantages of a requirements diagram like Fig. 9 is that the user can create any FRs and PSs and just link them together and by updating the software, the changes can be saved in other tables that could be exported for other usages.

We can use the Requirement Containment Map (RCM) and Requirement Derivation Map (RDM) to review, analyze, and decompose the Requirements. In these decompositions as trees, the RDM displays the decomposition of requirements related to the derived relationship. Figures 10 and 11 show the RDM and RCM of the SMF of the Hyperloop infrastructure project respectively. The user can determine the level/depth of decomposition to display results.



Requirements Excel Sheet *Cameo Requirements Table*

Fig. 7. The FRs table in Cameo

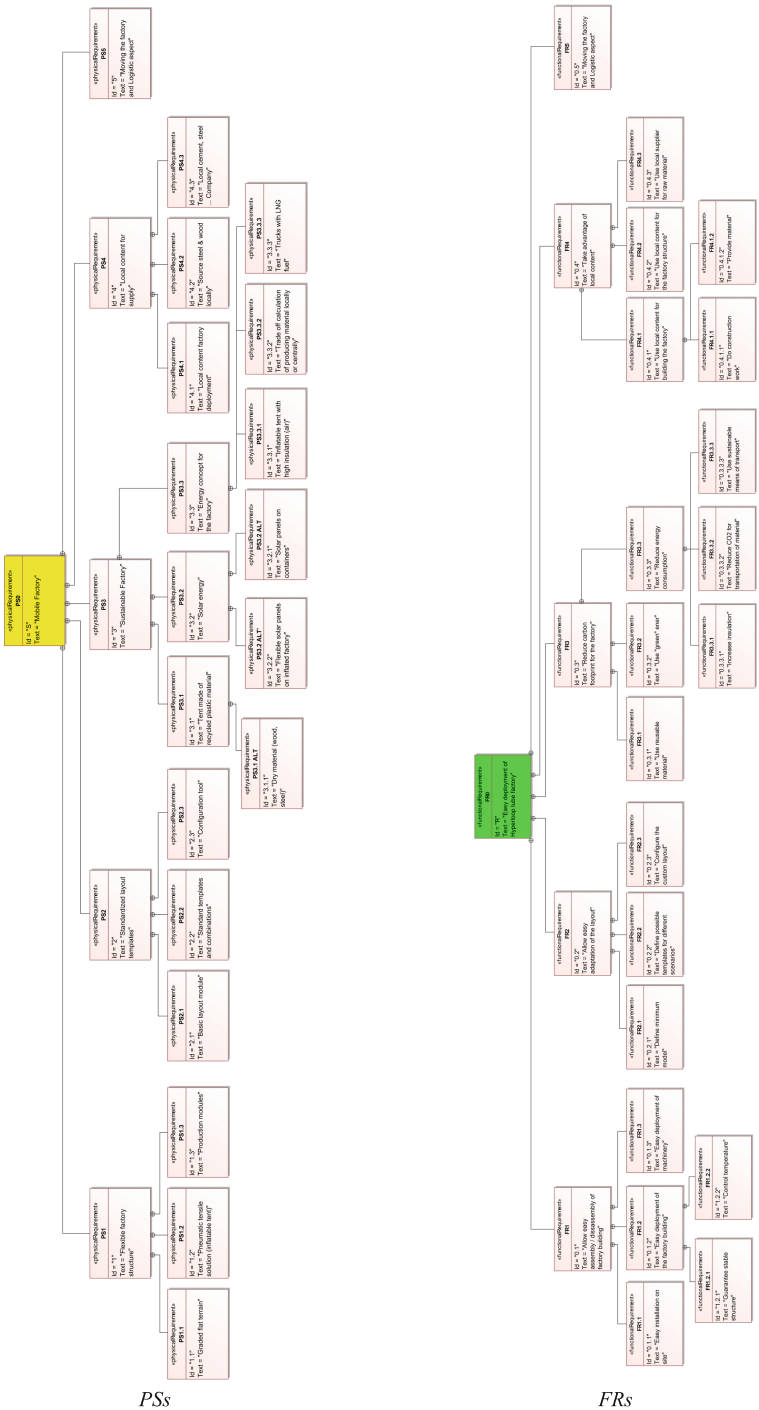


Fig. 8. The FRs and PSs diagrams in Cameo