Requirements for Usage Control based Exchange of Sensitive Data in Automotive Supply Chains

Sebastian Opriel
TU Dortmund University
and Fraunhofer ISST
Sebastian.Opriel@
tu-dortmund.de

Frederik Möller
TU Dortmund University
and Fraunhofer ISST
Frederik.Moeller@
tu-dortmund.de

Ute Burkhardt
Volkswagen Konzernlogistik
GmbH & Co. OHG
Ute.Burkhardt@
volkswagen.de

Boris Otto
TU Dortmund University
and Fraunhofer ISST
Boris.Otto@
isst.fraunhofer.de

Abstract

Current inter-organizational data exchange is restricted to essential information that serves to fulfill contractual commitments. Restricting the exchange of data in these terms, leads to non-consideration of potential improvements in operational processes. One objective of this article is to expose the variety of reasons that prevent these data from being exchanged. The focus is paid to data that are exchangeable from a technical and legal point of view, but whose exchange is not desirable from a company's perspective for reasons like potential data misuse or competition disadvantages. Based on our findings we derive a set of requirements for a software prototype, which is properly equipped to enable the exchange of sensitive data, paving the way of fostering transparency in automotive supply chains. For this purpose, we draw from a deep single-case study in the German automotive industry dealing with the exchange of demand and capacity information.

1. Introduction

Most managerial studies, dealing with the future of the automotive industry, identify a rising complexity as major issue which, amongst other reasons, leads to increased pressure on cost, individualization, elevated work load and high level of stress with remarkable effects on employee's physical and mental health [1, 2]. One approach to tackle this issue is by sharing information, which results in a higher supply chain transparency [3]. Both, information sharing and transparency, have positive impacts, e.g., on improving operational and supplier performance [3], or a reduction of operational uncertainty [4].

Today, we face the enormous potential to share data easily and lever optimization potential both internally as well as externally in collaborative business processes [5]. However, today's data exchange between automotive companies is determined by contracts, which primarily aim to fulfill a company's need for industry-related services, such as supplies of material and parts. Yet, 82 % of automotive supply chain companies agree that data-gathering will increase, with significant benefits for both sides [6]. Nevertheless 36 % of supply chain participants criticize unsatisfactorily complied data demands for process optimization and 26 % of possible data providers are not prepared to share their data [1].

Amongst others, retention against data sharing can be explained by an inherent fear of organizations to show transparency to suppliers or customers. One such example is the disclosure of erroneous processes, which could be used to the disadvantage of the data provider in future pricing negotiations, quality assurances, or negatively impact sensitive areas, e.g., competitive power or market shares [7]. Ultimately the common concern in business relations is a lack of trust and the permanent incertitude how dispensed data could be used or even misused for other purposes [8, 9].

Our research goal is to provide a software prototype which is properly equipped to allow the exchange of sensitive data and foster supply chain transparency. Previous definitions of sensitive data refer, for example, to personal data [10] or intellectual property related information [11]. In our scope, we define sensitive data as *information that are exchangeable from a technical and legal point of view, but whose exchange is not desirable due to mistrust, unclear benefits, or other concerns*. That leads us to formulate two research objectives, which are:

- **Research Objective 1:** Identification of current problems and barriers for the inter-organizational exchange of sensitive data
- **Research Objective 2:** Derivation of requirements for a software prototype for the inter-organizational exchange of sensitive data

The remainder is structured as follows: In section 2 we describe the methodologies and data sources used during our study. Section 3 specifies the status quo of inter-organizational data exchange and the literature-based background of our approach. In section 4 we summarize

URI: https://hdl.handle.net/10125/70662
978-0-9981331-4-0

current data exchange problems and barriers. On this basis, in section 5 requirements enabling the exchange of sensitive information are defined. Ultimately we discuss the findings in section 6 and draw the conclusion in section 7.

2. Research methodology

The present derivation of requirements is part of a larger Action Design Research (ADR) project [12] with the ultimate objective to build a software prototype for inter-organizational data exchange in the context of the German automotive industry. ADR is a suitable research framework since it is a straight-forward method to design artifacts conjointly with practitioners. Thus, in alignment with the first principle of ADR, which prescribes the necessity for practical motivation of research, we derive requirements based on field data in this paper.

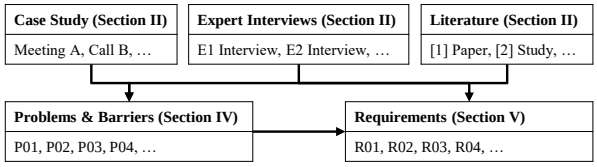

Figure 1. Data sources and derived artifacts.

In addition to the target to achieve the most comprehensive view on the issue, we triangulate our findings using three data sources [13] (Figure 1). Firstly we use data sources from a single-case study, such as internal documents, reports, presentations, protocols of meetings, workshops or phone calls. Secondly we enrich the findings through 9 expert interviews (Tables 1 and 2). Lastly by conducting a structured literature review we incorporate the existing knowledge base. All three data sources provide information about problems, barriers and requirements. A fourth source for requirements is given by the problems and barriers themselves (Figure 1).

As the phenomenon of interest is embedded in a complex inter-organizational setting, deep analysis and attention is required. Thus we chose to refer to a single-case study, since it is a suitable tool to analyze extreme cases and to derive rich and significant insights [14, p. 287]. In that, the extreme here, refers to the prototypical relevance of the object of investigation, as safe and sovereign inter-organizational data exchange of sensitive data in automotive supply chains is an unexplored phenomenon [15]. Furthermore, with 29 %, case study research is one of the most common methods to analyze issues of information systems and technology in automotive supply chains [16, p. 3856].

The single-case study between Tier 1 supplier and OEM (Original Equipment Manufacturer; in our case vehicle manufacturer) takes place in four phases: pre-project phase, concept phase, development phase, and pilot experiment (in latter which we are currently in). We have had 46 physical meetings, with 6 full-day workshops and 7 steering committees with 12+ participants. Additionally, we conducted 186 planned audio conferences over the whole single-case study (online or via phone, further referred as phone calls), which date back to late 2018. The duration of all meetings and phone calls sum up to at least 298 hours. In total the project consortium included over 90 participants from 17 different companies who were directly involved in physical meetings or participated in phone calls.

The main outcome of the single-case study is a continuously enhanced and revised concept document, detailing and consolidating the requirements and inputs of all contributing actors (final version: 45, slides: 135).

Table 1. Overview of expert interviews.

ID	Net/Gross	ID	Net/Gross	ID	Net/Gross
E1	45'/60'	E4	53'/60'	E7	48'/62'
E2	29'/40'	E5	53'/60'	E8	46'/55'
E3	30'/48'	E6	23'/26'	E9	54'/58'

Table 2. Domain and role of experts.

Domain	Business Unit (Interview Count)
OEM	Innovation (3), Corporate IT (1), Analytics (1), Logistics (1)
Supplier	Controlling (1)
Consulting	Supply Chain Expert (2)

As a second source, we conducted 9 interviews with experts from the automotive supply chain from 7 different companies (Tables 1 and 2). We chose the method of interviews as it is "the most common and one of the most important data gathering tools in qualitative research" [17, p. 3] to collect data from the field with industry experts. The interview partners were identified through interaction of the single-case study and chosen regarding their expertise in the field of data exchange and their ability to provide a holistic view on this topic. Therefore, each of them has at least 3 years of professional business experience in automotive companies (avg. 6 years). Additionally, they all have experience in demand and capacity management either by research-related examination of the field or by work experience. Prior to each interview, each interviewee received guiding questions (GQ) for the four interview phases:

- **GQ1:** How are data exchanged currently?
- **GQ2:** What are the biggest issues in data exchange?
- **GQ3:** What projects and innovative solutions are there in data exchange?

- **GQ4:** What is your vision for data exchange? (Time span: roughly 15 years)

In order to gain qualitative insights open questions were asked, so that each interviewee could answer as freely as possible and address issues according to their proper assessment. On average, the interviews lasted 42 minutes (net; recorded interview length) resp. 52 minutes (gross; total call duration). The interviews were recorded and partly transcribed for analysis and coding purposes.

Thirdly, we started our literature research in 12/19 following the recommended 3-step-approach for literature reviews of Webster and Watson [18], as they address explicitly literature reviews in the field of information systems and have emerged as a de facto standard. We used the computer sciences and information systems relevant databases aisnet.org, jstor.org, dl.acm.org and scopus.com. The most promising literature was reviewed and clustered. Contents were coded with a reference and knowledge manager. Afterwards we followed references backwards to identify further fundamental articles and handled them like the initial ones.

3. Research background

Europe's automotive industry standard for data exchange in supply chains is EDIFACT (United Nations Electronic Data Interchange for Administration, Commerce and Transport), which is an EDI standard [8]. First usages of EDI messages date back to the 1960s, followed by a broader adoption with the uprising internet in the early 1990s. Until 1993 92 % of all automotive component manufacturers used EDI for trading purposes [19]. Almost simultaneously with EDI, the exchange protocol OFTP (Odette File Transfer Protocol) was published in 1986 by Odette and is today the de facto standard within automotive industries [20]. The German Association of the Automotive Industry (VDA: Verband der Automobilindustrie) offers various definitions for messages within EDIFACT like VDA 4984 [21] (formerly VDA 4905) which specifies delivery instructions from customers to suppliers. Even though these types of standards do have a long-lasting history and are constantly enhanced, they do not define or promote any kind of technology-based, trust-gaining mechanisms for the usage of data [20].

Prior research in the field of data exchange has focused on inter-organizational data exchange, e.g., by regarding technical and semantic interoperability [22], collaborative supply chain management models [23] or trust-gaining frameworks for supplier-customer relationships [24]. Research and subsequently literature lack the focus on trust-gaining software concepts and software features to foster a software based exchange of sensitive information. The starting point of our single-case study thereby was the adoption of the concept of data sovereignty, which "refers to the self-determination of individuals and organizations with regard to the use of their data" [25, p. 550]. The literature provides various frameworks to conceptualize sovereign data exchange from different perspectives. One such concept is access control, which "constrains what a user can do directly, as well what programs executing on behalf of the users are allowed to do" [26, p. 40]. Nowadays companies share data in consideration of access control, which means that they decide, which data will be accessible by whom. Another approach is to restrict usage on the data receiver's side. In the field of Digital Rights Management (DRM), information can be protected by client-side reference monitors with a focus on intellectual properties within payment-based processes [11, p. 131]. In times of processing big data, structured raw data are exchanged. DRM solutions are not flexible enough due to their limitation on "a fixed set of usage scenarios" [27, p. 82]. Another approach to process data without having raw access to them is Secure Multiparty Computation (SMC) [28]. Through the use of cryptographic functions, inputs remain secret to the owner whilst computing a result with input of all participants. As the usage of the results is not protectable and the functions pursue a fixed calculation, this method is also not flexible enough. A third approach coined by Park and Sandhu [11] is usage control, which "is a generalization of access control to cover authorizations, obligations, conditions, continuity (ongoing controls), and mutability" [11, p. 128]. Its ultimate goal is to define what can be done with data on the data-receiver's side and therefore "encompasses traditional access control, trust management, and DRM and goes beyond them in its scope" [11, p. 172].

Usage control is a promising approach to gain trust in a receiver of own data, because it can be applied on a per-data level. Therefore, it is independent of both, the application domain and the used systems. However, case studies such as [7] in the Norwegian oil and gas industry are rare. The closest correlation to our study has [5], which defines architecture options for the enforcement of usage control in automotive supply chains. Domain-related, [29] defines general requirements for time-critical knowledge management in automotive industries, but without focus on the usage of control-enabled systems. To the best of our knowledge, no extensive in-depth requirement analysis has been realized so far for software prototypes enabling the exchange of sensitive data within automotive supply chains. Automotive industries have "some of the most complex supply chain dynamics in modern industry" [6, p. 16] and are characterized by just in time or just in sequence delivery, multi-sourcing, thousands of participants and end-products consisting of 20,000 parts [30]. Being one of the "largest and highly developed branch[es]" [5, p. 478] it has a unique position in the German economy.

4. Problems and barriers of data exchange

We describe current data-exchange problems and barriers summarized in Table 3. The problems and barriers were identified within the ongoing single-case study and were validated by expert interviews and a literature review.

Table 3. Problems and barriers.

	ID	Name	Origin
Problems	P01	Information lack	E1, E3, E6, E7, E8, E9
	P02	Rigidness and stiffness	E3, [31, 32]
	P03	Manual data exchange	E1, E4, E5, E6, E7, E8
	P04	Hardly processable formats	E1, E4, E5, E8
	P05	Human mistakes	E1, E6, E9
	P06	Low data quality	E1, E6, E9, [31]
	P07	Malicious actions	E1, E4, E6, E7, E8, [8]
	P08	Use of power position	E6, E7, E9, [33]
Barriers	P09	Unknown worthiness	E2, [23, 4, 34]
	P10	Unknown benefits for others	E3, E4, [34]
	P11	Missing foresight	E2, E4, [6, 31]
	P12	Effort to make data available	E1, E5, [31]
	P13	Lack of digital capabilities	E1, E7, E9, [1, 6, 8, 31, 35]
	P14	Investment cost	E1, E7, E8, [31, 35, 34]
	P15	Data misuse	E1, E2, E3, E4, E7, E9, [4, 34, 28]
	P16	Possibility of data breaches	E1, E9, [36, 30, 28]

4.1. Data exchange problems

To gain the most optimal competitive advantages, companies must utilize any data source available, including those from other organizations. Using another company's data implies processing of sensitive information, which they are not willing to share at this stage. Even though integration of data might result in optimized business processes for any participant in the supply chain, a lack of information (P01) is a significant problem.

Traditional supply chains usually rely on long-established organizational infrastructure, having often been solidified over centuries leading to rigidness and stiffness (P02). Subsequently, traditional ways of thinking and conducting business e.g., with long term contracts can hinder changes into flexible, disruptive and agile approaches. In particular, widely-used legacy systems cannot be replaced that easily. Therefore, it is not surprising that DOS-based systems nowadays still exist, which makes IT departments facing themselves with problems such as the integration of legacy systems into modern systems and applications [1].

Although EDI and platforms are broadly used, manual data exchange (P03) is still a common practice, especially in non-structured processes like managing bottlenecks, where a high degree of collaboration is required. The main potential for improvements is based on the optimization of used data formats and methods, such as email (texts, PDFs, spreadsheets or presentations) phone or fax. The problem is that these data are neither structured nor standardized (P04) and therefore difficult to import and process in IT systems. Furthermore, media breaks with human handling in between is a major source for human mistakes (P05), e.g., leading to wrong cell-formulas in spreadsheets or decimal point errors. Low data quality (P06) or simply wrong data coming from systems aggravate this problem.

Not all of the mistakes can be traced back to unintentional faults. Malicious actions (P07) sporadically occur, like the placement of phantom orders or unobvious lies in phone calls in order to boost supplies for safety reasons, which can lead to the well-known bullwhip effect in supply chains. One aspect of this is the often unequal dependence of the business partners on each other. Powerful positions are thereby traditionally on side of OEMs or key players within the supply chain. These companies can use their strong position to force business partners (P08) to comply with their needs, which is agreed to be replaced by collaboration approaches in the future [2].

The problems can be reduced to an old-fashioned manual handling of data, as well as potential actions contradicting a collaborative approach.

4.2. Barriers for changes

The first driver of insufficient data exchange, resulting from unwillingness to share, is the lack of knowledge. Companies usually do not know the worth of respective data (P09), which is particularly a problem of traditional industrial companies with non-digital-native background. Questions arise like "How much is the difference in worth of a data set, if it contains millisecond-based timestamps instead of second-based timestamps?" or "What is the exact value of stock information?". Very often these questions go along with a certain fear, to "sell" these data under price, due to the lack of knowledge about the benefits the exchange of data implies (P10). Together with the aspect that the profitability of digital solutions is difficult to evaluate, companies shy away from the effort to make data available and to prepare themselves to share them. This, especially, is even more critical, as operational units do not have a requisite foresight which particular data could be useful or for what

purpose data could be used for (P11). An explanation for this problem is that companies usually have a functional organizational structure. Operative employees of specialized departments know their processes fairly well and how to deal with existing information, but struggle with the identification of other data, due to the lack of knowledge of the availability of that kind of information on the business partner's side. Due to missing interaction with data research related departments, usually linked to the organizational ownership of a Chief Data Officer, requests for additional data or enhancements in data exchange are complicated to proceed.

The second driver is the effort needed to make data available (P12). Companies in general need to deal with a variety of different data silos which include, e.g., local data on employee's PCs, decentralized databases, file-based storage, software-based management systems (e.g., ERP, WMS, CRM, etc.) or shadow IT, such as self-generated spreadsheet-templates used aside of before mentioned managerial systems. Data sets being completely available from a single central point are mostly an exceptional coincidence. The majority are data sets being partly available and dispatched through several systems, generated over decades of time and therefore hard to maintain and to be connected with modern technologies like REST-APIs (Representational State Transfer-Application Programming Interfaces). Especially in deeper stages participants of supply chains, do often battle with a lack of necessary digital capabilities to solve problems of connectivity (P13). At the same time they usually do not have the budget to afford investments in cost-intensive IT solutions or to maintain them as required. That makes digitization being a significant cost factor (P14). The non-disclaiming fact for producing companies is that they need to "connect to uninterrupted IT systems [which] become[s] a matter of survival for suppliers/contractors" [1, p. 14].

The third driver, most accurately, can be called fear. Companies fear that data could be misused against them (P15), e.g., suppliers pressed in price levels due to information revealing that customers have bailed out, or that clients get to know that prices on raw material markets are supposed to decrease. Another fear is to become affected by data breaches, due to poor data security of business partners (P16). These concerns are justified by data incidents that are reported almost daily in the news, like breaches of Level One Robotics [36] or other companies. Also studies like [30] affirm this fact. One major problem in this context is that companies as well as humans tend to amass and archive data, which they "sometimes" forget to delete afterwards.

Most of the barriers outlined can be summarized to fears and missing trust between supply chain participants, which must be overcome to share sensitive data.

5. Requirements elicitation

We draw from the IEEE Software Requirements Specification (SRS) 29148-2018 [37] which is standardized and widely used for the definition of requirements. We structure the requirements referring to the recommendations of the SRS into Business Requirements and System Requirements with further sub-categories like Business Model, Business Process, etc. The requirements are defined with regard to the recommendations of the SRS, but are described as continuous text with additional argumentation and exemplified references to problems and barriers.

Hereafter we focus on specific requirements for designing a system to exchange sensitive data between participants in automotive supply chains. Requirements generally applying for information systems like security, data quality, or access control aspects are omitted, if not specifically needed for argumentation purposes. Resulting requirements are listed in Table 4 and 5, which give proper information about which problems they solve, which barriers they overcome and of which sources they originate from (i.e., interviews, interactions of the single-case study or literature).

5.1. Business requirements

Business model The purpose of a business model is to describe the logic of generating revenue and to conceptualize the blueprint of business conduct [41]. Usually that results in the business logic that is required to generate a positive ROI (Return on Investment) (R01). Ultimately, the adoption of a software prototype needs to be incentivized by clear organizational benefits to uncover the worthiness of the data (*P09*). Measuring the effectiveness of the solution twice, before and after its introduction, requires the design of appropriate KPIs (Key Performance Indicators) (R02). If KPIs are not available or not sufficient to lead to sophisticated conclusions, other methods for measures shall be used instead, e.g., questionnaires.

To increase the probability of acceptance and market share and to overcome rigidness and stiffness (*P02*), the solution shall be easily transferable, adaptable and applicable by other supply chain participants (R03). Especially for small and medium-sized enterprises, a major decision factor is the overall cost of adopting the solution (*P14*). Therefore, it shall be affordable with regard of implementation and maintenance (R04) going along with low know-how prerequisites to handle and maintain the system (R05) as a lack of digital capabilities is a possible hurdle (*P13*).

Due to efforts on both sides, the solution shall provide mutual benefits by its usage (R06). In particular, this requirement is the background for the long-term need of a positive ROI (R01).

Table 4. Business requirements.

	ID	Name	Addressed P&B	Requirement's Origin
Model	R01	Positive ROI	P02, P09, P12, P14	E7, CM190731, CM190902
	R02	Appropriate KPIs	P05, P06, P14	WM190626, [38, 32]
	R03	Transferable, adaptable, applicable	P02, P08, P13	E2, E8, WM190618, CD, [39]
	R04	Low cost for implementation	P02, P08, P14	E1, E8, PM191128, [5, 40]
	R05	Low know-how requirements	P02, P08, P13	E1, E8, PM191128, [1]
	R06	Mutual benefits	P08, P09, P13	E3, CM190731, CD
Process	R07	Accessible, exchangeable, combinable	P04, P12, P14	E2, E4, E5, E8, [29]
	R08	Solve a specific problem	P11	E5, CM190729, CM191128, CD
	R09	Collaborative approach	P02, P07, P08, P10, P11, P13, P15	E1, E6, E8, E9, [3]
	R10	Foster trust	P01, P07, P09, P15	E1, E2, E3, E4, E5, E6, E7, E8, E9, CS190902, CM191212, CD, [3, 32]

Abbreviations: CD=Concept Document; P&B=Problems and Barriers; Other interaction points are coded as{Type}{Evidence}{Date} with Type:{C=Call | P=Physical Meeting | W=Workshop}, Evidence:{M=Minutes | N=Notes| S=Slides}, Date:{YYMMDD=Year Month Day}

Business processes Efficient utilization of data in business processes requires data to be easily accessible, exchangeable and combinable (R07), which overcomes barriers for future systems like a high effort to make these data available (*P12*). That means that domain experts without background in IT must be able to run data analyses, pull reports, or establish new data links. The scope of the software prototype, rather than being too general, shall focus on solving excellently a specific problem and not on solving mediocrely a wide array of general functions (R08). Next, the system shall follow a collaborative approach (R09) to steer processes from both sides, which gives a natural four-eye principle and reduces power positions (*P08*). Trust is one of the major attributes of a firm customer/supplier relationship. Especially, if it is desired to share sensitive data to overcome a lack of information (*P01*), a high level of trust is vital and shall be supported by system mechanisms (R10).

5.2. System requirements

System architecture In devising a software prototype to facilitate secure exchange of sensitive data, a significant and foundational architectural requirement is to ensure that no third-party has access to the data (R11). Subsequently, that implies that data shall be stored decentralized at the sender resp. the receiver (R12). These requirements tackle the problem of data breaches (*P16*), e.g., of Level One Robotics [36] where data of some of the most important car manufacturer were exposed. To prevent the danger of being dependent on and locked into one specific execution environment, the system shall be runnable on arbitrary environments (R13). That also complies with business rules, which could prohibit the usage of platforms like AWS (Amazon Web Services) or GCP (Google Cloud Platform). Although platform providers affirm that data are protected, data breaches or data misuse got revealed in the past, most commonly because of wrong configurations which lead to publicly exposed data sets. Still, platforms are the desired target-architecture, due to their characteristics, like ease of use, real-time abilities, scalability or instantly available updates. Therefore, platform features shall be provided (R14) to comply with decentralized storage (R12).

System policies and regulations The system shall provide mechanisms to define and technically enforce usage control policies (R15) on the data-receiver's side, which is the central approach for data sovereignty (see section 3). It can foster trust in each other and reduce risks being affected in data breaches (*P16*), e.g., when policies regarding deletion of data are applied. To secure legal aspects, the system shall provide functionalities to link usage policies with contractual definitions (R16). It is assumed that with usage control, different contractual and legal aspects can be resolved easier.

To further assist usage control mechanisms, the system shall support traceability of the data (R17), which means to provide detailed information about their origin, route through different systems and metadata, e.g., date and time of receipt, which is already required in GDPR-settings (General Data Protection Regulation) in the context of personal data. Furthermore, in settings where highly sensitive data are shared, the system shall provide functionalities for data access and usage logging in order to monitor and document the specific usage, also going along with GDPR specifications (R18). This means that it can be identified when, by whom and which data were accessed or used. These types of mechanisms are known from top-secured IT systems like in banking or secret-service sectors, where each action is logged to prevent misuse (*P15*). Generally preceding requirements like role and rights management are presupposed to provide access control mechanisms, e.g., with RBAC (Role-Based Access Control).

Table 5. System requirements.

	ID	Name	Addressed P&B	Requirement's Origin
Archit.	R11	No third-party data access	P15, P16	CS190902, CD
	R12	Decentralized data storage	P03, P15, P16	CD, [2]
	R13	Runnable on arbitrary environments	P08, P13, P14	CN190718, CD
	R14	Platform features	P05, P12, P13, P14	E1, E2, E3, E4, E5, E7, E8, [2]
Pol. & Reg.	R15	Usage control mechanisms	P15, P16	E1, E2, E3, E4, E5, E6, E7, E8, E9, WM190826, CM190902, CD
	R16	Link usage policies with contracts	P15, P16	WM190826, WS200129, CD
	R17	Traceability of data	P15, P16	E1, PM190513, PS191205, CD, [42]
	R18	Log data access and usage	P15, P16	CM190718, CM190813, CD
Funct.	R19	Precise connection configuration	P03, P15	WM190618, WM190626, CN190729, CN190820, PS191205, CD, [40]
	R20	Quick establishable connections	P01, P03, P12, P13	E1, CD
	R21	Real-time data exchange	P03	E6, PM190513, CD, [2, 29]
	R22	Agree mutually on connections	P05, P08, P15	WM190722, CM190731, PM190815, CD
Info. Mgt.	R23	Up-to-date and correct data	P05, P06	E5, CD, [29]
	R24	Accurate, consistent, complete data	P05, P06, P09, P10	CM190813, CD, [43]
	R25	Define data types precisely	P05, P06	CM190731, PS191205, CD, [40]
	R26	Standardized and structured formats	P04, P06, P12	E8, E9, WM190722, PM190902, [5, 43]
	R27	Machine-readable usage policies	P01, P05, P15	CS190902, CD
Security	R28	Mutually authenticate and authorize	P15, P16	CN200110, CD
	R29	No secretly changes of configuration	P07, P16	CD, [44]
	R30	Prevent malicious data extraction	P07, P15, P16	E3, E4, CS190902, CD
	R31	Prevent data misuse	P07, P15, P16	E1, E6, E7, E9, CM190902, CD, [32]
	R32	Data thriftiness	P07, P15	CM190731, CM190813, PS191205, CD
Interface	R33	Automatically exchange data	P03, P05, P06	E8, CD
	R34	Retrieve data from host systems	P05, P06	CN190312, WM190826, CD
	R35	Standardized API	P03, P04, P06, P12	E1, E5, WM190618, WM190826, PM191128, PS191205, CD
	R36	Combine usage policies and payload	P04, P15, P16	E8, PM191128, PS191205, CD
	R37	Provide a GUI with high usability	P13, P14	WM190626, PS191205, CD, [40, 32]

Abbreviations: CD=Concept Document; P&B=Problems and Barriers; Other interaction points are coded as{Type}{Evidence}{Date} with Type:{C=Call | P=Physical Meeting | W=Workshop}, Evidence:{M=Minutes | N=Notes| S=Slides}, Date:{YYMMDD=Year Month Day}

System functionalities The solution shall provide functionalities to precisely configure data connections (R19), which allows a fine granular parameterizability, e.g., times of a data exchange, validity of connections, exchanged data types, data granularities, time windows for which data are valid or usage policies. These connections shall quickly be establishable (R20) to support urgent incidents and make it unnecessary to bypass the system via "faster" exchange methods, like by sharing spreadsheets via email (*P03*).

Within incidents like bottlenecks and resulting phone or video-conference discussions, it is crucial to provide the most current data in order to have a common knowledge base. The system therefore shall allow a real-time data exchange to overcome issues outlined above as well as confidentiality issues due to sharing screens with front ends of internal IT systems (R21). Real-time in this context means that data are passed towards the data receiver with no pause in between, e.g., sending and receiving emails which will be read by the receiver with a delay. Furthermore, these data connections shall be mutually confirmed (R22), in order to ensure that the data provider is willing to share data and the data receiver is willing to respect according contractual and legal aspects (R16).

System information management First, data-quality aspects shall be respected (*P06*). This means in particular that data shall be up-to-date and correct (R23), which is why they shall be fetched directly from host systems (see in advance R34). The combination of these two aspects is crucial for a detailed analysis to derive business decisions. With real-time data, companies can manage processes more precisely within even shorter decision times frames, e.g., in just in time or just in sequence supply settings. Especially wrong or imprecise data entail the risk of ending up in more

inaccuracies than before, because the data receiver could rely on the provided data (*P05*), instead of generating e.g., more accurate forecasts by himself. Further usual quality aspects concerning a high level of detail, consistency and completeness of data shall be respected (R24). This allows solid conclusions for process-optimization, it supports system's integrity and prevents false decisions, based on misinterpretations of incomplete data. Further, it raises interest of business partners, to make use of the data, which could lead to new use cases (*P10*).

In order to make the system widely adoptable and to support data quality aspects, a precise definition of exchangeable data is essential to be provided (R25), since various deviating definitions and calculations of stock types (e.g., safety stocks and others) exist. Furthermore, these stock types vary from system to system, which aggravates the mapping problem of predefined types of stock (data interoperability). As a supporting requirement the system shall use standardized and structured data formats (R26) which makes them easily processable (*P04*). As previously stated, the system shall be able to enforce usage policies (R15), which is the reason for the requirement that usage policies shall be machine-readable and processable (R27).

System security In general, every-day security requirements like encryption of data transfers, regularly patched runtime environments or usage of strong passwords are presupposed. Firstly, systems shall mutually authenticate and authorize each other on data access (R28), which is the prerequisite for data traceability (R17). Aside from that, the data-providing system thereby gets the information which systems have received the data (R18). A second technical security-related requirement is that the system shall prevent a secretly change of data-connection configuration without knowledge of the affected data-connection partner (R29). Such a manipulation of configuration (*P07*) could e.g., concern the applied usage policies.

The system shall prevent unauthorized access and malicious data extraction (R30), which would violate requirements of data sovereignty (R15). The requirement targets two groups of persons. The first group are IT employees with physical access to the system like admins, who could be instructed by supervisors to give raw-access to the data. The second group are system users who try to bypass system features due to ignorance, like saving data for later usage, by copying data to local files or by taking screenshots. Due to the sensitivity of received data, the system shall prevent data misuse and restrict knowledge derivation (R31), e.g., to prevent conclusions regarding other customers or suppliers contracted, or conclusions about the degree of dependence on business partners (*P15*). In general, the system shall reduce data transmissions to necessary exchanges and reduce the scope of the data to the minimum required, in order to satisfy information demands for a specific task that results in the requirement to foster data thriftiness (R32). The importance of this requirement is high, due to its strong supporting character for other requirements like mitigating impacts of malicious data extractions (R30) or fostering trust of a solution (R10). At the end it also provides a sense of security for data receivers, not having too much information.

System interface We distinguish between the system interface on API level and a GUI (Graphical User Interface) for users. In the context of the API level, the system shall be able to exchange data automatically and provide them on request (R33) to overcome a manual exchange (*P03*). Even if requirements should not be merged with design decisions, the reader shall recognize that this requirement especially applies in data-pull scenarios, which are preferred over data-push scenarios, which would violate the data thriftiness requirement (R32). To allow a real-time accessing of up-to-date data and to avoid the necessity of manual input eventually leading to mistakes (*P05*), the system shall have an API-based access to root systems of requested data (R34). Furthermore, an API shall be provided (R35) to allow data access from specialized company-internal systems, e.g., for analyzing purposes (*P12*). To allow other systems to comply and enforce policies, data shall be transmitted together with usage policies (R36). In conjunction with the requirement of traceability (R17), the eligibility of the data flow through different systems can be validated at each point.

For user interactions with the system, a GUI shall be provided (R37), which also is a consequence of the requirement to provide access to exchanged data (R35). The GUI shall comply with well-established usability principles like ease of use or clarity on system feedback to support adoption and overcome rigidness and stiffness (*P02*). Several advantages arise from a GUI equipped system. Firstly it allows a direct usage of the system prior to necessary adjustments of the internal system landscape, to work with the newly available sensitive data. Also companies with limited digital capabilities (*P13*) or in cases where the benefit of integration does not prevail the necessary effort (*P14*), advantages can be drawn from an integrated GUI. Another big advantage is that the system could enforce usage policies in this GUI, which makes the data usable whilst maintaining one of the strictest usage policies to prohibit the use of data outside of the system boundaries.

6. Discussion

Surprisingly, a prevailing issue is the continuous use of traditional communication channels, such as fax machines. The identified requirements have a strong bias towards data

sovereignty and usage control, which is the key mechanism to foster trust in the single-case study and consequently gain transparency. Overall the requirements match with other requirement elicitations for inter-organizational data exchange like [5, 29, 40]. The requirement's elicitation process also showed that today's product features like those of platforms (e.g., real-time ability, collaboration approaches, etc.) are implicitly assumed. Therefore, such requirements like the mentioned real-time data requirement are rarely mentioned in interviews, but need to be considered of course.

Naturally, our study is subject to limitations. First and foremost, our research only covers one particular bilateral relationship within an automotive supply chain, in particular the alliance between an OEM and the according Tier 1 supplier. This focus has implications as, usually, Tier-n ($n > 1$) suppliers have multiple customers for a specific product, with whom also supplier-stocks are shared with. Thus, the study only claims to rely on findings that are relevant for the specific characteristic relationship between OEM and Tier 1 supplier, with a product exclusively produced for this OEM. Next, our study does not cover legal aspects of inter-organizational data exchange, as it is still an ongoing investigation to uncover settings and boundaries for the legal exchange of sensitive data. Lastly, we only rely on one deep single-case study, expert interviews and literature, which is just one view on the subject of sensitive data exchange.

A first evaluation of the requirements is current objective of the ongoing single-case study, where the requirements were used to guide the development of the software prototype, which is currently piloted. From the current point of view the requirements fit adequately the needs and the aimed goal of an exchange of sensitive data. A profound evaluation with examination of different design aspects with ADR's required derivation of design principles is a part of future studies.

Even though our work is strongly inspired by practice, it provides multiple scientific implications. It contributes to extending the emerging and relevant field of data sovereignty, by argumentation how data sovereignty can foster trust which is needed to overcome barriers of sharing sensitive data. Secondly the requirements are built on a holistic view in order to be directly adopted by other researchers and practitioners setting up new inter-organizational information systems.

7. Conclusion

Our study revealed a comprehensive array of requirements for the inter-organizational exchange of sensitive data. These data are exchangeable from a technical and legal point of view, but whose exchange is generally not desirable due to mistrust or other concerns. The requirements to overcome these reservations and to allow their exchange, are structured alongside accepted standards and are classified dichotomously into business and system requirements. The findings were derived from a deep single-case study within the automotive supply chain, expert interviews and literature review.

The identified 37 requirements focus on different necessary aspects for productive use of a data exchanging system. Aspects relate for example to applicability, in order to enable the usage for a broad variety of supply chain participants, feasibility, to use resulting benefits in business processes, or foster trust by data sovereignty with the support of usage control.

Further research will cover the evaluation of the practical use of the requirements in the ongoing pilot of the single-case's prototype.

Acknowledgements This work has been partially funded by the Fraunhofer-Cluster of Excellence Cognitive Internet Technologies.

References

[1] W. Kersten, M. Seiter, B. von See, N. Hackius, and T. Maurer, *Chancen der digitalen Transformation: Trends und Strategien in Logistik und Supply Chain Management*. Hamburg: DVV Media Group GmbH, 2017.

[2] P. Farahani, C. Meier, and J. Wilke, "Digital supply chain management agenda for the automotive supplier industry," in *Shaping the Digital Enterprise* (G. Oswald and M. Kleinemeier, eds.), pp. 157–172, Cham: Springer, 2017.

[3] W. Ahmed and M. Omar, "Drivers of supply chain transparency and its effects on performance measures in the automotive industry: Case of a developing country," *International Journal of Services and Operations Management*, vol. 33, no. 2, pp. 159–186, 2019.

[4] Z. Lotfi, M. Mukhtar, S. Sahran, and A. T. Zadeh, "Information sharing in supply chain management," *Procedia Technology*, vol. 11, pp. 298–304, 2013.

[5] J. Zrenner, F. O. Möller, C. Jung, A. Eitel, and B. Otto, "Usage control architecture options for data sovereignty in business ecosystems," *Journal of Enterprise Information Management*, vol. 32, no. 3, pp. 477–495, 2019.

[6] Automotive Industry Action Group, "The future of the automotive supply chain: Part 2 of 3: Supply chain professionals in the americas and europe share their insights and expectations," 2019.

[7] Å. A. Nyre and M. G. Jaatun, "Usage control in inter-organisational collaborative environments – a case study from an industry perspective," in *Multidisciplinary Research and Practice for Information Systems* (G. Quirchmayr, J. Basl, I. You, L. Xu, and E. Weippl, eds.), vol. 7465, (Berlin), pp. 317–331, Springer, 2012.

[8] R. Ostertag, *Supply-Chain-Koordination im Auslauf in der Automobilindustrie: Koordinationsmodell auf Basis von Fortschrittszahlen zur dezentralen Planung bei zentraler Informationsbereitstellung*. Gabler Edition Wissenschaft, Wiesbaden: Gabler, 1 ed., 2008.

[9] L. Li, "Information sharing in a supply chain with horizontal competition," *Management Science*, vol. 48, no. 9, pp. 1196–1212, 2002.

[10] R. Wong, "Data protection online: Alternative approaches to sensitive data?," *Journal of International Commercial Law and Technology*, vol. 2, no. 1, pp. 9–16, 2007.

[11] J. Park and R. Sandhu, "The ucon abc usage control model," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 128–174, 2004.

[12] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," *MIS Quarterly*, vol. 35, no. 1, pp. 37–56, 2011.

[13] U. Flick, *An Introduction to qualitative Research*. London: SAGE Publications Ltd, 4 ed., 2009.

[14] H.-G. Ridder, "The theory contribution of case study research designs," *Business Research*, vol. 10, no. 2, pp. 281–305, 2017.

[15] J. Gerring, *Case Study Research: Principles and Practices*. Cambridge: Cambridge University Press, 2 ed., 2017.

[16] J. González-Benito, G. Lannelongue, and J. A. Alfaro-Tanco, "Study of supply-chain management in the automotive industry: A bibliometric analysis," *International Journal of Production Research*, vol. 51, no. 13, pp. 3849–3863, 2013.

[17] M. D. Myers and M. Newman, "The qualitative interview in is research: Examining the craft," *Information and Organization*, vol. 17, no. 1, pp. 2–26, 2007.

[18] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS Quarterly*, vol. 26, no. 2, pp. 13–23, 2002.

[19] D. R. Mackay, "The impact of edi on the components sector of the australian automotive industry," *The Journal of Strategic Information Systems*, vol. 2, no. 3, pp. 243–263, 1993.

[20] Odette International Ltd, "Oftp2 explained," 2009.

[21] Association of the German Automotive Industry, "Vda 4984: Data transfer of delivery instructions," 2018.

[22] F. B. Vernadat, "Enterprise integration and interoperability," in *Springer Handbook of Automation* (S. Y. Nof, ed.), Berlin, Heidelberg: Springer, 2009.

[23] G. Dudek, *Collaborative Planning in Supply Chains: A Negotiation-Based Approach*. Berlin: Springer, 2004.

[24] N. Kumar, "The power of trust in manufacturer-retailer relationships," *Harvard Business Review*, vol. 74, no. 6, pp. 92–106, 1996.

[25] M. Jarke, B. Otto, and S. Ram, "Data sovereignty and data space ecosystems," *Business & Information Systems Engineering*, vol. 61, no. 5, pp. 549–550, 2019.

[26] R. S. Sandhu and P. Samarati, "Access control: Principle and practice," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[27] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, no. 2, pp. 81–99, 2010.

[28] M. J. Atallah, H. G. Elmongui, V. Deshpande, and L. B. Schwarz, "Secure supply-chain protocols," in *EEE International Conference on E-Commerce*, pp. 293–302, 2003.

[29] A.-C. Tietze, J. Cirullies, and B. Otto, "Automotive supply-chain requirements for a time-critical knowledge management," in *Digitalization in supply chain management and logistics* (W. Kersten, T. Blecker, and C. M. Ringle, eds.), (Berlin), pp. 467–489, epubli, 2017.

[30] Automotive Industry Action Group, "The future of the automotive supply chain: Part 1 of 3: Asia-pacific supply chain professionals share their insights and expectations," 2019.

[31] Harvard Business Review, "An inflection point for the data-driven enterprise," 2018.

[32] T. Enders, D. Martin, G. G. Sehgal, and R. Schüritz, "Igniting the spark: Overcoming organizational change resistance to advance innovation adoption - the case of data-driven services," in *Exploring Service Science* (H. Nóvoa, M. Drăgoicea, and N. Kühl, eds.), vol. 377 of *Lecture Notes in Business Information Processing*, pp. 217–230, Cham: Springer, 2020.

[33] K. Bouchbout and Z. Alimazighi, "A framework for identifying the critical factors affecting the decision to adopt and use inter-organizational information systems," *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, vol. 2, no. 7, 2008.

[34] M. K. Khurana, P. K. Mishra, and A. R. Singh, "Barriers to information sharing in supply chain of manufacturing industries," *International Journal of Manufacturing Systems*, vol. 1, no. 1, pp. 9–29, 2011.

[35] T. A. Leopold, V. S. Ratcheva, and S. Zahidi, *The future of jobs report 2018*. Cologny: World Economic Forum, 2018.

[36] S. Cowley, "Big red flag: Automakers' trade secrets exposed in data leak." The New York Times, 2018.

[37] ISO/IEC/IEEE, "Systems and software engineering – life cycle processes – requirements engineering (29148:2018(e))," 2018.

[38] O. Kohnke, "It's not just about technology: The people side of digitization," in *Shaping the Digital Enterprise* (G. Oswald and M. Kleinemeier, eds.), pp. 69–91, Cham: Springer International Publishing, 2017.

[39] R. Rajaguru and M. J. Matanda, "Effects of inter-organizational compatibility on supply chain capabilities: Exploring the mediating role of inter-organizational information systems (iois) integration," *Industrial Marketing Management*, vol. 42, no. 4, pp. 620–632, 2013.

[40] C. Siemen, N. Clever, B. Barann, and J. Becker, "Requirements elicitation for an inter-organizational business intelligence system for small and medium retail enterprises," in *20th Conference on Business Informatics*, (Vienna), pp. 129–138, 2018.

[41] A. Osterwalder, Y. Pigneur, and C. L. Tucci, "Clarifying business models: Origins, present, and future of the concept," *Communications of the Association for Information Systems*, vol. 16, pp. 1–25, 2005.

[42] J. Willemson and A. Ansper, "A secure and scalable infrastructure for inter-organizational data exchange and egovernment applications," in *3rd International Conference on Availability, Reliability and Security*, (Barcelona), pp. 572–577, 2008.

[43] C. Falge, B. Otto, and H. Österle, "Data quality requirements of collaborative business processes," in *45th Hawaii International Conference on System Sciences*, (Maui), pp. 4316–4325, 2012.

[44] N. Menz, A. Resetko, and S. Wessel, "Criteria catalogue for components - connector." International Data Spaces Association, 2020.