21. AALE-Konferenz
Dresden, 12.–14. März 2025

Securing Data Sovereignty and Data Security for independent participants in supply chains

Jonas Kallisch[1], Prof. Dr. Karl-Heinz Niemann[2], Prof. Dr. Christoph Wunck[1], M. Runge[2], M. Voß[2]

Abstract

The paper describes implementing an information-sharing approach for companies that are connected via supply chains. In contrast to previous and existing solutions, no raw data is exchanged in this kind of system; only agreed information is shared. The concept is therefore data-saving and suitable for protecting the intellectual property of the interacting companies. The implementation of the concept, the design and the components used for implementation are described. Furthermore, the concept is placed in the context of existing approaches to data exchange between companies. In addition to demonstrating the necessity of such a concept, the questions of what risks the proposed architecture poses for the participating companies in terms of IT security are addressed. Furthermore, it is explained how these risks can be counteracted. In doing so, the proposed architecture will be examined for the potential to minimise possible misuse. The paper ends with an outlook on future activities within the project.

Keywords

Supply Chains, Data Exchange, Data Security

1 Supply Chains and intercompany data exchange

The goal of this paper is to present an architecture that enables secure information exchange between companies in supply chains without the necessity of direct data sharing. This architecture is being tested as part of a pilot project supporting the digitalization of small and medium-sized enterprises in Lower Saxony. It focuses on safeguarding data sovereignty and IT security through decentralized data processing and advanced standards.

Supply Chains (SC) have become a keystone of global economic architecture [1]. In addition, digitization enables companies to analyse their operations and manufacturing systems to improve their value creation better than at any time before [2]. Machine learning and data analysis yield opportunities to reduce waste, improve the timing and quality of the products produced at the shop floor[3]. At the same time prices of such technologies are decreasing, which enables even small businesses to use them. Therefore, many companies have started to collect data from their shop floors to take advantage of the opportunities or to lay the ground to do this in the future. Aware of the value of their data, the companies have become very sceptical about sharing these shop floor data with other companies, e.g., their suppliers. By doing so, they give up opportunities to improve the overall production efficiency along the value creation chain [4]. This paper will start with an examination of the state of intercompany data exchange to explore potential improvements.

[1] Hochschule Emden/Leer, Emden
[2] Hochschule Hannover, Hannover

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

1.1 Current Supply Chain intercompany data exchange

The current state of intercompany data exchange in a supply chain can be considered as fractured and often reduced to the bare minimum. This means that the data exchange between the companies in a supply chain is often limited to business communication [5]. All this happens at the Enterprise Resource Planning (ERP) level. The Manufacturing Execution System (MES) and the systems on the shop floor are usually not involved in the exchange. Companies use to communicate with their suppliers and customers in horizontal communication by sending material orders or by converting customer orders into production orders and later into individual machine orders. The result is that neither the participating companies nor the supply chain management can access all data that might be available on a certain step inside the SC [6]. Another issue is that the systems working independently cannot be as efficient as if they were connected.

To address these challenges, this paper introduces an approach where only pre-defined and agreed-upon information is shared instead of raw data. This concept helps to protect sensitive information and intellectual property, providing a viable solution to the concerns raised by many companies. The authors conducted a series of interviews with experts, executives, and representatives from non-governmental organizations to better understand the reasons behind the limited data integration in SCs. The results revealed that the reluctance to share data stems from a fear of losing control over it and the potential risk of exposing critical intellectual property to competitors. By offering a structured approach to selective data sharing, this paper aims to alleviate these concerns while maintaining the confidentiality of proprietary information.

Additionally, the fear of exposing production infrastructure to cyberattacks, such as hacking or misuse by SC partners, further discourages companies from integrating their shop floor systems. These results are consistent with findings from other studies, such as the interview series conducted by Södergren and Cartling Wallén, which highlight similar challenges in fostering trust and collaboration in supply chains [7].

Beyond identifying these barriers, the paper examines how IT security risks, including data misuse and cyberattacks, can be mitigated within the proposed architecture. Moreover, the study positions this concept within the context of existing data-sharing solutions, demonstrating its novelty and practical application for modern supply chains.

Looking at these facts, it can be concluded that shop floor data exchange between companies is not widespread in practice. In the following section, we will show the benefits of shop floor data exchange in supply chains and propose a solution to the problem. Then, in part two, the paper will explain why existing architectures are unsuitable for the solution and how research can address this gap. Finally, in section three, the paper will show how the IT security requirements of the proposed architecture can be met.

1.2 The benefits of horizontal integration

A major opportunity for horizontal integration is to reduce the costs of overall data handling inside the SC [8]. Much of the data used by the participants is collected at different stages of the SC for various purposes. The cross-company sharing of this data would be a low-level entry to the usage of a supporting data platform because the shared data is already available at the different companies along the supply chains. In addition, the companies involved in the SC can be seen as members of a community of trust, as they share a common interest in improving the group's results [9].

The proposed architecture allows companies to securely share information without exposing sensitive raw data, thereby addressing concerns about intellectual property protection. This selective sharing approach also reduces redundancy in data collection and facilitates a more efficient analysis

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

along the entire value chain. By linking data from different stages of the manufacturing process, it is made possible to generate new knowledge and reveal patterns that would otherwise remain hidden. For example, correlations between events in later production stages and data patterns from earlier stages can be identified and addressed. This additional information allows for the reduction of rejects and optimization of the overall production system [9].

In addition, as mentioned in the first part, data analytics and Machine Learning (ML) have proven to create value on the shop floor [10] [11]. A survey has shown that companies largely use ML and analytics in classic fields like optimizing order scheduling or calculating costs [12]. Besides these tasks, ML is used in predictive maintenance or to analyze quality data. By that, it can be taken as proof that data analytics can address problems and reduce cost in manufacturing environments of a single company or shop floor. The extension of the described approach to the supply chain level enables companies to leverage these benefits across the entire network, creating opportunities for global optimizations [13].

The concept presented in this paper builds on these proven benefits and demonstrates how horizontal integration, supported by a secure and selective data-sharing architecture, can enhance collaboration and efficiency in supply chains. Even without mentioning every possible application, such integration represents a significant improvement over the current state of practice.

1.3 Projekt “Zukunftslabor Produktion” Lower Saxony

To support the digitalization of businesses, the government of Lower Saxony in Germany has started the Project 'Zukunftslabor Produktion' [Futurelab Manufacturing, ZLP]. This interdisciplinary project is developing solutions and models, especially for small and medium-sized businesses in the manufacturing sector. Based on a use case involving the production of die-cast aluminum parts, the project examines how manufacturers can use data analytics and other Industry 4.0 methods to improve their shop floor systems and to create a more resilient supply chain.

A central focus of the project is the development of a secure and decentralized architecture for connecting shop floor data from independent businesses along the supply chain. Unlike traditional approaches, this architecture ensures that raw data remains protected while only pre-defined, agreed-upon information is shared. This selective sharing not only preserves the intellectual property of participating companies but also reduces the risk of data misuse.

The project part 'Infrastructure and Security' specifically investigates how to implement such a data-sharing architecture while addressing the unique challenges of security and interoperability. The proposed solution builds on federated analytics and advanced data-sharing protocols, aligning with standards like GAIA-X and OPC UA to ensure seamless integration into existing ecosystems. Safeguarding data is particularly critical as the intellectual property of small and medium-sized businesses often represents a key asset of their business model.

In the next chapter of this paper, we will show a suitable solution for information sharing between companies in supply chains that preserves the rights of their individual data and the intellectual property of the data owners. In later parts, we will show possible threats to the solution and how the data bridges between the companies can be secured.

2 The prototype of a supply chain workflow connector

In this part of the paper, the authors will show how a connection of companies along an SC can be reached. We will discuss how different kinds of data storage can be related and how a connection is possible if only information, not raw data, shall be exchanged.

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

2.1 Concepts to connect shop floor data of independent companies

A key goal of the ZLP is to create a support data platform for an aluminum die-casting process. As mentioned, this platform should be able to connect the SC data stores while ensuring that the property rights of this data are not touched. The decentralization of data elements comes with significant challenges.

First, the boundaries between the data storages of the companies must be clearly defined, and the relationships between the process elements must be described without combining the data. To address this, the process of analyzing distributed databases requires knowledge of analytical methods in all companies involved. Every SC member must be able to adapt the model to its own database.

2.2 Linking individual data storages

The SC of the aluminum die-casting process involves a variety of stakeholders. These include CAD designers, manufacturers of the cast, and companies that manufacture the die cast parts. This diversity results in the use of different database systems. Additionally, companies within the SC utilize various MES and ERP systems with distinct data models.

To connect these disparate databases, the ZLP has studied several existing approaches. While the operating database systems differ, the boundaries between the data elements are often easy to identify. As a starting point, serial or batch numbers of exchanged goods are used to link the data elements of SC partners. Companies retain full responsibility for selecting the relevant data they are willing to share, ensuring data sovereignty.

2.3 Federated Analytics, Federated Catalogue and Vertical Federated Learning

A key issue of decentralizing data stores is that analytical algorithms typically require a combined dataset. Due to the SC's concerns, members of ZLP have investigated the usage of federated analytics and the concept of the federated catalogue proposed by GAIA-X, as well as vertical federated learning (vFL) [14].

Federated analytics enables algorithms to operate on distributed datasets without requiring raw data transfer. The global model is trained iteratively using data subsets from individual partners, ensuring that raw data never leaves the premises of the contributing organizations.

A second option is the usage of a federated catalogue. This concept, promoted by the GAIA-X architecture, allows sharing of data elements under a public catalog [14]. In this concept, every partner within the SC can see the catalog of data available but can only access data when access is granted. Therefore, the companies can choose to permit sharing data on a piece-by-piece level.

Besides these architectures, some other, not mentioned concepts, have been investigated. Since these and the presented concepts do not fit all requirements, the ZLP has started working on a concept that enables companies to share knowledge without sharing data.

Vertical Federated Learning (vFL) extends this approach by focusing on datasets that share overlapping sample IDs but contain different feature sets along the value chain [15]. For instance, in an SC scenario, company A might have process-level data, while company B has detailed quality assurance data. Using vFL, a joint machine learning model can be trained by securely aligning and processing these complementary datasets without jeopardizing data privacy. This allows SC partners to uncover cross-company correlations, such as how precursor processes influence product quality at later stages, while preserving their individual data sovereignty.

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

2.4 Suggested architecture for a Supply-Chain data connection

The authors have identified that existing concepts fail to meet all requirements for solving the problem of intercompany information exchange without direct data sharing. To address this, the proposed architecture combines federated analytics vFL and other approaches into a new, data-preserving and information-sharing solution.

The architecture facilitates information sharing via a linking platform that neither requests centralized data processing nor passes raw data between SC partners [16]. Instead, it uses existing connections, such as the flow of goods identified by batch or serial numbers, to link data across the supply chain.

To implement vFL effectively, the Flower framework [17] was integrated into the architecture. Flower provides a flexible and scalable approach to coordinating federated learning workflows across heterogeneous data sources. By leveraging Flower, the architecture enables SC partners to securely train machine learning models on vertically partitioned datasets.

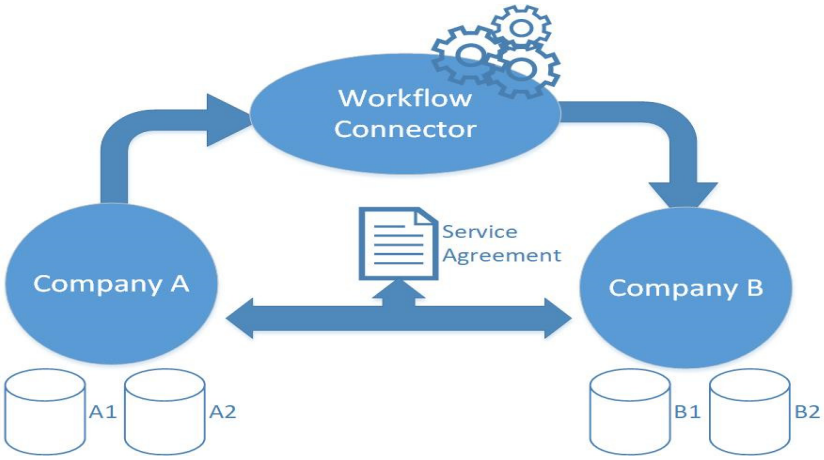


Figure 1: Concept of suggested architecture

This description of possible networks results in a concept whose core is a value-oriented relationship between at least two partners. As displayed in Fig. 1, the partners are connected via a process support platform that distributes information, based on the stored exchange relationships. The participants would be company A with the dataset A1 and the derived information A2, and company B with the dataset B1 and the derived information B2. In this scenario, A2 and B2 are exchanged. Thus, participant A holds the information A1, A2, and B2, and participant B holds A2, B1, and B2. Each participant can determine the specific information provided.

Based on this core concept, the participants of the process support platform can improve their analyses through individual agreements on services. Such a service could involve cross-company fault cause detection. For example, if a fault occurs at company B that cannot be explained by its processes, company A might need to determine whether this fault traces back to its production. This collaborative approach minimizes information leakage while enabling actionable insights.

A prototype for cross-company information exchange was developed iteratively in coordination with participating companies. Data from casting machines that were already digitally connected were linked with data from precursor processes and quality assurance. The pilot project aimed to determine relationships between processes such as machine preparation, the casting process and the resulting quality. Validation was supported by the willingness of participating institutions to exchange data and compare the quality of the solution, which only exchanges information, against the results of direct data consolidation.

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

The prototype implementation consists of three layers:

- The data layer: Information is securely stored and managed using a Hadoop-based platform [18].
- The agent layer: Implemented with the JADE framework, this layer provides individual services that guarantee the availability of specific information under predefined conditions [19].
- The workflow connector layer: This layer organizes the information flow and links data points using batch or serial numbers.

Each agent in the workflow connector guarantees the availability of specific information based on the provided input conditions. The individual components, implemented as Hadoop containers, ensure portability and scalability. By integrating federated learning workflows via Flower, the architecture ensures secure collaboration across distributed systems.

3 Threats for the suggested concept

As described before, the past security concepts for production facilities tried to separate the production system from other IT systems of the company using the so-called cell concept [20]. The defense in depth approach backs this cell concept [21], which uses a layer of complimenting measures to protect the production system. Nevertheless, the communication in the production domain was unprotected against attacks and internal offenders [22] could attack the production systems and the real-time communication. Attacks on real-time communication systems on the shop floor are possible and documented in the literature [23].

There are various approaches to classifying different risk factors in IT systems. In this paper, we will first analyze the impact of the vulnerabilities with respect to the concept presented. The authors will use the factors Jouini, Rabai, and Aissa described [24]. This approach divides the threats into human, environmental, and technological factors. In addition, all factors can be internal and external. The authors find that the proposed architecture increases vulnerability because human and technological factors are affected.

New technical systems introduced in this paper may lead to unintended information sharing among companies. In addition, data leaks can occur through misuse, SC data can be misinterpreted or corrupted, and the aggregation of manufacturing data into the internal platform creates a point where a single malicious employee can do significant damage by gaining access to the collected data. Malicious partners and external attackers, such as hackers, are additional examples of potential threats. A malicious partner could exploit the system by making false requests to gain more knowledge about fellow participants than they are entitled to.

The integration of vertical federated learning (vFL) introduces additional risks:

1. Model manipulation: A malicious participant could introduce erroneous data into local computations, which might distort the global model and lead to inaccurate predictions or analyses [25].
2. Meta-information exposure: Even when raw data is not shared, meta-information, such as model updates, could reveal sensitive patterns or correlations, potentially exploitable by competitors or attackers [26].
3. Increased dependency on secure coordination: The federated learning orchestrator (e.g., Flower framework) must remain secure and reliable. Any compromise in the coordination layer could affect the entire federated learning process [27].

There are inherent security risks in applying the newly proposed information-sharing system. Some of the systems used require complex shielding and precise adjustment. For example, the transport layer between companies must be encrypted appropriately, and the communication functions must be guaranteed to ensure availability. On the other hand, internal links must also connect securely to the databases of production plants and machine data acquisition systems, which may not currently

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

be connected. These connections must be secured, and the data streams consolidated carefully. Without proper measures, these vulnerabilities could lead to data theft, data leaks, erroneous data and erroneous conclusions, resulting in corrupted datasets [28]. These issues not only endanger a company's internal conclusions and physical facilities but also pose risks to the partner companies that indirectly process this data or make decisions based on it.

4 Resulting security requirements

The external and internal threats result in specific measures that can be used to protect the architecture proposed in this paper from identified threats. In this section, we will first describe the requirements arising from the proposed architecture. The requirements are the result of a research study conducted within the project. In the second part of this chapter, we will describe measures that are suitable for ensuring the security of the data bridges. In the current thesis, various protection concepts are being analysed and examined to see whether the measures described here are suitable and sufficient.

4.1 Special security requirements for the Production domain

The increasing horizontal and vertical integration of business processes leads to the situation that the cyber-security on the shop floor needs to be improved and streamlined with the rest of the security organization in the company. It must be considered that a production environment has special security requirements that differ from the concepts in the IT domain. These are, for example:

- Priority is the availability of the production system.
- SW Patches cannot be installed immediately but only after a pre-test in a non-critical environment.
- Signature updates for virus scanners must be tested bevor installed in a production environment.
- User authentication with name and password might be a problem when the plant is in a critical situation.

These special requirements in the production domain are summarized under the ex-pression OT-Security. The different requirements for IT-Security and OT-Security are shown and compared to the requirements of the IT domain. To address the OT-domain's special needs, the standard Series IEC 62443 has been developed to support plant designers and system manufacturers concerning OT security. The most relevant part of the described concept is part IEC 62443-3-3[29].

4.2 Security requirements for the described concept

In the first run, the concept described has typical security requirements for a state-of-the-art production system. In 2014 one of the authors described already 18 security requirements in the context of Industry 4.0[30] that are today still valid for the approach discussed. The key requirements are (excerpt):

- Secure Communication in the OT domain
- Cyber-Physical Systems need to be considered
- Secure connection of components to the system
- Inclusion of the human factor into the concept
- Monitoring of the security status
- Protection of intellectual property
- Adaptability to changing requirements

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

- Consideration of cloud services
- Intelligent sensors and actuators must be included in the concept.
- Long operation time of the production plant.

The requirements described above can be allocated to different parts of the system. In the first run, the shop floor with real-time communication shall be considered. All intelligent components (IO-Devices, PLCs, intelligent Sensors, and Actuators) need to communicate via a secure protocol. If we consider PROFINET as one of the possible means of communication, the secure version of PROFINET must be used [31]. This ensures the integrity and authenticity of the real-time data communicated in the automation system. Intelligent sensors with Ethernet interface increasingly use Single-Pair-Ethernet. These sensors and their communication need to be included in secure communication [32].

Once acquired in the field, the data leaves the shop floor and is forwarded to the database system previously described. To maintain network segmentation according to IEC 62443-3-3 [33], the shop floor is separated from the rest of the company network by a firewall. Servers that need to be accessed from the shop floor as well as from other parts of the company often reside in a Demilitarized Zone (DMZ) [34]. The communication of production data from the shop floor PLCs or CPS can be performed by a middleware protocol, e.g., OPC UA [35]. OPC UA supports secure communication between the Client (the described application) and the Server, e.g., the PLC or CPS that acquires and provides the data.

With the security measures described, it is ensured that real-time data acquired on the shop floor is communicated securely inside the shop floor network and to the database server outside the shop floor. In the next step, the access of different stakeholders to the database needs to be considered. This includes secure communication across the boundaries of the company that acquired the data, meaning that different companies access certain aspects of the data. The platform Industrie 4.0 worked on this topic and defined the requirements and possible approaches for a secure intercompany data exchange [36]. This also includes legal aspects.

5 Conclusion

This paper introduces a architecture designed to address the challenges of secure and efficient information sharing among participants in supply chains (SCs). By shifting the focus from raw data exchange to the sharing of pre-defined information, the proposed concept emphasizes data sovereignty and the protection of intellectual property. This selective sharing approach is supported by vertical federated learning (vFL), and decentralized linking platforms, ensuring the confidentiality and integrity of the shared insights.

The major contributions of this work include the demonstration of secure data exchange, enabling companies to collaborate through the exchange of actionable insights rather than raw data, thereby mitigating risks associated with data misuse. Furthermore, the integration of vFL and frameworks like Flower allows SC partners to uncover cross-company correlations without compromising data privacy. The concept aligns with established industry standards such as IEC 62443 and OPC UA, ensuring interoperability and compliance with modern cybersecurity requirements, and addresses potential risks with detailed mitigation strategies.

The prototype developed within the "Zukunftslabor Produktion" project validates the feasibility of this approach. Its integration of decentralized data storage, federated analytics, and secure communication protocols provides a scalable foundation for future enhancements. Validation efforts confirm that the concept effectively bridges the gap between independent SC participants, fostering cross-company collaboration while safeguarding sensitive information.

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +

6 Literature

[1] Holweg, M., Disney, S., Holmström, J. u. Småros, J.: Supply Chain Collaboration. European Management Journal 23 (2005) 2, S. 170–181

[2] Marmolejo-Saucedo, J. A., Hurtado-Hernandez, M. u. Suarez-Valdes, R.: Digital Twins in Supply Chain Management: A Brief Literature Review. In: 2020 – Intelligent Computing and Optimization, S. 653–661

[3] Weichert, D., Link, P., Stoll, A., Rüping, S., Ihlenfeldt, S. u. Wrobel, S.: A review of machine learning for the optimization of production processes. The International Journal of Advanced Manufacturing Technology 104 (2019) 5-8, S. 1889–1902

[4] Supply Chain Design for the Industrial Internet of Things and the Industry 4.0, Radanliev, P., Roure, D. C. de, Nurse, J. R. C., Montalvo, R. M. u. Burnap, P., 2019

[5] Stock, J. R. u. Boyer, S. L.: Developing a consensus definition of supply chain management: a qualitative study. International Journal of Physical Distribution & Logistics Management, 39(8), 690-711. International Journal of Physical Distribution & Logistics

[6] Xu, Y. u. Chen, M.: An Internet of Things based framework to enhance just-in-time manufacturing. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture 232 (2018) 13, S. 2353–2363

[7] Södergren, F. u. Cartling Wallén, M.: Creating Value Through Information Sharing: Exploring the Transition Towards a Digital Supply Chain, 2022

[8] Alcácer, V. u. Cruz-Machado, V.: Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems. Engineering Science and Technology, an International Journal 22 (2019) 3, S. 899–919

[9] Rong, K., Hu, G., Lin, Y., Shi, Y. u. Guo, L.: Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors. International Journal of Production Economics 159 (2015), S. 41–55

[10] Wuest, T., Weimer, D., Irgens, C. u. Thoben, K.-D.: Machine learning in manufacturing: advantages, challenges, and applications. Production & Manufacturing Research 4 (2016) 1, S. 23–45

[11] Monostori, L., Markus, A., van Brussel, H. u. Westkämpfer, E.: Machine Learning Approaches to Manufacturing. CIRP Annals 45 (1996) 2, S. 675–712

[12] Sharp, M., Ak, R. u. Hedberg, T.: A Survey of the Advancing Use and Development of Machine Learning in Smart Manufacturing. Journal of Manufacturing Systems 48 Pt C (2018), S. 170–179

[13] Kozlenkova, I. V., Hult, G. T. M., Lund, D. J., Mena, J. A. u. Kekec, P.: The Role of Marketing Channels in Supply Chain Management. Journal of Retailing 91 (2015) 4, S. 586–609

[14] GAIA-X: Technical Architecture, 2021. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-xtechnical-architecture.html

[15] Yang, Qiang; Liu, Yang; Chen, Tianjian; Tong, Yongxin (2019): Federated Machine Learning: Concept and Applications. In *ACM Transactions on Intelligent Systems and Technology (TIST) Volume 10 Issue 2, Article No. 12, January* (12). Available online at https://arxiv.org/pdf/1902.04885

[16] Kallisch, J.; Marx-Gómez, Jorge; Wunck, C. (2024): Challenges and Opportunities of Intercompany Big Data Analytics in Supply Chains. In *Development Methodologies for Big Data Analytics Systems*, pp. 249–262. DOI: 10.1007/978-3-031-40956-1_10.

[17] Flower (2023): Flower: A Friendly Federated Learning Framework. Available online at https://flower.dev/, updated on 11/14/2023, checked on 11/14/2023.

[18] Apache Software Foundation, Apache Hadoop. [Online]. Available: https://hadoop.apache.org/ (accessed: Aug. 28 2022).

[19] Jade Site | Java Agent DEvelopment Framework. [Online]. https://jade.tilab.com/ (accessed: Sep 3 2022).

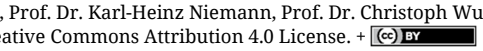
[20] PROFIBUS Nutzerorganisation e.V., PROFINET Security Guideline. [Online]. Available: https://www.profibus.com/download/profinet-security-guideline (accessed: May 9, 2022).

[21] NCCIC/ICS-CERT, “Recommended Practice: Defense in Depth,” [Online] https://www.cisa.gov/uscert/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[22] Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security: Innentäter. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_061.html (accessed: Jul. 29 2015).

[23] R. Perdisci, Detection of Intrusions and Malware, and Vulnerability Assessment: 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19-20, 2019, Proceedings. Cham: Springer International Publishing AG, 2019. [Online]. Available: https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5921892

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. + CC BY

[24] Jouini, Mouna, Latifa Ben Arfa Rabai, and Anis Ben Aissa. "Classification of security threats in information systems." Procedia Computer Science 32 (2014): 489-496.
[25] Han, Song, et al. "Practical and robust federated learning with highly scalable regression training." IEEE Transactions on Neural Networks and Learning Systems (2023).
[26] Durrant, Aiden; Markovic, Milan; Matthews, David; May, David; Enright, Jessica; Leontidis, Georgios (2022): The role of cross-silo federated learning in facilitating data sharing in the agri-food sector. In *Computers and Electronics in Agriculture* 193, p. 106648. DOI: 10.1016/j.compag.2021.106648.
[27] Zhang, Jie; Guo, Song; Qu, Zhihao; Zeng, Deze; Wang, Haozhao; Liu, Qifeng; Zomaya, Albert (2022): Adaptive Vertical Federated Learning on Unbalanced Features. In *IEEE Trans. Parallel Distrib. Syst.*, p. 1. DOI: 10.1109/TPDS.2022.3178443.
[28] Zhang, Jie; Guo, Song; Qu, Zhihao; Zeng, Deze; Wang, Haozhao; Liu, Qifeng; Zomaya, Albert (2022): Adaptive Vertical Federated Learning on Unbalanced Features. In *IEEE Trans. Parallel Distrib. Syst.*, p. 1. DOI: 10.1109/TPDS.2022.3178443.
[29] J.-M. Flaus, Cybersecurity of Industrial Systems. Newark: John Wiley & Sons Incorporated, 2019. [Online]. https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5813671
[30] IEC 62443-3-3:2013 + COR1:2014: Security for industrial automation and control systems Part 3-3: System security requirements and security levels, International Electrotechnical Commission, 2013.
[31] K.-H. Niemann, “IT-Security-Konzepte für die Prozessindustrie,” atp, vol. 56, 07-08, pp. 62–69, 2014, doi: 10.17560/atp.v56i07-08.2256.
[32] K.-H. Niemann, “IT security extensions for PROFINET,” in 2019 IEEE 17th International Conference on Industrial Informatics (INDIN): Aalto University, Helsinki-Espoo, Finland, 22-25 July 2019: Proceedings, Helsinki, Finland, 2019, pp. 407–412.
[33] K.-H. Niemann and S. Merklin, “OT security requirements for Ethernet-APL field devices,” in ATP-Magazin.
[34] N. Jiang, H. Lin, Z. Yin, and L. Zheng, “Performance Research on Industrial Demilitarized Zone in Defense-in-Depth Architecture,” in 2018 IEEE International Conference on Information and Automation: August 11-13, 2018, Wuyishan, China, 2018, pp. 534–537.
[35] IEC TR 62541-1:2020 - OPC Unified Architecture - Part 1: Overview and concepts RLV | IEC Webstore. [Online]. https://webstore.iec.ch/publication/68039 (accessed: May 9, 2022).
[36] IEC TR 62541-2:2020 - OPC Unified Architecture - Part 2: Security Model RLV | IEC Webstore. [Online]. https://webstore.iec.ch/publication/68036 (accessed: May 9, 2022).

Open Access. © 2025 Jonas Kallisch, Prof. Dr. Karl-Heinz Niemann, Prof. Dr. Christoph Wunck, M. Runge, M. Voß
This work is licensed under the Creative Commons Attribution 4.0 License. +