# Security Considerations for Collaborations in an Industrial IoT-based Lab of Labs

Jan Pennekamp*, Markus Dahlmanns*, Lars Gleim†, Stefan Decker†, Klaus Wehrle*
*Communication and Distributed Systems, RWTH Aachen University, Germany · {lastname}@comsys.rwth-aachen.de
†Databases and Information Systems, RWTH Aachen University, Germany · {lastname}@dbis.rwth-aachen.de

***Abstract*—The productivity and sustainability advances for (smart) manufacturing resulting from (globally) interconnected Industrial IoT devices in a lab of labs are expected to be significant. While such visions introduce opportunities for the involved parties, the associated risks must be considered as well. In particular, security aspects are crucial challenges and remain unsolved. So far, single stakeholders only had to consider their local view on security. However, for a global lab, we identify several fundamental research challenges in (dynamic) scenarios with multiple stakeholders: While information security mandates that models must be adapted wrt. confidentiality to address these new influences on business secrets, from a network perspective, the drastically increasing amount of possible attack vectors challenges today's approaches. Finally, concepts addressing these security challenges should provide backwards compatibility to enable a smooth transition from today's isolated landscape towards globally interconnected IIoT environments.**

***Index Terms*—secure industrial collaboration; interconnected cyber-physical systems; stakeholders; Internet of Production**

## I. Introduction

New advances in the area of the Industrial Internet of Things (IIoT) [1] and the Internet of Production (IoP) [2] show that the traditional focus on local communication is antiquated given the progress the Internet of Things (IoT) initiated. These advances promise to improve the manufacturing sector on a broad scale by utilizing knowledge across organizations [3]. Due to the exchange of process knowledge, the advances range from business-related aspects, such as a reduced time-to-market or improved productivity [4], to sustainable aspects, like decreased amount of scrap or less machine wear [5]. Overall, the shift towards smart production enables companies to unlock currently unrealized value.

Lab of Labs: In the following, we refer to collaborating IIoT devices at different physical locations as a *lab of labs*. Such a lab of labs interconnects different production sites, supply chains, and cyber-physical systems (CPSs) with each other even across organizational borders to enable visions, such as the IIoT or the IoP. Consequentially, the challenge of security considerations is imminent because, now, multiple stakeholders have to be considered which amplify traditional risk surfaces. While comparable issues are present in the consumer IoT [6], they usually have fewer consequences.

**Contributions.** To bridge the gap in security considerations from a single lab to requirements for a lab of labs enabled by IIoT devices communicating across company boundaries, in this paper, we study the associated risks and identify future challenges. More precisely, our contributions are as follows:

1) From an information and network security view, we identify ten distinct risks that emerge in an interconnected lab of labs. To complement these angles, we discuss legal aspects for the participating stakeholders and their data.
2) Subsequently, we derive security requirements that enable stakeholders to minimize their expose and attack vectors.
3) To address these aspects, we highlight the current state of applicable solutions and identify future work.

## II. Motivation for a Lab of Labs

Reasons for establishing a connected digital production landscape are manifold. While the main driver is to make knowledge from local data sites globally accessible and to utilize data from various sources [2], these advances also allow more flexible collaborations between stakeholders [2]. Furthermore, existing business relationships can be improved by providing sophisticated digital information to previously only analog flows [7]. Next, we highlight the reasons to create a foundation for understanding the associated security risks.

**Connecting Data Sources and Data Silos.** In today's production landscape, domain knowledge is usually retained locally and thus results in the creation of data silos. This situation in conjunction with conservative data sharing polices of stakeholders significantly hinders the exchange of information [8]. Hence, sensor data and other parameters are only accessible for a single stakeholder and not for the complete landscape. Today, industrial devices, e.g., CPSs or IIoT devices, mostly communicate with (local) infrastructure, potentially even over propriety protocols with vendor lock-in [9], effectively hindering the advances they claim to facilitate. Thus, future improvements have to make data sources accessible on the one hand, and remove the borders of currently isolated data silos on the other hand, to allow for an increased productivity and sustainability.

**Enabling Dynamic Collaborations.** Nowadays, technical improvements enable stakeholders to create connections more easily and to establish trust more quickly. As a result, companies can utilize short-term collaborations, which in turn yields flexible relationships in a lab of labs. In a traditional production environment, simply deploying a new machine or switching the input raw materials was a challenging, time-consuming, and non-sustainable process because finding the ideal set of parameters was far from trivial. Industrial collaborations promise to ease such obstacles as these parameters could potentially be shared, i.e., newly deployed IIoT devices

Author manuscript.

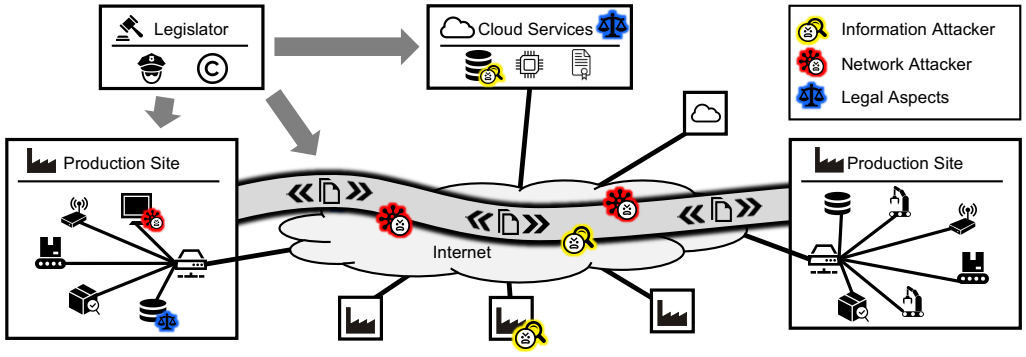


Fig. 1. Industrial collaborations in a lab of labs introduce new security challenges as IIoT devices, CPSs, and services from different stakeholders are interconnected globally through the Internet. In particular, (global) information and network attacker as well as legal aspects must be considered.

can retrieve configuration settings from a knowledge repository that contains appropriate settings. Hence, even such short-lived relationships can significantly improve the productivity.

**Improving Existing Business Relationships.** So far, the motivation to establish a lab of labs mainly originates from aspects regarding manufacturing technology. However, similar advances are also expected for existing relationships along the supply chain [2], enabling the tracing of products from design until operation and, in cases of faulty production batches or other alarming conditions, simplifying the analysis and communication between involved parties.

On a different note, the connection of previously isolated data silos and the improved business relationships might allow companies to tackle the issue of the bullwhip effect [10]. In the past, companies were unaware of the real demand on the market because of missing insight into the consumer's business needs. This lack of information resulted in inaccurate estimates that ultimately led to unsold goods, filled warehouses, and even the need to treat them as scrap. With an interconnected landscape, the required information is easily accessible and miscalculation can be prevented to a certain extent, effectively improving the sustainability of the supply chain.

Overall, the motivation for interconnecting IIoT devices in a lab of labs is reasonable and its implementation would result in significant changes to today's (isolated) manufacturing landscape. To structure the changes and perform a smooth transition between current production and a future lab of labs, three major steps are envisioned [3]. In a first step, companies need to explore the benefits a lab of labs introduces in known settings with trusted partners before integrating information from non-competitors in a second step and from competitors in a third step. However, applied to their fullest extend, these changes introduce risks which we analyze in the following.

## III. Risks of a Globally Interconnected Industrial Internet of Things

Figure 1 provides an overview on a lab of labs and the three different angles of security risks. Basically, different production sites are connected to the Internet while exchanging information, i.e., IIoT devices generate and transmit data over the Internet to other production sites. Furthermore, they can rely on cloud services to store, transfer, and process data. However, all these possibilities introduce attack vectors on the different layers of production (production cell, production site, global lab of labs) to the companies which were previously unknown in a locally contained scenario.

First, exchanging data might allow adversaries to retrieve information from the data and the communication patterns which were not intended for (external) disclosure. These entities acting as information attackers could be located at various vantage points, e.g., cloud providers or other collaborators. Second, attackers on the Internet might not necessarily target specific transmissions. Instead, they could simply have an incentive to disturb or alter the communication. Due to the increased number of attack vectors, network attackers might not only be located in the Internet, but also in the local network, e.g., controlling an IIoT device in a production cell. Third, global data transmissions and storage under external control also affect the legislative view on security, i.e., legislators define which data can be transferred, which stakeholders may be granted access, and where data may be stored. Hence, this angle affects information exchanges, the production sites, especially their local data storage, and cloud services alike.

Next, we introduce the different angles in more detail.

### A. Information Security

Collaborations and resulting data exchanges have an effect on the data usage as well as on data access. Thus, a lab of labs introduces significant risks in terms of information security.

*Risk IR1 Loss of Data Sovereignty:* A core requirement for many production companies is the concept of data sovereignty to ensure the protection of their intellectual property and trade secrets. While an increasing amount of interconnection between IIoT devices has the potential to improve productivity, it equally poses a threat regarding a loss of control over proprietary know-how, intellectual property, data, and processes [11].

*Risk IR2 Information Leakage:* Concretely, the disclosure of sensitive information can lead to adversarial effects. For example, warehouse inventory numbers could be exploited by customers, competitors and suppliers in various ways to manipulate negotiations. Similarly, sharing too detailed process data could facilitate imitation or counterfeit products by competitors, vertical integration by suppliers, or generally result in leakage of proprietary know-how to third parties.

Even superficially arcane information with no obvious connection to trade secrets can convey critical information through side channels [12], [13]. For example, timestamps that reveal when products were produced could allow for inferences wrt. the production capacities, outages, and further insights into internals that should not be disclosed. As such, every shared piece of information may increase the chances of adversaries to reverse-engineer sensitive details. These issues are already well-known from traffic analysis, e.g., website fingerprinting attacks reveal a comparable risk on the content of transmissions [14]. Similarly, even if data is apparently requested by legitimate endpoints, all stakeholders should act with caution to prevent data leakage due to targeted phishing attacks [15]. Past attacks on production facilities have revealed corresponding threats to company networks.

*Risk IR3 Loss of Control:* Regardless, additional data sovereignty considerations even apply for data which is objectively not privacy sensitive, as data providers may want to control who can use their data for which purposes, how long, and how to deal with derivative works. This situation introduces a dilemma between the sovereignty aspects and the desire to participate in a lab of labs. So far, data providers usually want to minimize the risk of losing data control and introducing uncertainty of data sovereignty.

*Risk IR4 Unreliability:* On the other end of the spectrum, data consumers are faced with uncertainty wrt. the reliability of data providers and the quality of both data itself and its annotations. In practice, data frequently lacks interpretability due to different standards, data structures, value ranges, as well as differences between cultural and individual understandings of certain terms and concepts. Similarly, the quality of the measured data itself can vary greatly and is often hard to evaluate without detailed knowledge as to how it was generated.

As such, trust between data providers and data consumers can be hard to establish and is always challenged by the risk of malicious data providers, intentionally sabotaging data and processes for different reasons. Additionally, processes tightly coupled to digital information exchange can introduce novel attack vectors to manufacturing, such as impersonation attacks, traditionally not associated with the manufacturing domain.

### B. Network Security

Connecting production networks to public networks like the Internet does not only require security considerations related to the transferred data between communicating stakeholders, but also detailed analyses regarding network security.

*Risk NR1 External Intruders:* The goal of interconnecting different labs relaxes the borders of the labs networks and consequently former isolated networks form globally reachable endpoints. These networks, however, do not only consist of secured IIoT devices, but also of older industrial controllers and machines, e.g., Programmable Logic Controllers (PLCs), not initially intended for global network access.

The devices were designed with an isolated network in mind, i.e., no network security aspects were considered. This situation is unlikely to change in the upcoming years since manufacturing devices usually have a longer lifetime than off-the-shelf consumer hardware [16]. Therefore, we can still expect these devices to have a remaining lifetime of several decades. However, already during the digitalization independent of a proposed lab of labs, more and more industrial devices are reachable from the Internet [17]. Thus, we observe that attackers are able to control local devices without any posed challenges or constraints since these devices lack any security features. Consequently, attackers might also able to override safety features designed to protect humans from harm.

*Risk NR2 Threat of Surveillance:* Equally, legacy PLCs and industrial machines communicate over various antiquated protocols that were designed for communication in isolated networks as well. Thus, these protocols are either not capable to provide any security features or they fail to match today's security requirements. Nevertheless, they are already used to connect industrial devices over the Internet without any (newly) added security features [18]. Consequentially, we derive the possibility for attackers to intercept ongoing communication and to modify the transferred data, such as launching Man-in-the-Middle attacks or tracking communication [19], as a network risk.

*Risk NR3 Implementation Vulnerabilities:* Connecting formerly isolated devices to a global network often discloses, apart from the risks that arise due to the communication itself, other vulnerabilities that were not considered by the typical testing, design, and usage of industrial devices, i.e., typical production tests normally focus on safety when all devices interact in a non-malicious way but not on security. Hence, when attackers do not comply with these specifications, they might reveal vulnerabilities in the devices' implementations.

*Risk NR4 Malware Infections:* Moreover, even when legacy devices reside in an isolated part of the network, which does not permit any communication to the outside, control computers can be infected with a worm which then is able to infect the production devices. One sophisticated example is the Stuxnet worm which was able to infiltrate highly-secured devices in nuclear power plants [20]. To achieve these infections, after the first contact to the control network, Stuxnet practically spread to every device in reach. Therefore, we conclude that a spreading of malware in a highly interconnected production lab is also a severe threat.

### C. Legal Security

Following these two previous categories, security researchers are usually well aware of, we also identified several risks of legal security as challenges in a global lab of labs. In particular these risks can be categorized as follows.

*Legal Regulations:* Rules regarding data sharing may be imposed by legal frameworks, resulting in data sharing being illegal in some jurisdictions, essentially resulting in a felony for the stakeholder when ignored. A recent prominent example is the introduction of the General Data Protection Regulation (GDPR) in the European Union to protect customer information and to require consent before sharing related

data [21]. Furthermore, international regulations, such as export limitations due to matters of national security [22], can also restrict the ability to participate in collaborations.

*Ownership Responsibilities & Liabilities:* A different aspect deals with the ownership and provenance of data [23]. Currently, legal regulations of dealing with these aspects might not be completely developed for our targeted scenario. Issues regarding derivative works, resulting respective royalties, and equitable benefit sharing emerge. Compliance with existing business agreements, such as licensing restrictions, between collaborators and third parties must also be analyzed. Similarly, concerns about the liability are an issue from the legal security of such a lab of labs [24], e.g., what is the outcome if one company incurs damages due to faulty information from another. This aspect also applies to the safety of humans and potential hazards or danger to the physical environment. Whether the rights and responsibilities are distributed between all involved parties remains unclear, especially considering that a clear history of origin might not be derivable.

### D. Takeaways

To conclude, our three legal risks have a common outcome, i.e., participating stakeholders are challenged by unforeseeable legal expenses and claims of liability. We furthermore identified four risks regarding network security which mainly focus on the inability to monitor the increasingly large number of possible threats on the one hand and to discover all realistic attack vectors on the other hand. Finally, for a lab of labs, we defined four risks in the area of information security, which relate to two main concerns. First, data exchanges are hindered by a lack of clarity regarding the sovereignty of data. Second, unreliability of data can have severe negative consequences.

The risk of privacy invasions of humans and especially of workforce at the production sites is increasingly surfacing following the ubiquitous data collection. This statement also holds when introducing interconnected IIoT devices in today's production processes. However, for this paper, we consider this area to be out of scope and leave a respective analysis for future work to research with a more encompassing background.

In the remainder of this paper, we focus on technical aspects of security, i.e., on information and network security. Whether existing thread modeling approaches, such as STRIDE [25], are applicable frameworks, remains an open research question.

## IV. Requirements for Secure Collaborations

Based on the described risk factors, we derive a number of requirements for secure industrial collaboration scenarios. A crucial aspect is to obtain a reasonable trade-off between confidentiality and the willingness to disclose data is important. In general, establishing trust between the involved parties to enable fruitful and sustainable collaboration is also necessary.

### A. Information Security

First, clear and verifiable inter-organizational digital identities of the participants need to be established to be able to authenticate the participants of a given data exchange, potentially in a mutually distrustful environment or even with masked identities. Second, ensuring data quality is a crucial building block for successful collaborations. Clever labeling and modeling of information (also taking into account and preventing side-channel leakage) should enable interpretability of the data semantics, employing ontologies for interoperability, and linking to related physical entities, data sources and involved agents and processes. All information should further be indexable to enable performant information retrieval. These requirements address the risk of information leakage IR2.

Provenance information and audit logs of the data's formation history enable accountability and subsequently further trust and incentives for high-quality data. This information may even legally be required for the documentation process, e.g., in defense or biomedical applications. Digital signatures provide means to verify the integrity of data [3]. Preserving associated data for as long as the product exists or is in use can assist in backtracing of unexpected behavior and product failures to its potential root causes. Overall, these measures improve the reliability of information as challenged by IR4. Finally, to fully enable data sovereignty and to counter IR1 and IR3, data usage policies need to be established. To this end, either by relying on legal agreements, which is a common practice in the anglo-saxon business world, or using technical means, such as usage policies [26].

### B. Network Security

In NR1 we identified the possibility for attackers to control industrial components which are reachable from the Internet. This aspect introduces the requirement of controlled communication, i.e., the application of paradigms that prevent attackers to connect to and control industrial components. One paradigm is authentication which allows the connection end point to verify the identity of a user and therefore allows access control.

Authentication, however, does not tackle the risk of altered communication which we identified as NR2. More precisely, even messages between authenticated endpoints can be modified. Hence, another requirement is integrity protection of the communication which allows the communication endpoints to recognize altered messages, i.e., the industrial devices do not execute commands contained in altered or replayed messages.

In the course of protecting the network against the risks NR1 and NR2, one important feature is to detect security vulnerabilities that lead to these risks early. Then, administrators can close the vulnerabilities before attackers are able to exploit them. However, since many production lines operate 24 hours a day, a requirement apart from the discovery of vulnerabilities itself is that the detection and patching should not interfere with the production, i.e., detecting and addressing vulnerabilities should not result in a loss of productivity.

The relaxation of network borders in a lab of labs cannot result in prohibiting communication as the communication is an integral and non-removable part to implement the envisioned advantages. However, no network connected to global networks like the Internet can be considered secure since zero-day exploits allow attackers to intrude into a network

using exploits undetectable for security vulnerability scanners. Hence, intrusion detection systems in production networks are required to detect unusual behavior of devices connected to the network. The usage of intrusion detection mechanisms, in combination with a vulnerability scanner, allows a reduction of the risks NR3 and NR4.

## V. Towards a Secure Lab of Labs

To address the analyzed security risks in a lab of labs (cf. Section III) and the derived requirements (cf. Section IV), we first analyze the current state of research and discuss today's approaches before we define future research steps afterward.

### A. Current State

State-of-the-art research currently tackles some requirements that we defined in Section IV. Hence, we give an overview before we derive future research directions.

**Information Security Perspective.** In a lab of labs stakeholders are expected to profit from exchanging information, e.g., production sites offload extensive data processing to the cloud or labs collaborate to compute results jointly. However, in both cases the data owners aim to not reveal any of the input data. A current technique that promises to uphold these needs is homomorphic encryption which allows the computation on encrypted data without direct access to the data, i.e., it enables stakeholders to offload expensive computation to powerful cloud services without revealing any data [27]. A similar approach is secure multi-party computation which allows stakeholders to jointly compute results without sharing the input data [28]. Unfortunately, the performance of such techniques is insufficient to fulfill today's, much less tomorrow's needs, but first advances show a performance increase by reducing the computational overhead [29].

To enable stakeholders a consistent maintenance of provenance information (also called data lineage), the currently most established standard is the PROV model and ontology [30], which allows users to describe the use and production of *entities* by *activities*, which may be influenced in various ways by *agents*. Extending upon these concepts, Audit Logging can be realized, e.g., using the SPLog Audit Log Ontology and usage policies defined and compliance validated using the corresponding SPECIAL usage policy language [31]. The Open Digital Rights Language (ODRL) [32] provides another flexible and interoperable information model, vocabulary, and encoding mechanisms for representing statements about the usage of content and services. As such, policies represent permitted and prohibited activities or actions of stakeholders over specific entities or assets and may be limited by, e.g., how data is allowed to be processed or where it may be stored [26]. When upheld, data requirements can be met without introducing significant overheads to the data processors. Here, penalties for misbehavior in an industrial context must still be defined.

Recently, initiatives, such as the Personal Health Train initiative [33] or the International Data Spaces Association [34], have lead to the development of approaches that strive to utilize data right under the data providers control. To this end, these approaches include algorithms and statistical models to data sources, rather than sharing data with third parties, such as researchers [35]–[37]. The main benefit is the ability of utilizing all data, including sensitive and private information which the industrial context introduces, without data having to leave the original data source. As such, they are destined to provide a way to further support data sovereignty from a technological perspective.

A requirement to enforce such policies is to ensure that the communication partner is indeed who she claims to be. Otherwise, participating entities might be challenged by false information. Hence, authentication is important such that data processors can prove their identity to data owners and data owners can be sure that the policy is applied properly. To create a network of trust in the industrial context, Internet certificate authorities have to evolve as well. Today's established processes are too static for a dynamic environment such as a lab of labs, effectively limiting the opportunities to also exchange data anonymously. Fortunately, certificate authorities are not the only way to gain trust between different stakeholders. Modern technologies can leverage the properties of distributed ledgers and blockchains to establish trust and to provide protection against manipulation [38]. To this end, all stakeholders are required to participate in the blockchain and to monitor any alterations of the blockchain content. Enhanced blockchains also offer the concept of smart contracts that provide notary-like functions without introducing another central entity to deal with [38]. Hence, they provide an approach to provide authenticity in a digital environment.

**Network Security Perspective.** A recommended practice to increase the production network security in a traditional environment is network segmentation [16]. Splitting the company's network in two parts using a firewall, separating the corporate network which is connected to the Internet and the production network allows intercepting any data exchange that does not follow established and pre-defined rules. As some devices located in the production network need to communicate with devices in the corporate network, e.g., data historians, the firewall needs to forward this specific communication. To increase security, a recommendation based on the usage of a single firewall is the establishment of demilitarized zones (DMZs). Devices that need to communicate with both, the corporate network and the production network are moved in a DMZ between both networks. Hence, no device from the corporate network that is connected to the Internet needs to be allowed to communicate with the production network directly, i.e., infected corporate devices cannot interfere with the production. However, in a lab of labs, this approach has several drawbacks. First, no device from the production network is allowed to communicate with external devices which interferes with the basic idea of a lab of labs, i.e., production devices need to communicate over the Internet [18]. Second, malware infections in the corporate network remain a risk, especially when a device is allowed to communicate with other devices in the DMZ and, thereby, spreading its malicious activities via the DMZ to devices in the production network (cf. Risk NR4).

One way to enable production hardware to communicate over the Internet securely is the usage of security-enabled protocols that allow confidentiality, integrity, and authentication. However, since already deployed industrial (IoT) devices are often constrained, have a long lifetime, and software changes need to pass several testing phases, adding protocols with security extensions for communication, e.g., Modbus Security [39] or OPC UA, often is impossible. Therefore, old hardware would need to be replaced with devices that support security features [40]. However, replacing functional and expensive production hardware is unlikely and reduces the profit even with company-tailored solutions.

Proxying data over the Internet via a security-enabled protocol is another possibility to ensure that the transmitted data is not altered and vulnerable devices are reachable from the Internet [41]. Here, proxy devices need to intercept the connection on sender's and receiver's side to convert the data from an unsecured protocol into messages of a secure protocol on the sender's side and vice versa on the receiver's side. However, in this course, proxy devices need to interpret the source protocol. Measured by the variety of industrial control protocols available, this step results in a big effort. Nowadays, standardization efforts, such as the Web of Things [42], already try to define gateways to integrate IIoT devices into a single architecture to improve the general interoperability.

Finally, we consider the detection of unusual behavior of network devices. Here, different forms of Intrusion Detection Systems (IDS) already exist [43], i.e., host-based and network-based IDS as well as rule-based and anomaly-based IDS. However, host-based IDS is not practical in an industrial control system due to the constrained devices, i.e., these devices are not able to run an IDS. Additionally, for rule-based network IDS, rules need to cover all legitimate configurations, i.e., administrators have to define rules for every device in every situation. In contrast, anomaly-based network IDS need to create signatures by recording a system not under attack. However, in a highly dynamic environment, ensuring the correctness of the generated signatures is almost impossible.

### *B. Future Research Challenges*

Based on the current state of research, we can conclude that the derived security requirements are not yet sufficiently satisfied. Hence, we define several future research directions to fully enable the benefits of a lab of labs securely.

**Open Information Security Aspects.** To properly secure sensitive data, security models must be adjusted to also work in a global setting with multiple stakeholders. Here, the business secrets of a single stakeholder should be protected to match his interests. To this end, today's approaches of secure computation, such as secure offloading, e.g., via homomorphic encryption or secure multi-party computation, should also support tomorrow's industrial data rates and models. Hence, challenges wrt. scalability but also applicability must be addressed.

Another important direction follows from the trade-off between verifiability of (past) data exchanges and confidentiality requirements of information. Similarly, information security over time is a pressing and open issue: How to realize (confidential) accountability in a lab of labs (a) for parties that could change in the future, i.e., a subsequent selling of a product, or (b) by parties that disappear, e.g., dissolved companies. Distributed ledger technology already promises to implement accountability in an applicable way. Finally, the overhead when properly addressing all discovered risks is challenging with existing solutions. Hence, the complexity, when applying these technologies, must be reduced significantly.

**Open Network Security Aspects.** Given that network security is traditionally concerned with multiple parties, having multiple stakeholders in an industrial setting is not entirely new. However, the highly dynamic communication patterns in a lab of labs yield further aspects that were not considered in traditional networking. Most notably, the support of legacy devices, where security was not incorporated during the design process, is still an open challenge. Since traditional IT devices have a significant shorter lifetime, matching solutions are not available yet. Consequentially, research must focus on these aspects to address this remaining aspect of network security in an interconnected industrial setting. Besides, the flexibility and dynamic of communication in a lab of labs rises new challenges in identifying atypical and dangerous network behavior rendering today's solutions ineffective. Unfortunately, a pattern-based approach is likely to fail as communication simply consists of temporary relationships of previously unconnected parties that provide no past knowledge to train autonomously operating systems. Current generations of intrusion detection systems are mostly based on such techniques.

## VI. Conclusion & Future Work

Modern advances in production technology predict significant benefits by interconnecting IIoT devices and CPSs. This progress on the future of manufacturing de-facto establishes the creation of a global *lab of labs* that spawns numerous industrial collaborations between different stakeholders. However, besides the benefits, such as productivity and sustainability, this intention comes with imminent security risks.

**Security Risks.** We considered three different angles as part of our security considerations of a lab of labs. In total, we identified four issues concerning the information perspective, four problems dealing with the network attack surface, and two major legal aspects. These aspects range from data confidentiality over network challenges due to larger attack surfaces to uncertainties in legal matters for involved stakeholders.

**Security Requirements.** Based on these risks, we subsequently derived requirements and highlighted the current state of research for information and network security that must be satisfied when trying to implement today's visions of collaboration in a lab of labs from a technical perspective. In both fields, researchers need to ensure that the security measures developed are deployable in a globally interconnected environment. In this context, a main challenge is to enable the bootstrapping of new relationships between previously unconnected parties. Traditional approaches do not suffice as a negotiation of covering contracts is a time-consuming activity.

**The Road Forward.** Both fields need to provide backwards compatibility with existing deployments and enable a masking of participants while still supporting the required accountability needs of a global environment. These aspects are very challenging, especially since stakeholders are reluctant to hand out sensitive information to possibly unknown entities. Moreover, solutions in both domains need to assure that they introduce flexibility into the industrial context, where traditionally long-lasting relationships and security parameters were used.

Overall, they span the design space that must be considered when trying to establish a lab of labs in a secure manner. For concrete steps on implementing new types of dataflows in a lab of labs, we refer to related work [3]. Given that existing approaches currently cannot address all issues, we also postulate various research directions that should eventually enable companies to implement a lab of labs without fearing harm resulting from neglected security considerations.

**The Next Steps.** As first future steps, we propose to enable stakeholders to exchange data obliviously and securely while utilizing already deployed legacy or unpatched IIoT devices. The risks introduced by operating insecure hardware should be minimized. To this end, the company network could be protected with IIoT gateways that proxy insecure network protocols to secure data transmissions on the Internet to prevent unintended data leakage. Eventually, the overall interest will increase as first potential can be made accessible, shaping the way to a smarter manufacturing and production environment.

Advances in the related and more flexible area of consumer IoT security might also have a positive impact on the IIoT.

## VII. Acknowledgments

The authors would like to thank the German Research Foundation (DFG) for the kind support within the Cluster of Excellence "Internet of Production" (IoP) under the project id 390621612. The authors would further like to acknowledge support from the RWTÜV-Stiftung (foundation) within the project IoTRUST (S189/10030/2017).

## References

[1] A.-R. Sadeghi *et al.*, "Security and Privacy Challenges in Industrial Internet of Things," in *DAC*, 2015.
[2] J. Pennekamp *et al.*, "Towards an Infrastructure Enabling the Internet of Production," in *IEEE ICPS*, 2019.
[3] J. Pennekamp *et al.*, "Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective," in *ACM CPS-SPC*, 2019.
[4] C. Brecher *et al.*, *The Need of Dynamic and Adaptive Data Models for Cyber-Physical Production Systems*, 2017.
[5] T. Bergs *et al.*, "Stamping Process Modelling in an Internet of Production," in *CIRP TESConf*, 2019.
[6] M. Serror *et al.*, "Towards In-Network Security for Smart Homes," in *IoT-SECFOR*, 2018.
[7] R. Glebke *et al.*, "A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems," in *HICSS*, 2019.
[8] J. M. Bryson *et al.*, "Designing and Implementing Cross-Sector Collaborations: Needed and Challenging," *Public Administration Review*, vol. 75, no. 5, 2015.
[9] E. Sisinni *et al.*, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Trans. Industr. Inform.*, vol. 14, no. 11, 2018.
[10] T. Moyaux *et al.*, "Information Sharing as a Coordination Mechanism for Reducing the Bullwhip Effect in a Supply Chain," *IEEE Trans. Syst., Man, Cybern. C*, vol. 37, no. 3, 2007.
[11] P. D. Filippi and S. McCarthy, "Cloud Computing: Centralization and Data Sovereignty," *European Journal of Law and Technology*, vol. 3, no. 2, 2012.
[12] A. Narayanan and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," in *IEEE SP*, 2008.
[13] A. Narayanan and V. Shmatikov, "De-anonymizing Social Networks," in *2019 30th IEEE Symposium on Security and Privacy*, 2009.
[14] A. Panchenko *et al.*, "Website Fingerprinting at Internet Scale," in *NDSS*, 2016.
[15] D. J. Benny, *Industrial Espionage - Developing a Counterespionage Program*, 2013.
[16] K. A. Stouffer *et al.*, "Guide to Industrial Control Systems (ICS) Security," Tech. Rep., 2015.
[17] A. Mirian *et al.*, "An Internet-wide view of ICS devices," in *PST*, 2016.
[18] M. Nawrocki *et al.*, "Uncovering Vulnerable Industrial Control Systems from the Internet Core," *arXiv preprint arXiv:1901.04411*, 2019.
[19] J. Hiller *et al.*, "Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments," in *IEEE ICNP*, 2019.
[20] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security Privacy*, vol. 9, no. 3, 2011.
[21] P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed., 2017.
[22] C. L. Evans, "US Export Control of Encryption Software: Efforts to Protect National Security Threaten the US Software Industry's Ability to Compete in Foreign Markets," *NCJ Int'l L. & Com. Reg.*, vol. 19, 1993.
[23] D. S. Siegel *et al.*, "Commercial knowledge transfers from universities to firms: improving the effectiveness of university–industry collaboration," *The Journal of High Technology Management Research*, vol. 14, no. 1, 2003.
[24] J. Eschenbächer *et al.*, "Business and legal issues in enterprise collaborations: A German perspective," *Production Planning & Control*, vol. 12, no. 5, 2001.
[25] L. Kohnfelder and P. Garg, "The Threats to our Products," 1999.
[26] M. Henze *et al.*, "CPPL: Compact Privacy Policy Language," in *ACM WPES*, 2016.
[27] X. Chen, "Introduction to Secure Outsourcing Computation," *Synthesis Lectures on Information Security, Privacy, & Trust*, vol. 8, no. 2, 2016.
[28] S. Micali and P. Rogaway, "Secure Computation," in *CRYPTO*, 1992.
[29] M. Dahlmanns *et al.*, "Privacy-Preserving Remote Knowledge System," in *IEEE ICNP*, 2019.
[30] T. Lebo *et al.*, "PROV-O: The PROV Ontology," *W3C Recommendation*, vol. 30, 2013.
[31] S. Kirrane *et al.*, "A Scalable Consent, Transparency and Compliance Architecture," in *European Semantic Web Conference*, 2018.
[32] R. Ianella, "Open Digital Rights Language (ODRL)," *Open Content Licensing: Cultivating the Creative Commons*, 2007.
[33] Dutch Tech Center For Life Sciences, "Manifesto of the Personal Health Train consortium," 2017.
[34] B. Otto *et al.*, "Industrial Data Space: Digital Souvereignity Over Data," *Fraunhofer White Paper*, 2016.
[35] L. C. Gleim *et al.*, "Schema Extraction for Privacy Preserving Processing of Sensitive Data," in *MEPDaW-SeWeBMeDA-SWeTI*, vol. 2112, 2018.
[36] T. M. Deist *et al.*, "Infrastructure and distributed learning methodology for privacy-preserving multi-centric rapid learning health care: euroCAT," *Clinical and Translational Radiation Oncology*, vol. 4, 2017.
[37] A. Jochems *et al.*, "Distributed learning: Developing a predictive model based on data from multiple hospitals without data leaving the hospital – A real life proof of concept," *Radiotherapy and Oncology*, vol. 121, no. 3, 2016.
[38] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, 2016.
[39] "MODBUS/TCP Security – Protocol Specification," Modbus Organization, Inc., Standard, 2018.
[40] T. Alves *et al.*, "Securing SCADA Applications Using OpenPLC With End-To-End Encryption," in *ICSS*, 2017.
[41] T. Alves *et al.*, "Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers," *IEEE Embedded Syst. Lett.*, vol. 10, no. 3, 2018.
[42] D. Guinard and V. Trifa, "Towards the Web of Things: Web Mashups for Embedded Devices," in *ACM WWW*, 2009.
[43] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," *Computer*, vol. 35, no. 4, 2002.