# IT-Security Risk Based Approach for Secure Operation of Distributed Data Platforms in Supply Chains

Marvin Voß[1], Jonas Kallisch[2], Maxim Runge[1], Tobias Theus[3], Karl-Heinz Niemann[1], Christoph Wunck[2]

[1]Faculty I - Electrical Engineering and Information Technology, University of Applied Sciences and Arts, Hannover, Germany

[2]Department of Engineering Section Electrical Engineering and Computer Science, University of Applied Sciences, Emden/Leer, Germany

[3]Faculty of Mathematics, Informatics and Statistics, Ludwig Maximilian University, Munich, Germany

(marvin.voss@hs-hannover.de; jonas.kallisch@hs-emden-leer.de; maxim.runge@hs-hannover.de; t.theus@campus.lmu.de; karl-heinz.niemann@hs-hannover.de{https://orcid.org/0000-0001-8931-6789}; christoph.wunck@hs-emden-leer.de)

*Abstract* - **This research paper examines the topic of secure data exchange in a supply chain within the manufacturing sector. The objective is the development of a data platform that optimizes operational efficiency and promotes cross-company collaboration. To achieve this, helpful tools are utilized and suitable standards are followed to create a secure system. Security measures are determined by conducting a risk analysis to identify, evaluate, and compensate for potential threats. Furthermore, the utilization of non-transparent federated learning models in combination with a method of security design of components contributes to the information sovereignty of data owners. In conclusion, secure data sharing practices play a pivotal role in supporting collaboration and operational effectiveness in the manufacturing industry.**

*Keywords* - **Supply chain security, supply chain risk analysis, confederated learning, OT security**

## I. INTRODUCTION

The exchange of data between companies is a regular part of many processes along their supply chains. [1] Many companies are using the cross-company data exchange to improve the efficiency of processing orders, invoicing or for solving logistical challenges between each other. However, the exchange is usually limited to the management level of the companies and therefore does not extend to the core processes of manufacturing companies, on their shop floor. [2] The reasons for this are manifold and depend on the industry and type of production system. Studies have shown that a common reason for not exchanging shop floor data is a lack of confidence in the security of the data exchange. Business leaders fear misuse or theft of intellectual property contained in the data provided. [3] A key barrier to sharing is the perceived or actual loss of sovereignty over the data. As the collaboration and the cross-company data analysis become some of the most important benefits in the future, companies need state-of-the-art solutions for inter-company data exchange.

One goal of the project Future Lab Manufacturing project was to identify methods and concepts for exchanging information between companies, without compromising their data sovereignty. Based on this goal, a data sovereignty concept was developed and a prototype was implemented. This approach differs from approaches used in many data ecosystems, such as GAIA-X [4] or Project-44 [5], which rely on exchanging data via an intermediary. In our approach, the direct exchange of information between the parties is based on vertical federated learning [6]. This approach gives the partners more sovereignty, but is associated with larger effort and potentially poorer analysis results.

In order to carry out a comprehensive analysis of the participants' data, the concept provides information models of each company dataset in an edge data platform and connects them via a connector platform [7]. No operational data needs to be exchanged within this connector platform. Instead only the models of the algorithms are transferred and updated after they have been trained on the individual datasets.

This gives companies sovereignty on their data, but allows them to benefit from cross-company data analyses. The concept therefore fulfils the requirements for a secure solution that preserves data sovereignty and may supported by direct data exchange between companies if required.

After first project work demonstrated, that the approach is able to solve this issue, the question come up, how the platform can be secured against cyber security threats. Therefore, this paper will analyse the architectures security aspects and provides a risk assessment of the platform design. Afterwards it will propose a set of measures that assure the security of the design.

## II. SECURITY ASPECTS OF DISTRIBUTED DATA ARCHITECTURES

This case in particular considers supply chain cooperation beyond company boundaries. This paper is limited only to the horizontal integration of production information transfer between the cooperating companies

DOI of the original publication: 10.1109/IEEM62345.2024.10857265

and not to the internal integration of data flow within the company. The increase of usage of digital technologies in supply chains leads to a higher demand on security in these systems. [8] Cyber incidents are the number one business risk worldwide, regardless of company size. Especially early detection and adequate preparation for serious cases are necessary to ensure a secure version of the supply chain. In addition, companies are currently looking to strengthen their business continuity management to ensure that essential functions can continue during and after a disaster or disruption. [9] Conversely, it is important that the design of a secure system should only lead to acceptable performance losses.

### *A. State of the Art of Hardening Cross-Company Data Platforms*

So far, there are limited state of the art solutions for implementing a distributed data platform, let alone for standardizing its security.

A closer look at various production companies reveals some obstacles to developing a consistent approach to a secure data platform. The IT infrastructures of these companies have a heterogeneous structure. This diversity makes creating and implementing an interface from the existing infrastructure to a data platform a challenge. [10]

Securing a shared data infrastructure to keep the sovereignty within heterogeneous IT environments requires a systematic approach to consider all relevant factors. This includes overcoming the complexity of multiple technological frameworks, interoperability issues, disparate security protocols, communication barriers and an expanded attack surface environment. The creation of a unified security standard requires careful planning and coordination of security measures to minimize vulnerabilities in advance and enable smooth collaboration between stakeholders. Depending on the individual architecture of the system, the preparation of a requirements analysis provides a suitable structure for the basic security of the system. This is followed by a risk analysis that is an essential component of many security strategies, as it identifies and evaluates potential threats. The systematic approach enables system integrators to select a suitable infrastructure approach and appropriate security features in order to rule out potential damage in advance. It can also help to consolidate stakeholder trust and improve resilience of the system to threats.

Therefore, the security of distributed data architectures is a common issue for companies. The fear of losing data when transferring sensitive information prevents many potential new entrants to shared supply chains from participating in the first place. [11] A secure data platform in this environment offers a number of advantages for companies that go beyond protecting against cyber-attacks. How can these benefits be used to strengthen the resilience of supply chains and ensure business continuity, as well as the optimal handling of production in cooperation at the same time?

### *B. Benefits of a Secure Cross-Company Data Platform*

Firstly, the data platform guarantees the protection of sensitive data, which should be established as the most important protection goal from the outset. It also has the advantage of strengthening user confidence in the system as a whole in order to develop a corresponding affinity for shared added value.

A technical monitored platform can also be scaled as needed to handle growing amounts of data and user requirements without compromising the security of the system. The use of a reliable protective framework of the system enables the company partners involved to work with reliable information, which is essential for new application features and the innovation of new ideas. This is the only way to make optimum use of the shared added value. It is important to point out that no security system can be considered completely invulnerable. Individual hardening techniques can sometimes be overcome with minimal effort. The remedy for this is a combination of many security features. The Defense in Depth principle combines a large number of security measures. [12] This means that in addition to the use of monitoring services features, a variety of other features are also required in combination in order to secure the system as well as possible.

### *C. Essential Elements for Achieving Key Protection Goals*

In order to create a suitable architecture for the data platform, which should be secure enough for this use case, all relevant security requirements are presented in the first step. The focus is on achieving the most important protection goals. These fundamental requirements include availability, integrity, authenticity and confidentiality. The requirements are explained using examples to illustrate their relevance.

- The availability ensures that the platform is accessible and operational at all times, which is essential for the operation of an uninterrupted supply chain.
- Integrity ensures the correctness of the data. It guarantees that data is protected against unauthorized changes.
- The confirmation that data and messages originate only from dedicated, verified sources is called authenticity. Ensuring the authenticity of shared information models in the supply chain is therefore of key importance.
- Finally, confidentiality protects sensitive information from unauthorized disclosure, e.g. product or other asset data. [13]

### C. Minimum Viable Product (MVP) for an Examination Model

The test object used here is based on a MVP, i.e. a system that contains the minimum set of functions necessary for system developers to represent its basic functionality. The focus here is on the security implementation. [14] The further security related issues will be used to optimize the system for a proposal of a proper version of the data platform.

In this project, the raw data from the shop floor is aggregated redundantly in the so-called edge data platform via a Kafka Connect [15] service. It should be noted that, in contrast to the more extensive system, the data connection between the technical process and the database of the edge data platform is not considered in this paper.

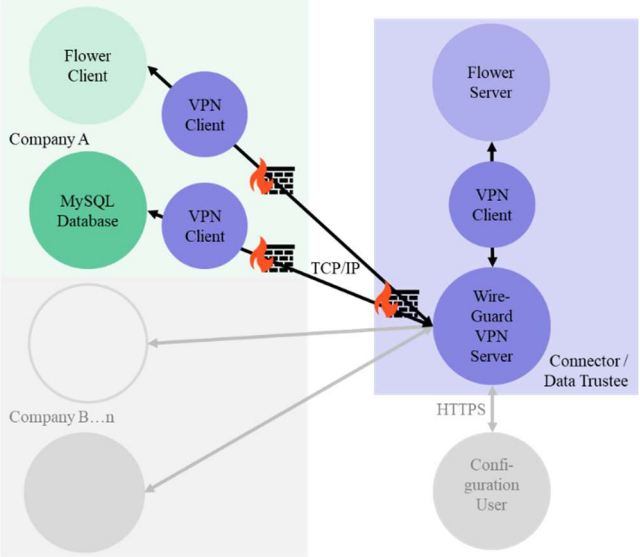


Fig. 1. Software architecture of the MVP for secure cross-company information exchange using machine learning.

Fig. 1 shows the topology of the used MVP. On the left side, all participating companies with their selection of microservices that form the respective edge data platform. In the concept, each participating company has such an interface in order to standardize the individual IT infrastructure for a homogeneous appearance within the shared data space.

To reduce the complexity of the evaluation, all containers run within a virtual cloud system, which offers the advantage of being clearer and simpler to configure. The Flower [16] Web Service and the Wireguard VPN service together form the connector node. All cooperating companies are connected to each other through only this mediator platform infrastructure. Wireguard creates a tunnel between the entities involved, enabling secure communication over a network or the internet. This is done by exchanging cryptographic keys using Curve25519 and using ChaCha20 for encryption and Poly1305 for authentication of data packets. These security techniques ensure that the transmitted data remains confidential and that the data transfer is protected against manipulation, while guaranteeing traffic performance. [17] The firewall of the connector is configured in a way that the source IP is checked and only known participants and services are allowed to communicate. The ports of the Wireguard VPN server, SQL ports and flower containers are known. In addition, a communication policy is defined as to who is allowed to communicate with whom.

Proxmox [18] was selected as the virtualization platform for the system. It is a user friendly and flexible open source platform which includes integrated functions for firewalls, high availability, network support, update management and backup options. The system is configured via a user interface using a secure HTTPS connection of the cloud server. The containers communicate with each other via the TCP/IP interfaces of the Flower service. With Flower federated learning, clients and webservice (Fig. 1) train machine learning models without exchanging raw data, increasing privacy and security. From the technical perspective, the raw data is stored locally and not in a shared data base, which increases data efficiency by reducing redundancy and minimizing data transfer overheads. Also, the data stays in sovereign territory, as long as the connector is considered as a neutral instance. Nevertheless, it is due to the central location of the VPN server that the raw data must be collected by the client. This means that it takes a detour via the data trustee.

Now it becomes clear how important a data trustee is when it comes to aggregating potentially transparent raw data. Without a solid concept for generating accountability, it is difficult to generate partners for such a form of supply chain.

### D. The Inclusion of a Data Trustee

A concept with or without the cross-location aggregation of non-transparent learning models or transparent raw data requires a responsible authority. The responsible entity should assume an independent position. A data trustee in terms of the EU Data Act [19] could be considered. This is responsible for the work of the connector, i.e. the aggregation of the information and who is allowed to communicate with whom. This step must be contractually defined in advance. A neutral third party or a selected supply chain stakeholder that has been agreed upon is therefore recommended as the operating authority.

### E. Performance Analysis of the Existing MVP

After the within this paper used experimental setup has been described, this part will present the results of the performance evaluation. The performance was measured in two scenarios: Direct communication from three Flower clients to the Flower server and communication from three MySQL [20] databases to three Flower clients, both with and without the VPN encryptions. The performance values were measured using My Traceroute [21] with 3000 packets being sent and pinged in each case. The

performance was measured in the following configurations:

- Clients communication: Three Flower Clients communicate directly with the Flower Server. Three Flower Clients communicate with the Flower Server via the Wireguard VPN server.
- Database communication: Three MySQL databases communicate directly with three Flower clients. Three MySQL databases communicate with three Flower clients via a VPN server.

The following tables summarize the relevant measurement results, including average latency and the corresponding standard deviations. The loss of packets was 0% in all scenarios.

TABLE I
NATIVE PERFORMANCE MEASUREMENTS

| Container | Hop to | Avg in ms | StDev in ms |
|---|---|---|---|
| flwr-client-1 | flwr-server | 0,1 | 0 |
| flwr-client-2 | flwr-server | 0,1 | 0 |
| flwr-client3 | flwr-server | 0,1 | 0 |
| mysql-db-1 | flwr-server | 0,1 | 0 |
| mysql-db-2 | flwr-server | 0,1 | 0 |
| mysql-db-3 | flwr-server | 0,1 | 0,1 |

TABLE 2
PERFORMANCE MEASUREMENTS USING WIREGUARD VPN

| Container | Hop to | Avg in ms | StDev in ms |
|---|---|---|---|
| flwr-client-1 | flwr-server | 1,1 | 0,3 |
| flwr-client-2 | flwr-server | 1 | 0,3 |
| flwr-client3 | flwr-server | 0,9 | 0,2 |
| mysql-db-1 | flwr-server | 0,8 | 0,3 |
| mysql-db-2 | flwr-server | 1,3 | 0,3 |
| mysql-db-3 | flwr-server | 0,9 | 0,3 |

The measurement results show a higher latency when using the VPN. For direct communication between the Flower Clients and the Flower Server as well as communication between the MySQL databases and the Flower Clients without VPN, the latency times are relatively low and remain constant. Constant remaining standard deviations (StDev) of the latencies indicate a functionality issue with the algorithm behind the interaction. In this case, there are no significant abnormalities and all values are very close to each other, which indicates a successful process.

Even if the encryption procedure slows down the data packets by a factor of ten on average, the use of VPN offers considerable security advantages. It should also be mentioned that this system is not designed for critical real-time requirements.

## III. RISK ASSESSMENT OF A DISTRIBUTED DATA PLATFORM

A functionally secure system is now available with the existing MVP. The following step is to design this next version of the data platform in such a way that further relevant security measures are identified, analyzed and adapted based on the threat situation via a risk assessment. In this context, security standards such as IEC 62443-3-2 [22] or VDI/VDE 2182 Sheet 1 [23] are used to ensure proven, systematic and reliable protective measures against cyber threats by the use of risk analysis. Both standards can be used to conduct a risk analysis in a production environment. Nevertheless, the procedure from VDI/VDE 2182 Sheet 1 is also used in this paper. This assessment process is cyclical and consists of sequential steps, which are described approximatively in the following text and are applied accordingly to the case of the MVP.

In the first step, all existing assets are identified, grouped and listed in an inventory list. Once this has been accomplished, the next step is to identify the threats in accordance with the standard. To ensure an accurate threat identification, it is beneficial to select tools or practices that facilitate this step.

### *A. Analyzing Threats*

In order to obtain an overview of existing threats to all assets of the system, thread modelling tools (TMT) can be used to support application-based threat analysis. [24] For this purpose, the software system is modelled on an abstract level. On this basis, the TMT is able to generate a catalogue of possible threats. The TMT from the developer Microsoft [25] was used within the scope of the project. This TMT is based on the STRIDE model, which divides the potential threats into the categories of spoofing, tampering, repudiation, information disruption, denial of service and elevation of privilege in order to cover the protection goals of authentication, integrity, non-repudiation, confidentiality, availability and authorization. [24]

Specifically, for the MVP, the threat modeling report summarized that the threat situation for the TCP/IP interactions between all containers (Fig. 1). The HTTPS connection has not been considered as part of the test object. The reason for this is that the instance does not exist in the real image of the data platform. It is only intended for configuring virtual test objects within the cloud environment. Nevertheless, it should be mentioned that the communication path is protected via the TLS encryption protocol.

Another method used today for supply chains to identify threats accordingly is the use of software bills of materials (SBOMs). SBOMs corresponds to a list of the components that compose all software elements of a

system or data platform. They are primarily used in supply chains to improve the transparency and maintenance of software products. By providing a clear overview of the components of a software, SBOMs help companies to identify potential vulnerabilities or security gaps in their system. When it comes to identifying threats to the system, additional more security relevant information is automatically gathered for detailed risk analysis when the SBOM is generated. [26] For this use case, the containers were executed separately using Docker. The input of the corresponding image name into the CLI tool and Go library Syft [27] generated the SBOM in JSON format. There are other ways to generate SBOMs, as well as several formats to represent it. Platforms such as snyk.io provide the appropriate information about the analysis of SBOMs by describing the vulnerabilities in technical detail. This also includes the description of violations to the protection goals. In the VDI guideline, a risk classification is carried out from the collected results.

### *B. Determine Protection Goals, Analyze Risks and Selection of Security Strategies*

The collected information is now used to list the individual threats, vulnerabilities, direct consequences and associated protection goals for each asset in the inventory list. The compiled results are used to rate the overall risk for each individual threat scenario. For example, the estimated extent of damage can be multiplied by the estimated probability of damage. The resulting product provides the overall risk for the corresponding threat. [23] The next step is to define the security measures, which are also to be documented with estimated costs / effort and effectiveness. Table 3 contains an excerpt of the results from the MVP in a simplified representation for a clear insight.

TABLE 3
EXCERPT RESULTS OF THE RISK ANALYSIS

| Asset | Threat | Protection goal | Risk | Actions |
|---|---|---|---|---|
| Flower Containers and WireGuard VPN server incl. Bind9 DNS server | System failure due to (D)DoS | Availability | Medium | Load balancing or direct prevention measures via DDoS protection services such as Cloudflare |
| | System intrusion by attackers | Availability, integrity, confidentiality | Medium high | Implementing an intrusion detection system IDS and antivirus software |
| | System failure for any reason | Availability | Medium | Application Backup |
| Flower TCP/IP communication | Loss of data sovereignty because of external VPN server localization | Integrity, confidentiality | Medium high | Adaptation of the system architecture by redistributing communication paths between the containers |
| | System intrusion by attackers / Man-in-the-middle | Availability, integrity | Low | VPN already provides protection; additional IDS checks network activities for anomalies |
| MySQL Database Container | SQL Injection | Availability, integrity, confidentiality | Medium | Set input validation, restrict database rights to a minimum, regular updates and patches |
| AlmaLinux - Container OS | Root manipulations | Availability, integrity, confidentiality, authentication | Medium high | Use by restricted users only |

One of the most important findings to be taken from the table is, that it is not enough to focus only on the software components of the data platform, even if the test object is only a virtual environment. It should be noted, that the hardware of the stakeholders must also be physically protected. To protect the data sovereignty of each company, it is also important to keep this information locally with the owners and to adapt the infrastructure of the data platform accordingly.

In accordance with VDI/VDE 2182 Sheet 1, the practical implementation of the protective actions now follows, as well as the process audit, which is described approximately in the next chapter. The entire process documentation as described in this chapter is a constantly repeating process that checks and adapts the system for the entire life cycle.

## IV. PROPOSAL FOR THE SECURITY DESIGN OF THE DISTRIBUTED DATA PLATFORM

After the risk assessment, the software architecture of the MVP has been adjusted to meet the identified shortcomings.

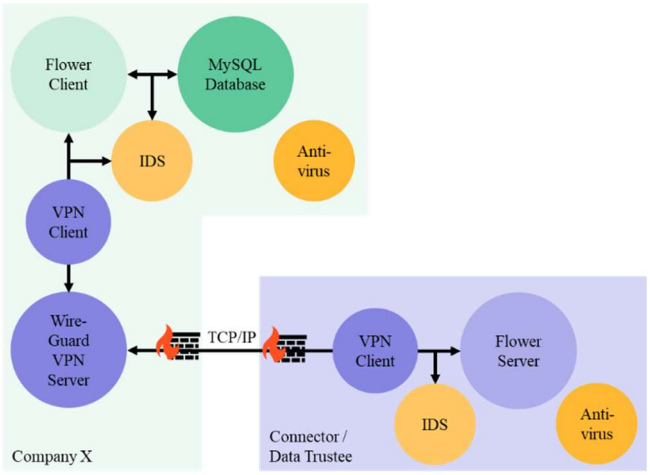


Fig. 2. Customized software architecture to preserve data sovereignty.

Fig. 2 shows that each company now has its own VPN server. Because the companies host their VPN tunnel themselves, they also have direct control over what information leaves the company. Assuming that a large number of companies are connected to the connector, this configuration also provides a performance advantage. This can be explained by the fact that no single VPN server in the connector now has to host the node of various connections. From now on, the raw data for creating the analysis model remains local and does not leave company x like in the first approach (Fig. 1). This step also reduces the responsibility of the data trustee for managing the connector service.

With respect to IEC62443-3-3 [28], the proposed security design of the distributed data platform fulfills the major requirements. The identification and authentication criteria are met because as the first barrier firewalls check the VPN tunnel by source IP and the Wireguard services support certificate-based authentication. Usage control over the containers is ensured by a selected data trustee who assumes the agreed responsibilities as an administrator. Sensitive company data does not leave its local source and only non-transparent learning models are created to optimize the supply chain. The integrity and confidentiality of the data exchange is guaranteed by Wireguard VPN's cryptographic hashing and encryption methods. To protect against suspicious data traffic and malicious code, IDSs and antivirus scans are included both in the companies' edge data platforms and in the connector. The data flow is restricted by only allowing a connection to the connector via the VPN network. Firewalls are configured so that only known addresses and their ports are allowed to communicate. Human-to-human communication is not part of this data platform. Proxmox contains monitoring functions for continuous system monitoring and timely reaction to events. Realistically, this responsibility lies upon the data trustee. Cloudflare [29] DDoS protection services protect resource availability. Backup options need to be available for configured services such as Flower Client and Server for the data platform functionality. However, it is recommended that a consortium implements a unified backup strategy for the stakeholders' individual data silos. As described, the database in the edge data platform is already a redundant representation of what exists in the warehouse inventory.

## V. CONCLUSION AND FUTURE WORK

The research presented in this paper describes the development and validation of a secure IT infrastructure for distributed data platforms in supply chains. The results for the security measures based on a risk analysis according to VDI/VDE 2182 Sheet 1 are presented. The implemented system integrates security components such as encryption, firewall configurations, and IDS/antivirus measures to ensure the protection goals of data integrity, confidentiality, authenticity, and availability. Using Wireguard VPNs with certificate-based authentication and encryption mechanisms effectively secures the communication channels. The content of the proposed architecture complies with the IEC 62443-3-3 standard and provides a framework for data sovereignty of participating companies and their secure communication via common non-transparent learning models within the data platform, administered by a data trustee.

The current research work forms the basis for further improvements and scaling tests of the system. Future work will focus on the following topics: Continued customization of the MVP, integration of new security measures and validation of the infrastructure through additional cycles of risk analysis and penetration testing. Scalability testing will assess the system's ability to handle more client connections and traffic. Particular attention will be paid to the performance of the Flower Server under various loads and its ability to maintain efficient operation with numerous VPN connections. In addition, the system will be deployed in a real cross-site environment, allowing for an evaluation of its practicality under actual operating conditions.

In conclusion, the developed system, incorporating a defense in depth strategy, provides a secure foundation for distributed data platforms in supply chains. Future improvements and extensive testing will further consolidate its robustness and scalability, paving the way for widespread industry adoption.

## ACKNOWLEDGMENT

This work was done in cooperation with the Zukunftslabor Produktion of the Zentrum für digitale Innovationen in Lower Saxony (ZDIN) Project No. ZN3489. Special thanks also go to the law firm Herfurth & Partner from Hanover, Germany.

REFERENCES


[1] G. Culot, G. Orzes, M. Sartor, and G. Nassimbeni, "The future of manufacturing: A Delphi-based scenario analysis on Industry 4.0," *Technological forecasting and social change*, early access. DOI: 10.1016/j.techfore.2020.120092.

[2] J. Kallisch and C. Wunck, "Options for connecting decentralized data infrastructure to improve Supply-Chain decision making without giving up individual data property," *Decision Sciences Institute 2022 Annual Conference Proceedings*, 2022.

[3] F. Södergren and M. C. Wallén, "Creating Value Through Information Sharing: Exploring the Transition Towards a Digital Supply Chain," *Umeå University, Faculty of Social Sciences, Department of Informatics*, 2022.

[4] "GAIA-X: Technical Architecture." Accessed: Jul. 11, 2023. [Online]. Available: https://tinyurl.com/262d7vwt

[5] J. D. Rodenberg and I. Anitsal, " A Review of Machine Learning Applications: Emerging Trends and Challenges in Supply Chain Management," *Institute for Global Business Research Conference Proceedings*, Volume 7, Number 3, 2023.

[6] J. Kallisch and C. Wunck, "Using vertical Federated Learning in industrial Supply Chains," *Decision Science Institute*, 2023.

[7] J. Kallisch and C. Wunck, "Development of a Prototype for a Process Support and Analysis Platform for Small and Medium-sized Enterprises," vol. 2022, 31-20, DOI: 10.29007/jmrk.

[8] J. Kołodziej, M. Repetto, and A. Duzha, *Cybersecurity of Digital Service Chains* (13300). Cham: Springer International Publishing, 2022.

[9] "Allianz Risk Barometer 2024: Identifying the major business risks for 2024," *ALLIANZ COMMERCIAL*, 2024. [Online]. Available: https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[10] T. Høyvarde Clausen, "Firm heterogeneity within industries: how important is 'industry' to innovation?," *Technology Analysis & Strategic Management*, vol. 25, no. 5, pp. 527–542, 2013, DOI: 10.1080/09537325.2013.785512.

[11] N. B. A. Aziz, R. B. Ahmad, and D. D. Dominic, "e-Supply Chain (e-SC) trust model for B2B collaboration- A case study of Malaysian construction industry," in *2014 International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, Malaysia, 2014, pp. 1–4, DOI: 10.1109/ICCOINS.2014.6868426.

[12] "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," (Industrial Control Systems Cyber Emergency Response Team), 2016. [Online]. Available: https://tinyurl.com/25wk5lrs

[13] N. Pohlmann, *Cyber-Sicherheit: Das Lehrbuch für Architekturen, Konzepte, Prinzipien, Mechanismen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Germany: Springer, 2022.

[14] J. Umbreen, M. Z. Mirza, Y. Ahmad, and A. Naseem, "Assessing the Role of Minimum Viable Products in Digital Startups," in *2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Kuala Lumpur, Malaysia, 2022, pp. 1073–1077, DOI: 10.1109/IEEM55944.2022.9989653.

[15] Srijith, Bantia, Govardhan, and Anala, "Inter-Service Communication among Microservices using Kafka Connect," in *2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, 2022, pp. 43–47, DOI: 10.1109/ICSESS54813.2022.9930270.

[16] Flower Labs GmbH. "Flower Framework Documentation." Accessed: May 31, 2024. [Online]. Available: https://flower.ai/docs/framework/

[17] Jason A. Donenfeld. "WireGuard Website." Accessed: May 31, 2024. [Online]. Available: https://www.wireguard.com/quickstart/

[18] Proxmox Server Solutions GmbH. "PROXMOX Website." Accessed: 34.05.2024. [Online]. Available: https://www.proxmox.com/en/

[19] European Commission. "Data Act: Commission proposes measures for a fair and innovative data economy." Accessed: May 31, 2024. [Online]. Available: https://tinyurl.com/ydgdk23j

[20] Oracle. "MySQL Documentation." Accessed: May 31, 2024. [Online]. Available: https://dev.mysql.com/doc/

[21] Cloudflare, Inc. "What is My Traceroute (MTR)?" [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-mtr/

[22] IEC 62443-3-2:2020: *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design,* IEC-International Electrotechnical Commission, 2020.

[23] *VDI/VDE 2182 sheet 1: 2020: IT-security for industrial automation - General model,* VDI Verein Deutscher Ingenieure e.V.

[24] Nancy Mead, Forrest Shull, Ole Villadsen, and Krishnamurthy Vemuru, "Hybrid Thread Modeling Method," 2020, DOI: 10.1184/R1/12366992.v1.

[25] Microsoft. "Microsoft Threat Modeling Tool threats." Accessed: May 10, 2024. [Online]. Available: https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool-threats

[26] A. Chaora, N. Ensmenger, and L. J. Camp, "Discourse, Challenges, and Prospects Around the Adoption and Dissemination of Software Bills of Materials (SBOMs)," in *2023 IEEE International Symposium on Technology and Society (ISTAS)*, Swansea, United Kingdom, 2023, pp. 1–4, DOI: 10.1109/ISTAS57930.2023.10305922.

[27] Cybersecurity and Infrastructure Security Agency (CISA). "Syft." [Online]. Available: https://www.cisa.gov/resources-tools/services/syft
[28] IEC 62443-3-2:2020: *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels,* IEC- International Electrotechnical Commission, 2020.
[29] Cloudflare, Inc. "DDoS Protection Services." Accessed: May 31, 2024. [Online]. Available: https://www.cloudflare.com/ddos/#DDoS-Page-Pricing-AS