*sustainability*

MDPI

*Article*

# Managing the Tension between Trust and Confidentiality in Mobile Supply Chains

**Nassim Ghondaghsaz [1,2,*], Zarina Chokparova [1,3], Sven Engesser [2] and Leon Urbas [3]**

[1] Boysen-TU Dresden-Research Training Group, Technische Universität Dresden, 01187 Dresden, Germany; zarina.chokparova@tu-dresden.de
[2] Institute of Media and Communication Science, Technische Universität Dresden, 01069 Dresden, Germany; sven.engesser@tu-dresden.de
[3] Process Control Systems and Process Systems Engineering Group, Technische Universität Dresden, 01069 Dresden, Germany; leon.urbas@tu-dresden.de
* Correspondence: nassim.ghondaghsaz@tu-dresden.de

**Abstract:** This research investigates the tension between trust and confidentiality in Mobile Supply Chains (MSCs), where a production asset that is owned by one of the partners is outsourced to another partner of the supply chain for the production of goods, chemicals, or pharmaceuticals. The novelty of the MSC concept is to be found in its innovative and sustainable approach to production and operation processes in supply chains. Implementation of the MSC model could, however, raise trust and confidentiality concerns. The interplay of trust and confidentiality, or preservation of information privacy, between partners plays a central role in the supply chains, particularly because they are genuinely dependent on each other. Qualitative data analysis was used, in which semi-structured interviews with the experts from the chemical and pharmaceutical industries in Germany were conducted to investigate the tension between trust and confidentiality, and important factors affecting it. The results of the study present four different integration scenarios, namely, the low-quality, conservative, grey-box, and innovation scenarios, which consider different levels of trust, confidentiality and information sharing. Subsequently, the tension between trust and confidentiality is analyzed within these scenarios, and three effective strategies which encourage partners to balance the tension between trust and confidentiality are proposed. The study indicates that the balance between trust and confidentiality can be maintained in some scenarios when critical factors such as transparency, trust negotiation, and a reward-sharing system are present.

**Keywords:** information sharing; trust; confidentiality; mobile supply chains; mobile factory; sustainability; mobility



**Citation:** Ghondaghsaz, N.; Chokparova, Z.; Engesser, S.; Urbas, L. Managing the Tension between Trust and Confidentiality in Mobile Supply Chains. *Sustainability* **2022**, *14*, 2347. https://doi.org/10.3390/su14042347

Academic Editor: Jozsef Mezei

Received: 22 December 2021
Accepted: 15 February 2022
Published: 18 February 2022



## 1. Introduction

Mobile Supply Chains (MSCs) contribute to developing sustainable production and transportation patterns, creating resilience in infrastructure, increasing mobility, and maintaining sustainable industrialization. MSCs are value creation systems that aim to reduce greenhouse gas emissions caused by the complete life cycle of products from start to finish [1]. They can be defined as more advanced supply chains that satisfy the demand for mobility and flexibility in producing and distributing goods. Thereby, this approach supports the 9th and 12th Goals for Sustainable Development formulated by the UN in 2015 [2], which relate to "industry, innovation and infrastructure" and "responsible consumption and production", respectively. MSCs provide not only transportation of raw materials and goods, but allow for the optimized relocation of production facilities and services between partners within a collaboration. Owing to the modularization and mobility of the manufacturing units, the degree of customization for products and process intensification that can be achieved, and the level to which transpiration efforts can be reduced. Movable production assets can be outsourced from one MSC partner to another

to fulfill their individual process needs and achieve sustainable operation and distribution of available resources.

Several stakeholders with different goals and missions need to cooperate in implementing MSCs, which can cause various challenges and requirements when production facilities are moved between the sites of different supply chain partners. To maintain a sustainable relationship between the partners of a mobile supply chain and its effective operation, a balance of trust in the partnership and a high level of confidentiality in the use of shared information within the cooperation is important. A trusting relationship could imply full disclosure of information by partners; however, the diversity in the nature of the confidential or proprietary information being shared is relatively large, including process inputs, operation conditions, control parameters, etc., all of which can be considered sensitive information. Similarly, trust and confidentiality concepts have been perceived to be profoundly interdependent elements in various research topics and areas of application. Specifically, this interconnection has been a subject of interest in supply chain collaborations [3], business knowledge management [4], project team environments [5], survey and experiment design [6] and even legal mediations [7].

Trust is required for building long-term strategic partner relationships in supply chains [8]. It is understood that the sharing of information [9], resources, knowledge, and assets takes place during the collaboration of supply chain partners [10]. Trust is described as an assumption of positive consequence derived from another party under some amount of uncertainty. It is associated with the calculation of anticipated risks caused by cheating actions of a supply chain partner and forecasting their behavior under different conditions [11]. There are numerous approaches to measuring trust and the risks related to threats and uncertainties within the relationship between parties in collaboration [9]. A certain level of predictability is needed to create a trusting environment and to reduce uncertainty [12]. In addition, an adequate level of communication between partners is necessary. Therefore, the trustworthiness of a partner could also be defined by their reliability, predictability, benevolence, and competence [13]. In addition, trust can be used to interpret the intentions of parties during the mutual exploitation of assets and services. Other factors, such as material shortages and shorter service periods, affect the ability of partners to meet the obligations of product supply or procurement under critical conditions [8]. Long-term trust, which has been tested by previous experience and reinforced by established reputations, could also be transferable from one source to another [14]. From the information perspective, trust facilitates the management of information security in the hierarchies of companies [12].

With the digital transformation and expansion of technological power in businessess and management of logistics, the issue of information confidentiality preservation is receiving increased attention. Digital assets are a valuable part of modern supply chains, including geographically dispersed operations, outsourcing practices, telecommuting, and freelance services [15]. Product data, technology, and know-how about processes and services are subjects related to intellectual property protection [16]. Due to the important role of data in production and operation management, the confidentiality of the information shared in supply chains should be protected. Moreover, the risks and balancing of costs and quality with regards to confidentiality need to be evaluated. The term confidentiality covers the disclosure [17] and security of information [3], protection of intellectual property, and cybersecurity [18]. In the case of mobile supply chains, the emphasis is set on the confidentiality of both physical and digital assets that are associated with them and the corresponding added value, control methods, and operational and maintenance costs. Security is one of the main knowledge management challenges that corporations encounter when sharing their resources and competencies. Strategies for the management of intellectual property, trade secrets, and the transferring and sharing of knowledge are tightly related to trust establishment between collaborators, and the development of privacy policies for shared sensitive information [4].

Multiple process, production, and distribution agents can constitute an MSC, and each operation for such collaborations requires continuous information and experience exchange. For example, when one MSC partner is operating the production equipment of another partner, the former needs exact and reliable information on the operation of that unit, while the latter might request or monitor usage and consumption data necessary for proper operation and the maintenance of safety. The amount of information they would actually share with each other depends on the trust between these parties, and the quantity of undisclosed or encoded information reflects the confidentiality level in their relationship [4]. Thus, one of the problems of mobile supply chains is the balancing of the tension between trust and confidentiality while preserving the flexibility, adaptability, quality level, innovation, and resilience of MSCs. Higher extents of information sharing could incur more awareness of and focus on security [19]. As a result, companies need to keep information sharing and information privacy levels in equilibrium. The interplay of trust and the confidentiality of shared information [5] describes the willingness of the supplier to disclose secret information with its customer. This can ensure that one party is ready to expose its vulnerabilities and accept the related risks and costs of information misuse. The intentional provision of access to confidential information for another party signals a level of benevolence of the party's intentions [20]. Thus, considering the commitment of partners to the relationship under the competing effects of influencing factors, the bond between supply chain partners can be nurtured over time [21].

The interplay of trust (T) and confidentiality (C), or privacy, between partners fulfills a central role in value-creating chains, particularly because they are genuinely dependent on each other. Due to the research gap of the T–C relationship in MSCs, it is important to study both terms individually and collectively in supply chain literature and to use a qualitative data collection approach.To the best of our knowledge, few researchers have addressed the tension between trust and confidentiality while considering the intervening effect of information sharing. Numerous investigations have highlighted the positive relationship between trust and information sharing [22,23], whereas others focused on confidentiality and information sharing [24–26]. However, a need exists for a comprehensive investigation that combines these three indicators in collaboration systems and elaborates on the tension between trust and confidentiality while considering the level of information sharing in MSCs. Therefore, the research questions (RQs) in this paper are as follows:

RQ1: What is the tension between trust and confidentiality in MSCs when various information sharing scenarios are involved?

RQ2: What are the applicable strategies for balancing the tension between trust and confidentiality in MSCs?

In this paper, we adopted a qualitative form of data analysis through semi-structured interviews with experts from the chemical, process, and pharmaceutical industries in Germany, and present a framework for the interconnection of trust and confidentiality through various integration scenarios. Moreover, three strategies are recommended which show promise in balancing the tension between trust and confidentiality.

The result of this study contributes to the literature by covering collaboration and integration systems in supply chain management, adding to the literature of integration scenarios, and presenting three critical strategies. In addition, from a managerial and practical perspective, this study augments the toolsets of practitioners and managers by providing decision-making criteria and pragmatic insights with recommendations to balance trust and confidentiality within the scope of implementation and integration of MSCs by partners.

This paper is organized as follows. Section 2 provides the background literature on trust, confidentiality, and their relationship, and explains the mobile supply chain concept. Section 3 presents the detailed methodology used for conducting this research and its limitations. Section 4 includes results and a discussion that contains a qualitative analysis and the identification of strategies for balancing T–C tension. Finally, Section 5

concludes this work with an outline of the contributions, implications, and remarks on future research directions.

## 2. Theoretical Background

This section provides background information related to the MSC concept, as well as an overview of trust, confidentiality, and their interconnection in supply chain management and collaborative environments.

### *2.1. Trust*

Trust is a complicated communication phenomenon with various dimensions and facets. This results in various definitions of trust in different disciplines. From a management perspective, most researchers emphasized goodwill and the benevolence aspects of trust [27–29]. The study in [29] suggested that trust is the confident prospect that a partner will perform as promised according to the trustor's expectation. According to seminal studies in the marketing field, trust is defined as the confidence of one party in the integrity, reliability, and sincerity of another party [30,31]. From the supply chain perspective [32], trust is described as the extent to which relationship partners perceive each other as credible and benevolent. Lee and Zhong [33] considered the credibility and benevolence aspects of trust in supply chain relationships when two stakeholders are collaborating. Credibility is associated with the ability of performing to promises, while benevolence reflects the consideration of the interests and welfare of the partners.

In some supply chain studies, trust has been examined through various categories and levels. For instance, Wu et al. [34] classified trust into calculated trust and relational trust. They argue that calculative trust exists when partners are investigating and negotiating contracts and written agreements. This category is the initial trust among partners after signing the contract. After continuous interactions of partners over time, relational trust will be established. Akrout and Diallo [35] categorized trust as calculative trust, cognitive trust, and affective trust. Here, calculative trust has the same meaning as in the study of [34], while cognitive trust is related to the confidence in the partner's performance through accurate information exchange without monitoring, and affective trust is based on interpersonal and emotional connections developed after repeated positive experiences in long-term relationships. According to [36], trust is a pre-requisite for a mutual, interdependent, and beneficial relationship where both parties are committed to each other's long-term interests or benefits. Ryciuk [37] defined inter-organizational trust as an uncertain situation in which one relies on the partner and hopes that the partner will not develop opportunistic behaviors. They argued that trust does not exist when future events are certain and under control. Therefore, trust is defined as a willingness to expose yourself to risk [37–39]. Multiple studies have found five specific types of trust: general, interpersonal, intra-firm, inter-organizational, and individual-to-firm trust [27]. Economists usually define trust according to transaction costs and game theory [34,40,41].

In previous studies, different factors and outcomes for better understanding the development and maintenance of trust have been evaluated [39]. Chen et al. [42] identified a positive relationship between trust and four factors, namely, information quality, information availability, information sharing, and behavioral uncertainty. Information quality is defined as the ability to fulfill both the specified and indirect demands of the recipient of information. Various dimensions for analyzing the quality of information have been suggested, such as inherent aspects (timeliness, reliability, completeness, concision, validity, security, etc.) and pragmatic dimensions (relevance, accessibility, credibility, understandability, ease of operations, etc.) [43]. The development process of trust in information can occur through predictions that are based on past behaviors of the information source [44]. With regards to information quality, trustworthiness can be used for the assessment of information trust. Confidence is one of the components of trust, and also refers to information quality through validity and reliability. As a result, trust has been identified as a mediating component between information quality and information usage. High information quality

has a positive impact on trust and can indicate beneficial intentions of partners [45]. Thus, the willingness towards information exchange increases. In addition, high information quality enhances transparency and reduces the risk of opportunism.

A study by [37] shows that partner characteristics (reputation of high product quality and a stable financial situation, as well being a well-known brand), relationship formalization (contracts), and poor bargaining positions are factors of trust. Cooperation, goodwill manifestation, and specific investments are positive results of building and maintaining trust. Trust in inter-organizational relationships contributes to efficient cooperation, resulting in open communication [41,46,47]. Moreover, it has been argued that trust is not only a desirable feature but a necessary one for establishing a collaborative environment in supply chains [27,36].

### *2.2. Confidentiality and Information Privacy*

Confidential information is a secret that has been shared or entrusted under the condition of non-disclosure to a third party [5]. Confidentiality aims to limit disclosure of proprietary information and to restrict the access of unauthorized parties. In supply chain networks, the confidentiality and integrity of information are essential components of the system [48]. In industries marked by intense competition, many information types that are provided by suppliers in supply chains require confidentiality protection. The term confidentiality is also closely related to information security. The management of information security is a critical challenge in collaborative environments [49], including supply chains. The cost of handling breaches of information security increases with the rising complexity of information environments and the sophistication of modern security attacks. Some confidentiality preserving solutions are based on the limitation of information access. For instance, the Bell–LaPadula model uses level controls to deny access to higher level information by the lower level partners [50]. Another example is the Brewer and Nash model, or Chinese Wall model, which attempts to intercept conflict of interest issues between organizations [51].

Confidentiality is important in information sharing, collaborative planning, and forecasting across the supply chain [52]. Supply chain parties can determine their confidentiality policies by limiting the exchange of information. Absence of confidentiality in a supply chain is impractical, because it does not provide joint benefit to all involved parties. Supply chain partners consider confidential information exchange as a way of meeting mutual expectations and acting as good collaborators [53]. According to [54], confidential information might contain commercial or industrial information, information confidential by law, information preserving legitimate economic interests, and other types of information that could cause harm if disclosed. Commercial information includes some activities or trades associated with profit, for instance proprietary information on production rates, demand values at specific sites, number of available trucks and their capacity, etc. [10]. Industrial information describes processes, including raw materials, manufacturing sequences, and production methods. Certain combinations of commercial and industrial information protected by common law can be treated as trade secrets [54]. Usually, disclosure of such information is limited to specific persons within the organization. It can contain particular methods, recipes, or formulas, which provide the holders with a competitive advantage in the market.

There are various techniques to maintaining the confidentiality of information in supply chain collaborations. They include privacy-preserving techniques, such as the use of a trusted third party [55], secure multiparty computation (SMC) [53], secure transformation [10], cryptographic techniques [53,56], etc. One of the industry practices aimed at preserving confidentiality of digital assets and their intellectual property within the supply chain network is the use of blockchain technology for the transmission and recording of the transaction history, validation and authentication of documents, and maintaining traceability [15]. Nevertheless, such technology might require additional defense mechanisms against attacks to avoid loss, manipulation, or theft of the information. Another way of

maintaining confidentiality is to strategically partition the information into categories of private and public information and distribute it according to the respective access status. In [24] it is suggested that the information status, i.e., having a secret, can be disclosed, whereas the information content, i.e., the secret itself, should be kept confidential. Regarding SMC, this protocol defines a provably secure communication between supply chain collaboration partners. Each party could define specific constraints that are considered while solving scheduling problems using privacy-preserving algorithms. As a result, none of the parties are expected to receive any information about inputs and outputs other than their own. However, due to the increasing complexity and size of the combinatorial functions used in computation, an SMC scheme could be inefficient and provide only limited security [57]. Another technique is based on obfuscation of private and sensitive information by representing them in a randomized sequence when sharing with other partners [10]. This prevents leakage of the proprietary information and allows computations of the jointly required outcome. Other solutions often proposed for supply chain management are homomorphic encryption schemes, which allow computation to be performed on encrypted data, and blockchain-based algorithms [58]. Due to the availability of a large variety of applicable methods for preserving confidentiality, each case of collaboration should be treated individually according to their demands in order to find a usable and efficient privacy-preserving tool.

### *2.3. Tension between Trust and Confidentiality*

Information is critical in supply chains and its value is defined by the status difference prior to and after access to the information [59]. Shared information can be classified according to the level of value and the level of sensitivity. The value can be represented by its utility, or the role in reducing uncertainty, and total costs incurred during the value creation process. The sensitivity of information quantifies negative impacts and damages due to information loss or exposure. When looking to share information across a supply chain, it is important to plan data protection measures to secure intellectual property and trade secrets [60]. As a result, ownership of shared data, data handling, and its consistency remain central concerns in a collaborative environment.

In some supply chain collaborations, certain parties may refuse to share information due to confidentiality concerns or lack of trust [61]. Building trust in a supply chain is an action which necessitates continuous commitment from the involved parties. Lack of trust would discourage partners from establishing a collaboration in spite of forecasted financial benefits. Thus, the risks imposed by initiating trust could be considered a threshold boundary which could be passed by sharing information forecasts or forecasting methods.

Secure information sharing is expected to have a positive impact on trust in a collaborative environment [19]. An increased amount of sharing requires higher attention to the security of the information. Therefore, the information sharing and confidentiality level between collaborating companies should be balanced. High information sharing might include the disclosure of financial reports, production schedules, and inventory data. Moreover, advanced production data and industrial decisions, including scheduling, logistics, and supply, could be aggregated and shared via IoT services [62]. Therefore, the relation between trust and confidentiality can be drawn through dependency on information sharing. The initiatives directed at securing information, including prevention of unauthorized access in supply chain collaborations, help to preserve the confidentiality of information and benefit supply chain intelligence [63]. Thus, confidentiality is regarded as a significant factor for setting up trust and sharing sensitive information between partners of a supply chain [11].

The relationship between trust and confidentiality is complex and intricate. Methods for maintaining trust and confidentiality have been proposed for application in supply chain collaborations. To contribute to building a trustful collaboration, a certain degree of transparency and clarity of information is required [29]. For this purpose, partners are recommended to increase the frequency of communication and develop documentation

and confidentiality agreements. Such agreements act as a binding tool that can prevent the leakage of information and encourages sharing between supply chain partners [64]. Most research in recent years has focused on information sharing as a significant factor for initiating and maintaining trust among supply chains partners [65]. The supply chain literature is replete with discussions on the benefits of sharing information, as well as the positive effect of that on trust in supply chains. It is generally accepted that less information sharing can result in less mutual trust [66]. Therefore, when one party refrains from sharing a certain amount of information due to confidentiality reasons, the other party loses trust in the partner because it does not signal the integrity and benevolence of that party.

### *2.4. Mobile Supply Chains*

Globalization has imposed high demands on the effective coordination of material and information flows in traditional supply chains [67]. Supply chain management aims to maximize the efficiency of manufacturing and delivery across the network. Striving for sustainability, customization, process intensification, and modularity have affected the status quo of traditional networks by introducing the possibility to mobilize production. Owing to technological improvements, the relocation of production setups [68], or their further integration in existing setups, the locational availability of products increases. Moreover, this reduces transportation efforts required for the delivery of materials and diversifies contributing parties. There are multiple such solutions being practiced in industry, including mobile manufacturing [69], reconfigurable manufacturing [70], Factory-in-a-box [71], location independent manufacturing [72], modular production [73], etc.

All these movable production solutions can represent the idea of mobile supply chains (MSCs). MSCs are value creation systems that aim to reduce greenhouse gas emissions caused by the complete life cycle of products from start to finish [1]. The global goal pursued by the concept of mobile supply chains is the sustainable production, distribution, and consumption of goods that can be achieved by the mobilization of stationary production resources. Apart from that, MSCs are expected to reach maximum efficiency through the reliable, fast, and low-cost adaptation of process decisions on site. Mobile supply chains [1] represent the idea of efficiently relocatable assets for the production of goods or their storage, and they are capable of adapting to changing demand and adjusting the transportation scheduling accordingly. The mobile production assets can be relocated to different manufacturing sites and adjusted to fit other systems.

Due to their modularity, the process units could be easily combined to fit the needed demand of various production locations. There are multiple features that modular manufacturing facilities could provide for the improved management of mobile supply chains. Adjustment of production amounts in accordance with capacity, performing process changes on site, and the relocation of containers offer improved short-term flexibility. The change of manufacturing capacity itself, process modifications, and the transportation of modules to different locations are advantages connected to long-term flexibility [74]. Subsequent categorization of flexibility drivers reveals mobility in production facilities and value chains. Since MSC components may represent a container or a set of containers, transportation from one site to another depending on customer requirements or resources means that the location of the containers should remain flexible [75]. Moreover, an opportunity to produce goods during transportation should not be neglected. Another aspect of modular production is scalability. Changing production capacity can be implemented simply with a concept of scaling up or down the number of facilities or producing modules [76]. Due to the standardization of production modules and their interfaces, processes could easily be reconfigured, and units could be replaced and reordered. Such a universal approach provides the foundation for a transformable plants concept [74].

Mobile supply chain or value chain concepts can find application in various industries, including chemical, process, pharmaceutical, food, etc. To describe the material and information flows in MSCs, roles and duties of the involved partners should be clarified. Figure 1 shows the interaction between MSC partners. The asset provider is a manufacturer

and provider of the process equipment, and the asset operator is a user of this equipment in their production or process. An asset operator receives a module or operating unit from the asset provider, and integrates it into their process sequence for the production of intermediate products, improvement of their process efficiency, or other process operation procedures. Therefore, this interaction causes the partners to exchange information about raw materials, operating conditions, or equipment parameters and indicators. The orchestration of information necessary for the operation and control of the assets is exchanged through the communication layer [77]. It can be assumed that such a system requires a certain extent of trust between asset providers and operators. In addition, such collaboration and operation of assets in a value creating chain would require confidentiality protection of the exchanged and shared information [78].

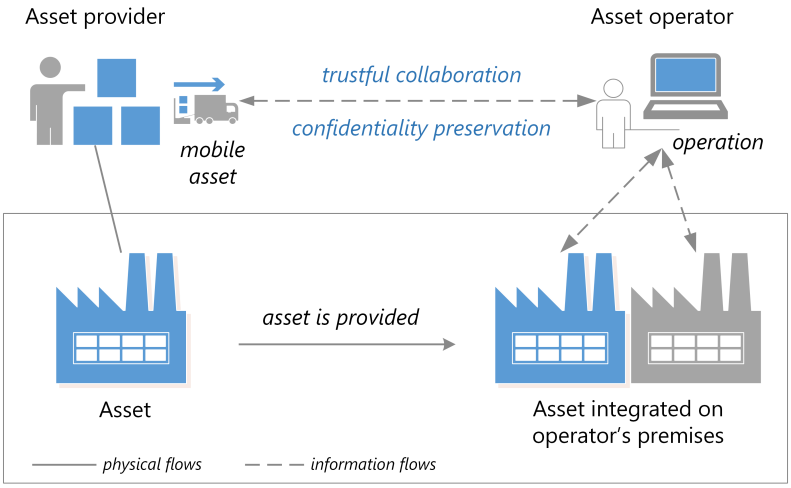


**Figure 1.** Integration between mobile supply chain partners.

Due to recent advances in information technology, the necessary data can be shared quickly and efficiently and provide information visibility in the collaborative environment [61]. Providing information about the products and services within the supply chain could decrease the uncertainty about predicted demand. Managing information for planning and production requires coordination and trust between traditional supply chain agents. In MSCs, the information sharing could appear to be a more complex task due to the flexibility of relocation and due to shared control over the assets. Therefore, collaborative trust and confidentiality concerns in MSCs and their mutual relationships are investigated further.

## 3. Methodology

In this study, we attempt to identify significant strategies for balancing the tension between trust and confidentiality for building secure and trusting relationships among mobile supply chain partners. We concentrate on the human side of collaboration since it is fundamentally dependent on rational relationships [29,79]. Collaboration is an evolving process in which two or more social entities actively collaborate to achieve a common objective [80]. It is not a linear process; it entails the reciprocal and active participation of all interrelated components and constitutes a series of interpersonal interactions [29]. As a result, the goal of this study is to investigate and comprehend the issue in depth by studying the interviewees' behaviors and relationships. We want to show the viewpoints of experts who are responsible for supply chains by investigating their experiences, beliefs, and perspectives of business strategies to understand how they manage trust and confidentiality in their collaboration processes. As a result, we decided to conduct a qualitative method, which is consistent with previous studies in the same context [29,81]. This method helps researchers to investigate and analyze the phenomena in detail according to the real experiences and views of various participants. Moreover, a deep understanding of the

interplay between trust and confidentiality in MSCs is sought, which is a new concept related to Industry 4.0 in developed and industrialized countries such as Germany, where sustainable production and transportation have become the core of industries.

We conducted semi-structured interviews with key practical experts with roles pertaining to the management of supply chains and process engineering. Semi-structured interviews enabled us to provide strategic propositions according to the real world experiences of the interviewees [82]. Semi-structured interviews encourage the respondents to reveal their own experiences, views, and attitudes by answering questions prepared by the researcher [83]. In addition, it helps the researchers to observe and collect data from real cases [29,84]. However, some studies [29,85,86] recommending a qualitative method in order to understand the context of new subjects in depth, studies of Crescentini and Mainardi [87], Almeida et al. [88] have noted some limitations regarding these methods as compared to quantitative ones, such as less structured theoretical frameworks, internal researcher's point of view, and longer time requirements for the scope of the study. To increase the effectiveness of a qualitative research method, Mayring [81] has recommended a set of guidelines which are also carried out in this study.

### *3.1. Data Collection*

The purpose of this study was to investigate the tension between trust and confidentiality based on the level of information sharing. This study aimed to investigate the following three major problems: investigation of the tension between trust and confidentiality in MSCs, strategies for balancing this tension, and integration scenarios in which trust, confidentiality, and information sharing are combined to indicate in which scenario the tension emerges. For this purpose, we conducted semi-structured interviews with top executives of German chemical and pharmaceutical companies which are closely associated with the mobile supply chains concept. Semi-structured interviews are a valuable instrument to thoroughly investigate an unidentified subject through the thoughts, experiences, and attitudes of participants [89]. Moreover, they contribute to collecting more realistic data from current industry practice. Through semi-structured interviews, both interviewee and interviewer have freedom in the direction of the responses and questions [41].

The authors selected participants through professional networks. A total of 7 top executives from 6 different companies agreed to participate. The reason behind the small study sample can be related to the limited number of companies practicing modular production and which are familiar with the concept, due to its novelty. According to a study by Crescentini and Mainardi [87], samples in qualitative methods are often small to allow for deeper case-oriented investigations that are essential for this form of research. According to recent research [90,91], purposive sampling is more efficient than random sampling in qualitative investigations. All the respondents have been active in either the chemical, process, or pharmaceutical industries for more than 10 years. We selected these top executives based on their profession and their knowledge in the field of mobile supply chains as well as modular production. All companies are pioneers and leaders in these industries and have their main headquarters in Germany; therefore, this study also contributes to the reinforcement of German modular production and the process industry.

We guaranteed the anonymity of all interviewees throughout the research by allocating numerical identifier codes to each participant. In this way, the authors refrain from disclosing the names and details of the participating companies.

### *3.2. Interview Protocol*

An interview guide consisting of three sections with overall 13 open-ended questions was prepared to manage the discussions with respondents (Appendix A). In the first section, we focused on the concept of MSCs and the status of this novel concept in the sampled firms. Then, we asked some questions regarding trustful collaboration in the context of MSCs, followed by investigating information sharing scenarios in which trust and confidentiality both interact. The interview guide was designed based on the literature

and was applied to all interviews. The goal was to assure uniformity and to streamline the analysis [29]. Before each interview, an online poster with information regarding the interview questions was sent to all participants. Each interview was started with a self-introduction of the interviewer and a brief presentation of the MSC concept to familiarize the participants with the objectives and questions of the interview. After building a comfortable environment for participants to share their thoughts and experiences more easily, the interviewer continued with the detailed questions as per the interview guide. The interview protocol was designed based on the literature and was applied to all interviews. Due to COVID-19 restrictions, researchers had to conduct interviews online through video conference software in accordance with privacy and data protection policies and the duration varied between 30 min to 1 h. All interviews were audio-recorded with the consent of the participants. Afterwards, each interview was transcribed word by word for further analysis.

### *3.3. Code Segments and Data Analysis*

All transcribed interviews were analyzed using the MaxQDA software following the methods adopted by [92]. Qualitative data analysis contributes to arranging the data properly in terms of order, shape, and significance. The researchers then create code categories and groups to define the relationship between groups and themes. Only through the creativity of the researchers is a better understanding of the phenomenon possible [89]. Regarding qualitative data analysis, researchers adopted a semi-inductive approach outlined by [81].

The coding process for the analysis was started by formulating the research questions and defining the code definitions and level of abstraction. Then the transcribed materials were read line by line to check if the material was related to the code definitions. We repeated this step until it was ensured that all the material had been assigned to the codes and no revision in the code system was needed. This process resulted in a list of codes (categories), which were then grouped together to form main categories for analysis. Codes are small pieces of information which convey the same meaning and concept, a similar idea, or signal the same subject. Similar codes and phrases are placed in a similar group, which create themes. Themes can be presented in tables or graphical to report the final conclusion of the study [89].

Regarding the reliability and validity of the research, we adopted inter-coder and intra-coder agreement procedures as suggested by [81]. After the first coding process, the first coder repeated the coding process for half of the material from the beginning to ensure that the allocated code categories were similar to the initially assigned categories. Then the material was sent to the second coder to check the code categories. The results of two coders were then compared. Differences between the two coders were discussed following the coding rules in order to enhance reliability. Moreover, we created a database of the collected data and findings (interview guide, interview description, recorded audios, transcription, coding-books and code system). In the findings section, some relevant responses from the interviewees are included to increase research validity.

## 4. Results and Discussion

The aim of this study was to investigate the tension between trust and confidentiality based on the level of information sharing. In this regard, this paper illustrates the scenarios in which the tension between trust and confidentiality arises and proposes three significant approaches which encourage partners to balance the tension between trust and confidentiality. During the semi-structured interviews it was apparent that a unique information sharing system is not present in the studied companies. This means that the participants mentioned different scenarios for information sharing, each presenting a different context regarding the relationship between trust and confidentiality. In some scenarios a tension between trust and confidentiality was mentioned, while others had no tension. In this regard, we elaborate on various integration scenarios to determine specifically where a tension between trust and confidentiality emerges and which strategies contribute to managing

this tension. In this section, firstly, the decision-making criteria which were mentioned by respondents to select the appropriate scenario for collaboration with their partners in MSCs are identified, after which the four integration scenarios are determined and described, followed by an investigation of the tension between trust and confidentiality in which three strategies for balancing this tension are recommended. Finally, a table summarizes the differences between scenarios based on their characteristics and applications to provide a comprehensive overview of all the scenarios and the level of tension in each scenario.

### *4.1. Decision-Making Criteria for Integration Scenarios*

As one of the respondents noted, "*I think the level of information sharing depends on the level of integration [among partners]*". Given this, nearly all participants admitted the existence of various integration scenarios in MSCs. They also emphasized the challenges this poses in the relationship between trust and confidentiality, or information privacy. Integration scenarios varied from intense integration, where partners share a high level of information in order to operate the production plant, to medium and low levels of integration. We categorized the scenarios based on the decision-making criteria mentioned by respondents. Figure 2 corresponds to these criteria: *partner's role*, *product type type of modular plants*, *service period*, and *market threat*. It is evident from the results that a significant number of respondents consider the partner's role as the most important criteria for deciding on the best scenario. Product types and service period follow as the second and third most important criteria, respectively, in the decision-making process. The remaining two criteria (modular plant types and market threat) have the same, lower importance.

**Partner's role**

As mentioned earlier, a considerable number of respondents stated that an important factor for them in decision-making is their role in the collaboration system. This implies the type of responsibilities and the role of partners in MSCs. As one of the respondents mentioned, "*It depends if the module supplier is also [the] owner of the process or whether the customer is [the] owner of the process*", which reveals the importance of the Partner's responsibilities and roles. In the chemical industry, the process owner is the party that owns the intellectual property regarding the process, i.e., recipe and operating conditions, and has the responsibility to manage and improve the processes. Specification of the process owner is important for "business process management" [93]. Various responsibilities are delegated to process owners for improving and managing processes, such as "planning", "controlling", and "governance" [93]. This means that if the module owner and process owner are not one in the same, the information sharing scenarios to manage the processes will be changed. In this case, the partners need to share a high level of information for managing and enhancing the processes; however, in the opposite model where the owner of both is the same, the process owner does not exchange much information with the module operator. This is due to the differences in distributing tasks, competencies, and responsibilities.

**Product type**

Some of the respondents noted that they are involved with different types of products, and that this leads them to different scenarios. This implies that companies consider different scenarios for different products. Several types of products were mentioned by our respondents: new product development, standard products, and customized products, etc. In most cases, partners adopt mass production for standard products using the one-size-fits-all approach and fulfilling the demand of several customers at one time. In this case, they do not need to share much information with their partners as they are more concerned about the quality of products than the information behind the production. However, regarding new product development process, the partners have to collaborate closely with each other. In line with the results from [29], high integration with transparent communication amongst various stakeholders is essential for innovative new product development. As one of the respondents stressed, "*It is a different story if you, for example, have a collaboration where you have commonly developed some product or whether you provide standard products*".

**Service period**

This criterion refers to the period between when a mobile facility starts the first batch and ending upon completion of the last batch. It is important for the Partner's transport planning to know how long a mobile facility needs to stay at a partner's site to complete the production process [94]. If they want to lease it for a short period, e.g., 3 to 5 weeks, they need support for repair and maintenance from the module provider. In this case, the module operator does not require operational and technical information, because the module provider is required to provide this kind of service with their equipment. However, if the operator is looking to lease the module for over 2 years, they demand much more information from the provider in order to run, maintain, and repair the module, for example, during night shifts with their own employees onsite. This was referred to by one of our respondents: "*When we, as owner operator, buy and run a module for years, I want to be able to maintain and repair it in the night shift with my own people. I can't do that if it's a black box. If it's a black box, I don't know which equipment I need, I don't have spare parts, I don't have trained people. It's a black box. So, for continuous use, we insist on having white box information which enables us to run it and to repair it. When I kind of rent equipment for 4 weeks, I have no chance to do maintenance myself. I have no chance to train my people. So, in that case I would need a support contract with the partner and ask them to guarantee a high availability and to be able to repair things within hours. That would be part of my rental contract. So, in this case, I don't have to know the details of the equipment*".

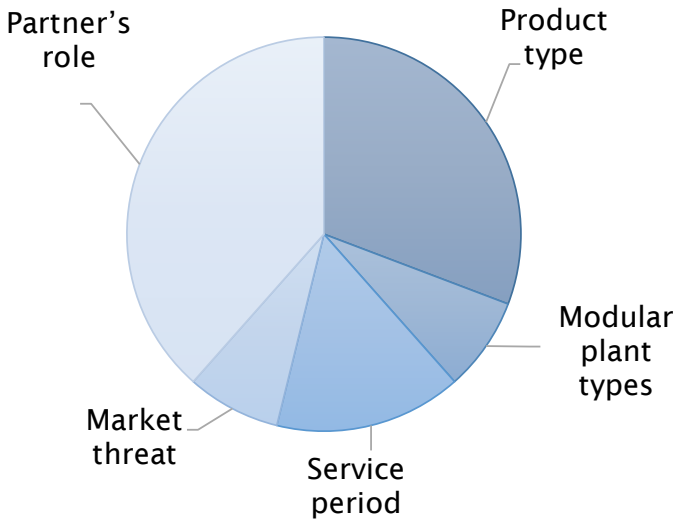


**Figure 2.** The decision-making criteria for integration scenarios.

**Type of modular plant**

This criterion refers to the function and size of the plants. One of the respondents mentioned, "*If I have a relatively small [piece of] equipment that I lease, I will not lease [a] full process system, I would [instead] lease a reactor, I would lease a separator, and things like that. So it would need less information exchange because they need the information just for this step*". The result reveals that the function of each plant is significant for determining the level of information sharing. The partners need to specify the goals of leasing the plant. If a small piece of equipment is leased, such as a reactor, distillation unit, or separator, just for a limited part of the production process, then they are not obliged to share a high level of information. Previous studies also emphasized that each mobile factory can contain various modules which are essential for producing different products [95,96]. According to the results, however, this criterion is not mentioned by most of the respondents. However, it is thought that determining the goal and function of the plants from the beginning of the collaboration system is necessary. With this knowledge, partners can determine how much information they should or should not share. The reason behind this low importance could

be that, since the function and goal of the mobile plants are clear to the respondents, it was not important for them to refer to the significance of this criterion in the interview.

**Market threat**

One respondent emphasized the risk of being pushed from the market as a significant threat if one refuses to share information. He stated that "*They had to open up the complete knowledge to the customer, otherwise [we] would have been out of business*". We coded this segment as market threat because the partners are somewhat obligated to interact with each other intensively to maintain their market position over competitors.

### *4.2. Integration Scenarios*

Four different scenarios are displayed in Figure 3. These scenarios were categorized based on trust level (high and low) and integration level (high and low), in consideration of the decision-making criteria. Confidentiality level and the state of tension between trust and confidentiality is depicted in each scenario by different colors. The lighter green and orange colors specify lower levels of confidentiality and tension, respectively. A detailed description of each scenario is provided in the following:

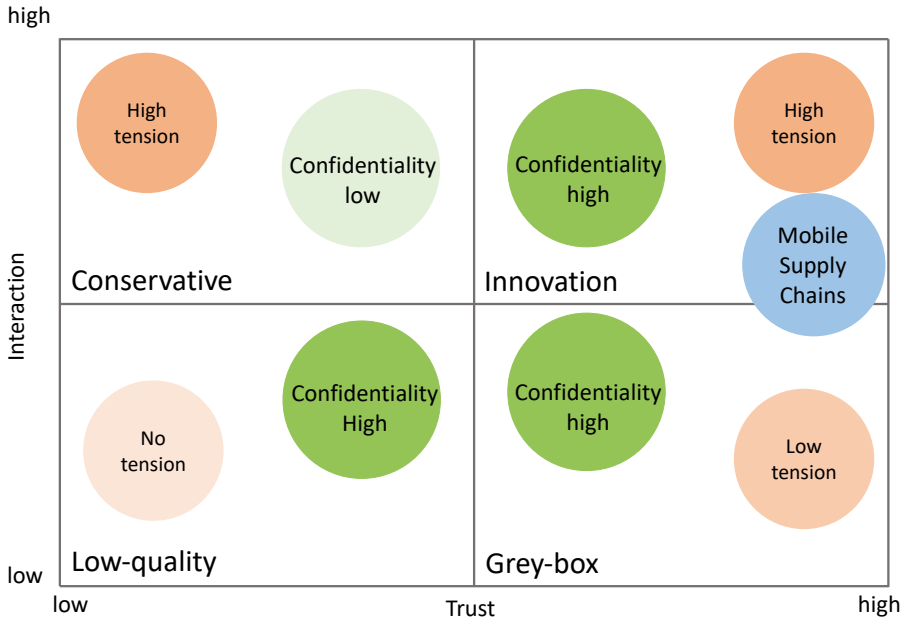


**Figure 3.** Integration scenarios in mobile supply chains.

#### 4.2.1. Low-Quality Scenario

The bottom left corner of Figure 3 presents a scenario in which one or both partners refrain/forget to share key information required for producing high quality products. On the one hand, this results in a higher level of confidentiality since partners can limit disclosure of the proprietary information [63]. However, on the other hand, the level of trust is low as the committed quality for the product is not met [97]. The module provider could not perform to the promised quality, signaling less competency and benevolence to the operator, leading to a lower level of trust [28]. In this scenario, no tension between trust and confidentiality is observed. Confidentiality is high due to the limited exchange of information [61]. Trust is low due to the low quality of specified products [97], not because of high confidentiality. As one of the respondents mentioned: "*If you're missing a key [piece of] information to make a precise product and you have a bad quality and you find there is missing information, then you have a trust problem*". It is obvious that the partners need to share a minimum level of information in collaboration systems to build and maintain trust, otherwise their collaboration may fail [98]. Since trust is key in strategic alliances [38], this scenario is not considered desirable and sustainable, especially in MSCs. This scenario is mentioned in this study to illustrate the consequence of missing key information for

production in MSCs. The results confirm the findings of previous studies which emphasized the presence of trust in strategic alliance [27,30,35,38].

#### 4.2.2. Conservative

This scenario represents a situation in which one of the partners is conservative and fears change. Some respondents expressed their concern about this problem. Regarding Germany's conservative economic model [99], some companies tend to stick to existing production approaches, which prevents them from accepting new and innovation technologies and production procedures. Some companies are still producing products similar to those they were making 30 years ago. This situation leads to certain challenges in the field of mobile supply chains, which is considered an innovative and novel concept based on disruptive technologies and digitization. In this concept, partners should show their willingness to accept new risks and uncertainty in order to perform efficiently [1,94].

Despite this fact, some respondents mentioned that their partners are fearful of change. They refuse to accept the concept of shared mobile factories and its ability to provide services in dispersed locations for different clients. The reason behind this is, on the one hand, their unfamiliarity with the MSCs concept and, on the other hand, their fear of information leakage. They are not willing to share a high amount of information with their suppliers when they imagine the mobile factory moving to the next customer after finishing its service at their own site. As one of the respondents mentioned, "*They fear changes. They fear contamination. They fear everything that they don't have under control. They are really adverse to accepting any changing infrastructure, any change in the process, any change in the flow even any change in the personnel...they don't know, if there is another product. Can you assure that this facility comes back to our site in the same mode when it left us? So, it is out of our control. It is not at our premises anymore. We don't know the [next] client, we don't know what he's doing with it. They won't accept that*".

In this scenario, the tension between trust and confidentiality is high. One party requests a high level of information sharing; however, the other party suspects possible information leakage (low confidentiality), which leads to a lower level of trust [61]. Therefore, to manage the tension between trust and confidentiality, conservative partners require their supplier to adopt a customization approach regarding both products and mobile plants. In this case, the mobile factory is dedicated solely to one partner. This results in a scenario that suits suppliers who are willing to invest more in mobile supply chains and allocate individual and customized production facilities to their customers. Additionally, this scenario is applicable when the market threat is high; if the supplier does not collaborate with the other partner, they lose market share due to high levels of competition. Although customization is a crucial component of MSCs [100], previous studies have considered mass customization for implementing MSCs more economically efficient [94], requiring trustful collaboration with several partners.

Therefore, few respondents mentioned this scenario as an appropriate application of MSCs since the concept of shared mobile plants is not adopted [101]. Therefore, the use of this scenario is limited to specific situations. Moreover, this scenario is not applicable for short-term leasing approaches, but rather for long-term production.

#### 4.2.3. Grey-Box Scenario

A grey-box scenario of integration represents a moderation between the two extremes of total non-disclosure and full disclosure of information. Through the interviews, it became apparent that partners need to share a minimum level of information to operate MSCs. One respondent stated that "*In pharma[ceutical industry], we have to care about quality relevant information. There a black-box would not work*". A black-box scenario with extreme non-disclosure would not be applicable for the chemical and pharmaceutical industries. This result is also consistent with [102], which emphasizes the flow of information and material for controlling MSCs.

In a grey-box scenario, the tension between trust and confidentiality is lower than in a conservative scenario. Sharing a lower level of information between partners leads to higher confidentiality, assuring the partners that their proprietary information is protected from leakage. Since a confidentiality agreement is signed between the partners before initiating the collaboration, determining the level and scope of shared information, the partners have no expectation of extreme information exchange [63]. Therefore, high confidentiality has no negative effect on the level of trust, and trustworthiness is maintained amongst partners.

Trust is affected by other factors such as quality of products, performing to made promises, and knowledge about the process and products, rather than confidentiality and information sharing. The quality of products depicts competency and benevolence of one party to the other [28]. These results contradict with previous studies [103,104] which concluded that exchange of sensitive information is essential for cultivating long-lasting trustful relationship. This illustrates that the relationship between information sharing and trust is complicated and two-way [41,105].

This scenario is applicable when partners adopt modular plants for the mass production of standard products [94], or for short-term leasing situations [106]. According to the partner's role, respondents referred to the situation when module owner and process owner are the same. Here, they do not need to share a high level of information with their partners, as they build trust on the competency and integrity of their partner to produce high-quality standard products. In short-term leasing, applicable modular plants typically include basic pieces of equipment with simple functions like mixing, drying, etc. In this regard, the respondents mentioned that "*If you need pressurized air and somebody is running a compressor for you so that you get air as an energy supplier, for you as a customer basically only the electrical voltage and power rating is important. You are interested in a steady supplier for electricity*".

"*You need to have high trust that your partner will stick to [the] rules and that the little information that you have is sufficient for you to be successful. It does not mean no trust.You need to have a full trust that your partner is operating within such standards*."

"*If the module owner is also the process owner', there's no need [to exchange] his know-how. We had other projects where we just rent our own process and want to build it on the customers site, but we were the process owner as well. As the modular production owner, there's no need to exchange this information with the customer*."

"*It would need less information exchange because they need the information just for this step. So the level of know-how would be smaller because the module which I buy [rent] is smaller*."

The grey-box scenario was mentioned by a higher number of respondents, which shows that partners tend to employ grey-box approaches in mobile supply chains quite frequently. This willingness can be due to the lower tension between trust and confidentiality. In situations where partners are involved in the mass production of standard products, they determine the level of exchanged information while assuring confidentiality since they preserve their trust by producing high-quality products.

#### 4.2.4. Innovation

The grey-box scenario was mentioned as an appealing scenario for standard products. However, considering that MSCs are an innovative and novel concept [1], the innovation scenario was emphasized most frequently by our respondents. They believe that with innovative concepts, partners need to exchange a higher level of information. This result is in line with [29], which suggested that partners need to share a higher level of information for developing new and innovative products.

A high level of information exchange and integration in this environment results in a higher level of trust. This is in line with previous studies which illustrated a positive relationship between trust and information sharing [103,104]. However, a high level of information exchange leads to the issue of less confidentiality [63], resulting in a tension between trust and confidentiality. Especially when partners collaborate on "open innovation" and "new product development", intellectual property concerns arise [107]. This situation

is similar to the *conservative scenario*, in which fear of information leakage generates lower trustworthiness amongst partners. The difference between these two scenarios is partner's role in the collaboration system. This means that, when one party fears changes corresponding to new technologies, less trust is built amongst partners; thus, they seek individualized products and plants which lack the flexibility and sustainability aspects of MSCs. However, in innovative scenarios, partners are open to novel concepts and technologies and they understand the risk and benefits of MSCs. Therefore, they seek to manage the tension between trust and confidentiality with practical strategies.

The question emerges as to how partners can maintain trust if they employ confidentiality agreements and other privacy-preserving techniques. With the availability of numerous solutions for confidentiality preservation, partners can securely share their information with low risk of leaking sensitive information. According to the results from interviews, to build safe and secure environments they need to consider three critical factors to manage the tension: transparency, trust negotiation, and a reward-sharing system. In the next section, more detailed explanations of these strategies are given.

This scenario is applicable in MSCs when partners cooperate to jointly develop a process or a new product, or when the module owner and process owner are not one in the same. In cases where a partner produces a raw material which serves as a customized intermediate product for the other party [94], they need to share a higher level of information. In this regard, the respondents noted "*if the module owner is also the process owner, there's no need to exchange the know-how. If the customer is the process owner, yes, of course you have to exchange it*".

Moreover, it is important for all partners to understand the concept of MSCs and to present their willingness to take risks and accept the uncertainties. In this case, they are able to build and maintain a trustworthy relationship.

Table 1 summarizes the characteristics of each scenario, illustrating the differences of integration scenarios based on the levels of trust, confidentiality, and information sharing, as well as their applications. It is notable that the *low-quality scenario* and *grey-box scenario* both apply low levels of information sharing. However, the former misses the sharing of key information and results in lower trust, while the latter is designed to share the minimum level of information because the partners are able to collaborate with a minimum level of information. Trust is built upon the quality of the products. Therefore, the tension between trust and confidentiality is low. The grey-box scenario contains various applications such as Module-as-a-Service or producing standard products, while low-quality scenario is rather rare in MSCs.

**Table 1.** Differences of integration scenarios in mobile supply chains.

| Integration Scenarios | T–C Relationship | Characteristics |
| --- | --- | --- |
| Low-quality (rather rare) | **Trust:** low<br>**Confidentiality:** high<br>**Information sharing:** low<br>**Tension:** insignificant | **Product types:** poorly specified products |
| Conservative (rather rare) | **Trust:** low<br>**Confidentiality:** low<br>**Information sharing:** high<br>**Tension:** high; one party does not accept low level of confidentiality, results in low level of trust | **Partners:** conservative partners<br>**Product types:** customized products<br>**Modular plant types:** individual modular plants<br>**Market threat:** high threat from competitors<br>**Service period:** long-term |
| Grey-box<br>(more frequent) | **Trust:** high<br>**Confidentiality:** high<br>**Information sharing:** low<br>**Tension:** low; one party accepts low exchange of sensitive information due to the importance of trust for product quality | **Partner's role:** process owner and module owner are one in the same; low integration<br>**Product types:** standard products; modular capacity<br>**Modular plant types:** small modular units, Module-as-a-service<br>**Market threat:** low threat from competitors<br>**Service period:** short-term leasing |

**Table 1.** *Cont.*

| Integration Scenarios | T–C Relationship | Characteristics |
| --- | --- | --- |
| Innovation (most frequent) | **Trust:** high<br>**Confidentiality:** high<br>**Information sharing:** high<br>**Tension:** high; three major strategies and confidentiality preserving-techniques are used to manage tension between trust and confidentiality | **Partner's role:** different process owner and module owner; high integration<br>**Product types:** new product development; raw material; customized products<br>**Modular plant types:** Shared mobile facilities; Factory-in-a-box [71]; Manufacturing-as-a-Service [108]<br>**Market threat:** high threat from competitors<br>**Service period:** either short- or long-term |

Considering the scenarios with a high level of integration, *conservative* and *innovation* scenarios were highlighted. Although the tension between trust and confidentiality is high in both scenarios, the reason and the managing strategies are different.

In most cases, respondents believe that mobile supply chains can be operated in both *grey-box* and *innovation* scenarios because the partners need to maintain a trusting relationship throughout the partnership, but they can decide to share either a high level or low level of information based on the decision-making criteria as well as the applications of the MSC. When partners employ mass production of standard products, they are encouraged to employ grey-box. In this regard, partners are able to preserve confidentiality limiting the amount of exchanged information to a minimum, while they maintain a trusting relationship due to their commitment to deliver high quality products. Therefore, the tension between trust and confidentiality is low and the partners require less effort to manage it. However, most respondents believed that mobile supply chains are a concept best suited for processes beyond the simple mass production of standard products. The MSC concept contains innovative and novel solutions for increasing flexibility, reducing gas emissions, reducing transport costs, etc., requiring a strategic alliance for new product development [1,94]. This entails a high level of exchanged information while preserving confidentiality in a safe environment. Trust can be built and maintained while employing three strategies, namely, transparency, trust negotiation, and a reward-sharing system.

### *4.3. Strategies for Managing the Tension between Trust and Confidentiality*

As shown in Figure 4, three critical strategies qualify for building a safe and secure environment to manage the tension between trust and confidentiality. Each of these elements have been mentioned in the literature as a factor for building or maintaining trust [4,27,29,41]. However, the results of this study show that partners need to employ these three strategies simultaneously to manage the tension between trust and confidentiality. This is suggested not only as a means to enhance trust, but also to provide a safe and secure environment for secure information sharing.

**Transparency**

Transparency is associated with determining the goals by all partners. It means that the extent to which the role, responsibilities, objectives, vision, and type of exchanged information are clear to all participants, and all partners are involved in this exchange entirely. Transparency generates trust, which is enhanced especially when open and continuous communications are maintained amongst partners [29]. As one of our respondents noted "*I would lose trust if there were questions about why they are needed. I would say: I do not understand why they need it, so why do they want to have it? And I would get suspicious*". Only through transparency can partners ensure that a secure environment is created for the sharing of confidential information. A contract is valid and suitable to support such relationship when all tasks and responsibilities, including the details of shared information, are clear and transparent to all partners. Any ambiguity can lead to distrust, and ultimately, end their relationship. Transparency has been considered a crucial factor of trust in previous studies [29,41]. To enhance transparency, respondents recommended frequent communication, a clear distribution of tasks and responsibilities, and negotiation of privacy-preserving

contracts with detailed information. In addition, from the beginning of the collaboration, all policies and plans for continuous communication as well as the terms and conditions included in the confidentiality contracts should be provided to all partners [29]. This may incur increases in communication and negotiation efforts; however, once all details are determined, the partners can collaborate in a safe and trusting environment.

**Trust Negotiation**

Trust Negotiation (TN) is a means for building trust through negotiation and management of the relationship. In the literature, trust negotiation is referred to as techniques for controlling access to sensitive information in open environments when partners are strangers [4,109]. In the present study, a general definition of this system is considered without applying the results to a detailed explanation of peer-to-peer web communications. It is believed that TN is also required when parties are not communicating solely through digital means. Trust Negotiation is a transparent interaction among partners to discuss and decide on the dimension of property disclosure and information privacy. For instance, one respondent mentioned that "*If you have engaged in the contract and discovered that more information is needed then that needs to be negotiated again*". In this approach, mutual access to sensitive information is possible only when the negotiation process has been successfully completed [4]. As another respondent noted, "*If we find out that the partner needs more confidential information to fulfill our requirements, of course, we then give that to them*". This suggests that only after transparent negotiation and clear communication can partners build and maintain a trusting relationship with an optimized level of confidentiality.

To implement this strategy in MSCs, all partners need to negotiate about sensitive and private assets and proprietary information transparently from the beginning of the collaboration. All information about the users, processes, roles, and servers needs to be determined beforehand. Several strategies clarifying the type of sensitive information, the time and scope of disclosure, and the provision of frequent feedback (both positive and negative) need to be adopted.

**Reward-sharing system**

It is important for partners to know that their partnership is economically profitable for them: "*We had a quite valuable partnership which was quite economically profitable for both of us*". When partners are negotiating the contract and specifying their properties and information disclosure, it is important for them to know how they benefit from this disclosure. In the future, when one of the partners may require more sensitive information, they should also be made aware of the benefits. Only when they share benefits out of disclosure can they build and maintain a trusting relationship. Since the potential rewards of participating in advanced innovation are substantial [97], most respondents believe that the sharing of benefits can enhance trust. However, the risk of failure should also be taken into account by all partners. To implement this strategy, a model of the risk/benefit framework should be provided to all partners to specify the share of risk/benefits for each partner, including exceptional situations where more sensitive information is required from one party.

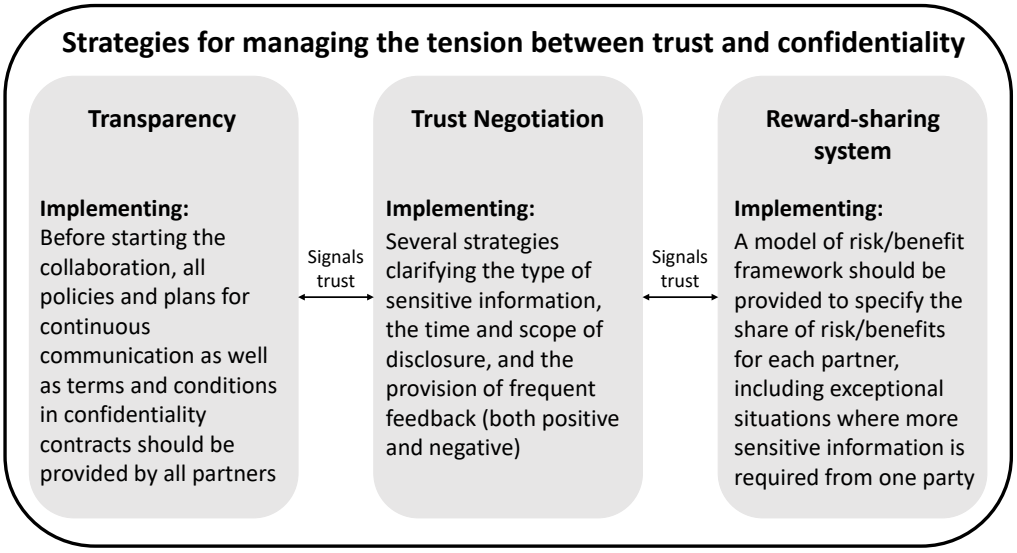


**Figure 4.** Strategies for managing the tension between trust and confidentiality.

## 5. Conclusions

Striving for "ecological" and "social sustainability" of production, as well as mass customization, has affected the status quo of traditional supply chains by introducing the possibility of relocating production sites [68]. Mobile supply chains are value creation systems that aim to reduce greenhouse gas emissions caused by the complete life cycle of products from start to finish [1]. MSCs enable the sustainable production and distribution of goods and services by the mobilization of stationary production resources. Several stakeholders with different goals and missions need to cooperate to implement MSCs, which can cause various challenges and requirements to arise when production facilities are moved between different supply chain partner sites. To maintain a sustainable relationship between partners in mobile supply chains, and their practical operation, a balance of trust in partnership and high level of confidentiality for shared information within the interaction is essential. Inevitably, such advanced industrial collaborations, such as MSCs, can encounter integration issues and raise concerns regarding the proper management of information flows. A trustful relationship could imply full disclosure of information by partners; however, there is a large variety of confidential or proprietary information, including process inputs, operation conditions, control parameters, and generally sensitive information.

In this regard, the aim of the study was to investigate the tension between trust and confidentiality based on the level of information sharing. Within this context, the paper illustrates the scenarios in which the tension between trust and confidentiality arises, and proposes three significant strategies which provide guidance for partners looking to balance this tension. During semi-structured interviews, it was apparent that a unique information sharing system is not present in the studied companies. This means that the participants mentioned different scenarios for information sharing, each containing a different context for the relationship between trust and confidentiality. In some scenarios a tension between trust and confidentiality was mentioned, while others had no tension. In this regard, we elaborated on various integration scenarios to determine specifically where a tension between trust and confidentiality emerges and which strategies contribute to balancing this tension.

The interviews with seven qualified experts from the chemical, process, and pharmaceutical industries allowed us to gain a better understanding of the integration and collaboration systems within this novel concept. Close attention was paid to various integration scenarios by considering the interconnection of trust, confidentiality, and information sharing. These integration scenarios are, namely, the *low-quality*, *conservative*, *grey-box*, and *innovation* scenarios. Most respondents suggested that the *innovation* scenario is the best fit

for mobile supply chains as this concept is novel and requires intensive integration in a secure and trusting environment to maintain both trust and confidentiality.

**Theoretical contribution**

The results of this study extend the research on collaboration systems and contribute to the literature in several ways. First, this study elaborates on the literature covering the interconnection of trust, confidentiality, and information sharing by presenting a framework including these three indicators that can serve as a conceptual basis for future empirical and quantitative research in supply chain management, especially for MSCs. Some scenarios contradict previous studies, which suggested the existence of a one-way positive relationship between trust and information sharing [103,104]. Therefore, this study adds additional insight to the literature in terms of the relationship between trust and information sharing. Second, the present study adds to the body of literature of integration scenarios by investigating four scenarios and specifying outcomes in which tension between trust and confidentiality emerges. Third, three critical strategies, namely, transparency, trust negotiation, and a reward-sharing system, are added to the literature with the aim of managing the tension between trust and confidentiality. These strategies were mentioned separately in previous studies to foster inter-organizational trust [4,29,97,109]; however, few studies have provided a conceptual model that considered these three strategies for balancing the tension between trust and confidentiality.

**Managerial implications**

From a managerial and practical perspective, this study contributes to decision-making for practitioners and managers in two ways. First, the study provides new guidelines for the decision-making criteria used to select the best integration system during the implementation of an MSC. Second, if partners select a scenario in which tension between trust and confidentiality is high, we recommend the employment of three strategies to manage this tension. Although partners are free to select the proper scenario for their relationship, the results of this study show that mobile supply chains perform more efficiently in innovative scenarios. The reason is that the partners need to share a high level of information if they are involved in novel concepts such as MSCs. In this regard, they need to be involved in frequent transparent communication to maintain a trusting relationship throughout the partnership.

**Limitations and future work**

The results of the study provide the primary basis for future research and should be interpreted bearing in mind several limitations. First, the sample size of 7 participants in the German market for the semi-structured interviews limits the generalizability of the results. Thus, we suggest that future research for other markets should employ a greater number of respondents. Second, this study provides a conceptual framework of integration scenarios and three critical strategies; therefore, future studies are suggested to analyze the impact and validity of this framework in a quantitative context and determine additional aspects. Third, the research model of this study was based on dyadic relationships, in which the interactions of two partners are analyzed. However, since multiple stakeholders need to collaborate to operate mobile facilities in the MSC concept, we strongly recommend future studies to include multi-agent or multi-stakeholder collaboration in the research. Moreover, it is suggested that future studies investigate the effect of information quality on the relationship between trust, confidentiality, and information sharing.

**Author Contributions:** Conceptualization, N.G., Z.C., S.E. and L.U.; methodology, N.G. and S.E.; software, N.G.; validation, N.G. and Z.C.; formal analysis, N.G., Z.C. and S.E.; investigation, N.G. and Z.C.; resources, N.G. and Z.C.; data curation, N.G.; writing—original draft preparation, N.G. and Z.C.; writing—review and editing, N.G.; Z.C., S.E. and L.U.; visualization, N.G. and Z.C.; supervision, S.E. and L.U.; project administration, S.E. and L.U.; funding acquisition, S.E. and L.U. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors would like to thank the Boysen-TU Dresden Research Training Group for the financial support that has made this publication possible. The Research Training Group is co-financed by TU Dresden and the Friedrich and Elisabeth Boysen Foundation.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Data was collected through interviews and can be provided on demand, whenever required.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

Interview questions:
Some of the questions were omitted if the interviewee mentioned them between their responses to previous questions.

1. Could you please explain the implementation and current status of MSCs projects in the industry and your organization?
2. What would be the next steps and future of this project?
3. In your opinion, how many partners need to collaborate to run MSC projects? and what is the role of each?
4. What can help partners to keep trustworthy relationships in MSCs? What are the elements and factors?
   Questions 5 to 11 are based on the presented information scenarios: If we consider a scale for information sharing, with one side representing intensive information sharing and the other side a low level of information sharing.
5. In your opinion, what is the framework of information sharing between partners in MSCs?
6. How can you decide to share information or do not share? What are the criteria or situations used to make a decision?
7. Let us focus on a scenario where you need to share a high level of information. Do you think there is a risk of information disclosure? In this case, how would you guarantee confidentiality regarding the information and equipment?
8. Let us imagine you anticipated that your partner could produce a certain amount of information, but it turns out that they cannot. What would be your approach if your partner cannot continue the production or research without the information?
9. (depends on the answers to previous questions) According to the contract, you are obliged to share a certain amount of information with you partner, and they are aware that some amount of information is not shared with them. How will it affect their relationship with you ( in terms of uncertainty/ lack of trust/ having a bad experience)? Do you think it could affect your mutual trust level?
10. What can help you keep a trustworthy relationship in both situations (high information exchange/low information exchange)?
11. From your experience, what is the interplay between confidentiality and trust in mobile supply chains?
12. In which applications is it possible to run a mobile asset but share a low level of information?
13. In your opinion, what are the challenges of information exchange in MSCs compared to traditional supply chains?

## References


1. Aßmann, U.; Buscher, U.; Engesser, S.; Schönberger, J.; Urbas, L. Software-Defined Mobile Supply Chains. In *International Conference on Dynamics in Logistics*; Springer: Cham, Switzerland, 2020; pp. 420–430.
2. UN. The 17 Goals. Transforming Our World: The 2030 Agenda for Sustainable Development. 2022. Available online: https://sdgs.un.org/goals (accessed on 15 January 2022).
3. Smith, G.E.; Watson, K.J.; Baker, W.H.; Pokorski, J.A. A critical balance: Collaboration and security in the IT-enabled supply chain. *Int. J. Prod. Res.* **2007**, *45*, 2595–2613. [CrossRef]
4. Bertino, E.; Khan, L.R.; Sandhu, R.; Thuraisingham, B. Secure knowledge management: Confidentiality, trust, and privacy. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2006**, *36*, 429–438. [CrossRef]
5. Harwood, I.; Ashleigh, M. The impact of trust and confidentiality on strategic organizational change programmes: A case study of post-acquisition integration. *Strateg. Chang.* **2005**, *14*, 63–75. [CrossRef]
6. Goldfield, E.D.; Turner, A.G.; Cowan, C.D.; Scott, J.C. Privacy and confidentiality as factors in survey responce. *Rev. Public Data Use* **1979**, *6*, 219–229.
7. Deason, E.E. The Need for Trust As a Justification for Confidentiality in Mediation: A Cross-Disciplinary Approach. *Kans. Law Rev.* **2005**, *54*, 1–25.
8. Sahay, B.S. Understanding trust in supply chain relationships. *Ind. Manag. Data Syst.* **2003**, *103*, 553–563. [CrossRef]
9. Colicchia, C.; Creazza, A.; Noè, C.; Strozzi, F. Information sharing in supply chains: A review of risks and opportunities using the systematic literature network analysis (SLNA). *Supply Chain. Manag.* **2019**, *24*, 5–21. [CrossRef]
10. Hong, Y.; Vaidya, J.; Wang, S. A survey of privacy-aware supply chain collaboration: From theory to applications. *J. Inf. Syst.* **2014**, *28*, 243–268. [CrossRef]
11. Tejpal, G.; Garg, R.K.; Sachdeva, A. Trust among supply chain partners: A review. *Meas. Bus. Excell.* **2013**, *17*, 51–71. [CrossRef]
12. Flowerday, S.; von Solms, R. Trust: An element of information security. *IFIP Int. Fed. Inf. Process.* **2006**, *201*, 87–98. [CrossRef]
13. Mayer, R.C.; Davis, J.H.; Schoorman, F.D. An Integrative Model of Organizational Trust. *Acad. Manag. Rev.* **1995**, *20*, 709–734. [CrossRef]
14. Cheng, J.H.; Yeh, C.H.; Tu, C.W. Trust and knowledge sharing in green supply chains. *Supply Chain. Manag.* **2008**, *13*, 283–295. [CrossRef]
15. Massimino, B.; Gray, J.V.; Boyer, K.K. The Effects of Agglomeration and National Property Rights on Digital Confidentiality Performance. *Prod. Oper. Manag.* **2017**, *26*, 162–179. [CrossRef]
16. Stjepandić, J.; Liese, H.; Trappey, A.J.C. Intellectual Property Protection. In Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges. In *Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges*; Springer International Publishing: Cham, Switzerland, 2015; pp. 521–551. [CrossRef]
17. Duncan, G.T.; Keller-McNulty, S.A.; Stokes, S.L. *Database Security and Confidentiality: Examining Disclosure Risk vs. Data Utility through the R-U Confidentiality Map*; Technical Report; National Institute of Statistical Sciences: Research Triangle Park, NC, USA, 2004. [CrossRef]
18. Shackelford, S.J. Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk. *Chapman Law Rev.* **2016**, *19*, 1–13. .
19. Panahifar, F.; Byrne, P.J.; Salam, M.A.; Heavey, C. Supply chain collaboration and firm's performance: The critical role of information sharing and trust. *J. Enterp. Inf. Manag.* **2018**, *31*, 358–379. [CrossRef]
20. Doney, P.M.; Cannon, J.P. An examination of the nature of trust in buyer-seller relationships. *J. Mark.* **1997**, *61*, 35–51. [CrossRef]
21. Zhao, X.; Huo, B.; Flynn, B.B.; Yeung, J.H.Y. The impact of power and relationship commitment on the integration between manufacturers and customers in a supply chain. *J. Oper. Manag.* **2008**, *26*, 368–388. [CrossRef]
22. Butler, J.K. Trust Expectations, Information Sharing, Climate of Trust, and Negotiation Effectiveness and Efficiency. *Group Organ. Manag.* **1999**, *24*, 217–238. [CrossRef]
23. Ebrahim-Khanjari, N.; Hopp, W.; Iravani, S.M. Trust and information sharing in supply chains. *Prod. Oper. Manag.* **2012**, *21*, 444–464. [CrossRef]
24. Li, T.; Tong, S.; Zhang, H. Transparency of information acquisition in a supply chain. *Manuf. Serv. Oper. Manag.* **2014**, *16*, 412–424. [CrossRef]
25. Chen, F. Information Sharing and Supply Chain Coordination. *Handb. Oper. Res. Manag. Sci.* **2003**, *11*, 341–421. [CrossRef]
26. Lee, H.L.; Whang, S. Information sharing in a supply chain. *Int. J. Manuf. Technol. Manag.* **2000**, *1*, 79–93. [CrossRef]
27. Fawcett, S.E.; Jin, Y.H.; Fawcett, A.M.; Magnan, G. I know it when I see it: The nature of trust, trustworthiness signals, and strategic trust construction. *Int. J. Logist. Manag.* **2017**, *28*, 914–938. [CrossRef]
28. Agarwal, U.A.; Narayana, S.A. Impact of relational communication on buyer–supplier relationship satisfaction: Role of trust and commitment. *Benchmark. Int. J.* **2020**, *27*, 2459–2496. [CrossRef]
29. Barrane, F.Z.; Ndubisi, N.O.; Kamble, S.; Karuranga, G.E.; Poulin, D. Building trust in multi-stakeholder collaborations for new product development in the digital transformation era. *Benchmarking* **2020**, *28*, 205–228. [CrossRef]
30. Morgan, R.M.; Hunt, S.D. The Commitment-Trust Theory of Relationship Marketing. *J. Mark.* **1994**, *58*, 20–38. [CrossRef]
31. Kumar, N.; Scheer, L.K.; Steenkamp, J.B.E.M. The Effects of Perceived Interdependence on Dealer Attitudes. *J. Mark. Res.* **1995**, *32*, 348–356. [CrossRef]

32. Nyaga, G.N.; Whipple, J.M.; Lynch, D.F. Examining supply chain relationships: Do buyer and supplier perspectives on collaborative relationships differ? *J. Oper. Manag.* **2010**, *28*, 101–114. [CrossRef]
33. Lee, L.S.; Zhong, W. Dependence Structure, Trust Dimensions, and Governance Choices in Asian Marketing Channels: Evidence in China. *Asian J. Bus. Res.* **2020**, *10*, 48. [CrossRef]
34. Wu, G.; Zhao, X.; Zuo, J. Relationship between Project's Added Value and the Trust–Conflict Interaction among Project Teams. *J. Manag. Eng.* **2017**, *33*, 04017011. [CrossRef]
35. Akrout, H.; Diallo, M.F. Fundamental transformations of trust and its drivers: A multi-stage approach of business-to-business relationships. *Ind. Mark. Manag.* **2017**, *66*, 159–171. [CrossRef]
36. Salam, M.A. The mediating role of supply chain collaboration on the relationship between technology, trust and operational performance: An empirical investigation. *Benchmarking* **2017**, *24*, 298–317. [CrossRef]
37. Ryciuk, U. Identification of Factors Related to Trust Formation in Construction Supply Chains. *Procedia Eng.* **2017**, *182*, 627–634. [CrossRef]
38. Kwon, I.W.G.; Suh, T. Factors Affecting the Level of Trust and Commitment in Supply Chain Relationships. *J. Supply Chain. Manag.* **2004**, *40*, 4–14. [CrossRef]
39. Ford, J.K.; Riley, S.J.; Lauricella, T.K.; van Fossen, J.A. Factors Affecting Trust Among Natural Resources Stakeholders, Partners, and Strategic Alliance Members: A Meta-Analytic Investigation. *Front. Commun.* **2020**, *5*, 9. [CrossRef]
40. Pech, W.; Swicegood, P. Trust And Trustworthiness: A Game Theory Transcontinental Experiment. *Int. Bus. Econ. Res. J. (IBER)* **2013**, *12*, 311. [CrossRef]
41. Ghondaghsaz, N.; Engesser, S. Identification of factors and outcomes of trust in mobile supply chains. *Eur. J. Manag. Bus. Econ.* **2021**, *ahead-of-print*. [CrossRef]
42. Chen, J.V.; Yen, D.C.; Rajkumar, T.M.; Tomochko, N.A. The antecedent factors on trust and commitment in supply chain relationships. *Comput. Stand. Interfaces* **2011**, *33*, 262–270. [CrossRef]
43. Myrelid, P.; Jonsson, P. Determinants of information quality in dyadic supply chain relationships. *Int. J. Logist. Manag.* **2019**, *30*, 356–380. [CrossRef]
44. Kelton, K.; Fleischmann, K.R.; Wallace, W.A. Trust in Digital Information. *J. Am. Soc. Inf. Sci. Technol.* **2007**, *59*, 363–374. [CrossRef]
45. Nicolaou, A.I.; Ibrahim, M.; Van Heck, E. Information quality, trust, and risk perceptions in electronic data exchanges. *Decis. Support Syst.* **2013**, *54*, 986–996. [CrossRef]
46. Opolski, K.; Modzelewski, P.; Kocia, A. Interorganizational trust and effectiveness perception in a collaborative service delivery network. *Sustainability* **2019**, *11*, 5217. [CrossRef]
47. Zhong, W.; Su, C.; Peng, J.; Yang, Z. Trust in Interorganizational Relationships: A Meta-Analytic Integration. *J. Manag.* **2017**, *43*, 1050–1075. [CrossRef]
48. Chen, K.; Shing, M.; Lee, H.; Shing, C. Modeling in confidentiality and integrity for a supply chain network. *Commun. IIMA* **2007**, *7*, 41–48.
49. Cezar, A.; Cavusoglu, H.; Raghunathan, S. Outsourcing information security: Contracting issues and security implications. *Manag. Sci.* **2014**, *60*, 638–657. [CrossRef]
50. Chen, K.L.; Lee, H.; Yang, J. Security Considerations on the Design of Supply Chain Networks. *Proc. Southwest Div. Decis. Sci. Inst. (SWDSI)* **2006**, *14*, 275–277.
51. Atluri, V.; Chun, S.A.; Mazzoleni, P. A Chinese wall security model for decentralized workflow systems. In Proceedings of the ACM Conference on Computer and Communications Security, Philadelphia, PA, USA, 6–8 November 2001; pp. 48–57. [CrossRef]
52. Li, L.; Zhang, H. Confidentiality and information sharing in supply chain coordination. *Manag. Sci.* **2008**, *54*, 1467–1481. [CrossRef]
53. Kerschbaum, F.; Schröpfer, A.; Zilli, A.; Pibernik, R.; Catrina, O.; de Hoog, S.; Schoenmakers, B.; Cimato, S.; Damiani, E. Secure Collaborative Supply-Chain Management. *IEEE Comput. Soc.* **2011**, *44*, 38–43. [CrossRef]
54. Information Commissioner's Office. Confidentiality of Commercial or Industrial Information (Regulation 12(5)(e)). Available online: https://ico.org.uk (accessed on 6 December 2021).
55. Rizvi, S.; Cover, K.; Gates, C. A trusted third-party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment. *Procedia Comput. Sci.* **2014**, *36*, 381–386. [CrossRef]
56. Yuan, H.; Qiu, H.; Bi, Y.; Chang, S.H.; Lam, A. Analysis of coordination mechanism of supply chain management information system from the perspective of block chain. *Inf. Syst. e-Bus. Manag.* **2020**, *18*, 681–703. [CrossRef]
57. Zhao, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Li, H.; Tan, Y. Secure Multi-Party Computation: Theory, practice and applications. *Inf. Sci.* **2019**, *476*, 357–372. [CrossRef]
58. Nakasumi, M. Information sharing for supply chain management based on block chain technology. In Proceedings of the 2017 IEEE 19th Conference on Business Informatics, CBI 2017, Thessaloniki, Greece, 24–27 July 2017; Volume 1, pp. 140–149. [CrossRef]
59. Shi, X.; Li, D.; Zhu, H.; Zhang, W. Research on Supply Chain Information Classification Based on Information Value and Information Sensitivity. In Proceedings of the International Conference on Service Systems and Service Management, Chengdu, China, 9–11 June 2007; pp. 1–7. [CrossRef]
60. Birkel, H.S.; Veile, J.W.; Müller, J.M.; Hartmann, E.; Voigt, K.I. Development of a risk framework for Industry 4.0 in the context of sustainability for established manufacturers. *Sustainability* **2019**, *11*, 384. [CrossRef]

61. Ali, M.M.; Babai, M.Z.; Boylan, J.E.; Syntetos, A.A. Supply chain forecasting when information is not shared. *Eur. J. Oper. Res.* **2017**, *260*, 984–994. [CrossRef]
62. Zheng, X.; Cai, Z. Privacy-Preserved Data Sharing towards Multiple Parties in Industrial IoTs. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 968–979. [CrossRef]
63. Sindhuja, P.N. Impact of information security initiatives on supply chain performance an empirical investigation. *Inf. Manag. Comput. Secur.* **2014**, *22*, 450–473. [CrossRef]
64. Kong, G.; Rajagopalan, S.; Zhang, H. Information Leakage in Supply Chains. *Springer Ser. Supply Chain. Manag.* **2017**, *5*, 313–341. [CrossRef]
65. Baihaqi, I.; Sohal, A.S. The impact of information sharing in supply chains on organisational performance: An empirical study. *Prod. Plan. Control* **2013**, *24*, 743–758. [CrossRef]
66. Butler, J.K. Behaviors, Trust, and Goal Achievement in a Win-Win Negotiating Role Play. *Group Organ. Manag.* **1995**, *20*, 486–501. [CrossRef]
67. Mentzer, J.T.; Keebler, J.S.; Nix, N.W.; Smith, C.D.; Zacharia, Z.G. Defining supply chain management. *J. Bus. Logist.* **2001**, *22*, 1–25. [CrossRef]
68. Fox, S. Moveable production systems for sustainable development and trade: Limitations, opportunities and barriers. *Sustainability* **2019**, *11*, 5154. [CrossRef]
69. Ask, A.; Stillström, C. Mobile Manufacturing Systems: Market Requirements and Opportunities. In Proceedings of the 2006 IJME-Intertech International Conference, Union, NJ, USA, 19–21 October 2006.
70. Alix, T.; Benama, Y.; Perry, N. Reconfigurable Manufacturing System Design: The Case of Mobile Manufacturing System. In *Advances in Production Management Systems. Innovative and Knowledge-Based Production Management in a Global-Local World. APMS 2014*; IFIP Advances in Information and Communication Technology; Grabot, B., Vallespir, B., Gomes, S., Bouras, A., Kiritsis, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 440.
71. Bengtsson, M.; Elfving, S.; Jackson, M. The factory-in-a-box concept and its maintenance application. In Proceedings of the 19th International Congress on Condition Monitoring and Diagnostic Engineering Management, Luleå, Sweden, 12–15 June 2006.
72. Peltokoski, M.; Lohtander, M.; Volotinen, J. Location Independent Manufacturing–Manufacturing Company Competitiveness in a Changing Business Environment. *Procedia Manuf.* **2017**, *11*, 863–870. [CrossRef]
73. Baldea, M.; Edgar, T.; Stanley, B.; Kiss, A. Modular Manufacturing Processes: Status, Challenges, and Opportunities. *AICHE J.* **2015**, *61*, 857–866. [CrossRef]
74. Wörsdörfer, D.; Lier, S.; Crasselt, N. Real options-based evaluation model for transformable plant designs in the process industry. *J. Manuf. Syst.* **2016**, *42*, 29–43. [CrossRef]
75. Wörsdörfer, D.; Lier, S.; Grünewald, M. Potential analysis model for case specific quantification of the degree of eligibility of innovative production concepts in the process industry. *Chem. Eng. Process. Process Intensif.* **2015**, *98*, 123–136. [CrossRef]
76. Lier, S.; Wörsdörfer, D.; Gesing, J. Business Models and Product Service Systems for Transformable, Modular Plants in the Chemical Process. In *Product-Service Integration for Sustainable Solutions*; Lecture Notes in Production Engineering; Meier, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 227–238. [CrossRef]
77. Klose, A.; Merkelbach, S.; Menschner, A.; Hensel, S.; Heinze, S.; Bittorf, L.; Kockmann, N.; Schäfer, C.; Szmais, S.; Eckert, M.; et al. Orchestration Requirements for Modular Process Plants in Chemical and Pharmaceutical Industries. *Chem. Eng. Technol.* **2019**, *42*, 2282–2291. [CrossRef]
78. Chokparova, Z.; Urbas, L. Utilization of Homomorphic Cryptosystems for Information Exchange in Value Chains. In Proceedings of the 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Västerås, Sweden, 7–10 September 2021; pp. 1–7. [CrossRef]
79. Wang, Y.; Wang, N.; Jiang, L.; Yang, Z.; Cui, V. Managing relationships with power advantage buyers: The role of supplier initiated bonding tactics in long-term buyer–supplier collaborations. *J. Bus. Res.* **2016**, *69*, 5587–5596. [CrossRef]
80. Bedwell, W.L.; Wildman, J.L.; DiazGranados, D.; Salazar, M.; Kramer, W.S.; Salas, E. Collaboration at work: An integrative multilevel conceptualization. *Hum. Resour. Manag. Rev.* **2012**, *22*, 128–145. [CrossRef]
81. Mayring, P. *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*; GESIS—Leibniz Institute for the Social Sciences: Klagenfurt, Austria, 2014.
82. Khakhar, P.; Rammal, H.G. Culture and business networks: International business negotiations with Arab managers. *Int. Bus. Rev.* **2013**, *22*, 578–590. [CrossRef]
83. Goworek, H.; Oxborrow, L.; Claxton, S.; McLaren, A.; Cooper, T.; Hill, H. Managing sustainability in the fashion business: Challenges in product development for clothing longevity in the UK. *J. Bus. Res.* **2020**, *117*, 629–641. [CrossRef]
84. Zafari, K.; Biggemann, S.; Garry, T. Mindful management of relationships during periods of crises: A model of trust, doubt and relational adjustments. *Ind. Mark. Manag.* **2020**, *88*, 278–286. [CrossRef]
85. Maxwell, J.A. *Qualitative Research Design: An Interactive Approach*, 3rd ed.; Sage Publication: Thousand Oaks, CA, USA, 2012.
86. Bhattacherjee, A. *Social Science Research: Principles, Methods, and Practices*; Textbooks Collection; University of South Florida: Tampa, FL, USA, 2012.
87. Crescentini, A.; Mainardi, G. Qualitative research articles: Guidelines, suggestions and needs. *J. Workplace Learn.* **2009**, *21*, 431–439. [CrossRef]

88. Almeida, F.; Superior, I.; Gaya, P.; Queirós, A.; Faria, D. Strengths and Limitations of Qualitative and Quantitative Research Methods. *Eur. J. Edu. Stu.* **2017**, *3*, 369–387. [CrossRef]
89. Tunio, M.N.; Jariko, M.A.; Børsen, T.; Shaikh, S.; Mushtaque, T.; Brahmi, M. How Entrepreneurship Sustains Barriers in the Entrepreneurial Process—A Lesson from a Developing Nation. *Sustainability* **2021**, *13*, 11419. [CrossRef]
90. Van Rijnsoever, F.J. (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE* **2017**, *12*, e0181689. [CrossRef] [PubMed]
91. Vasileiou, K.; Barnett, J.; Thorpe, S.; Young, T. Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Med. Res. Methodol.* **2018**, *18*, 148. [CrossRef] [PubMed]
92. Kuckartz, U.; Rädiker, S. *Working with Coded Segments and Memos*; Springer: Cham, Switzerland, 2019. [CrossRef]
93. Rudman, A.; Garbutt, M.; Seymour, L.F. Towards a Framework of Process Owner Competencies and Tasks. In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists, Association for Computing Machinery, Johannesburg, South Africa, 26–28 September 2016; pp. 1–7. [CrossRef]
94. Shahmoradi-Moghadam, H.; Schönberger, J. Joint optimization of production and routing master planning in mobile supply chains. *Oper. Res. Perspect.* **2021**, *8*, 100187. [CrossRef]
95. Becker, T.; Lier, S.; Werners, B. Value of modular production concepts in future chemical industry production networks. *Eur. J. Oper. Res.* **2019**, *276*, 957–970. [CrossRef]
96. Allman, A.; Zhang, Q. Dynamic location of modular manufacturing facilities with relocation of individual modules. *Eur. J. Oper. Res.* **2020**, *286*, 494–507. [CrossRef]
97. Fawcett, S.E.; Jones, S.L.; Fawcett, A.M. Supply chain trust: The catalyst for collaborative innovation. *Bus. Horiz.* **2012**, *55*, 163–178. [CrossRef]
98. Handfield, R.B.; Bechtel, C. The role of trust and relationship structure in improving supply chain responsiveness. *Ind. Mark. Manag.* **2002**, *31*, 367–382. [CrossRef]
99. The Economist. Germany's Conservative Economic Model Is Being Put to the Test. 2018. Available online: https://www.economist.com/special-report/2018/04/12/germanys-conservative-economic-model-is-being-put-to-the-test (accessed on 20 January 2022).
100. Mourtzis, D.; Doukas, M.; Psarommatis, F. A multi-criteria evaluation of centralized and decentralized production networks in a highly customer-driven environment. *CIRP Ann.* **2012**, *61*, 427–430. [CrossRef]
101. Shahmoradi-Moghadam, H.; Schönberger, J. Coordinated allocation production routing problem for mobile supply chains with shared factories. *Comput. Chem. Eng.* **2021**, *155*, 107501. [CrossRef]
102. Armbruster, D.; De Beer, C.; Freitag, M.; Jagalski, T.; Ringhofer, C. Autonomous control of production networks using a pheromone approach. *Phys. A Stat. Mech. Its Appl.* **2006**, *363*, 104–114. [CrossRef]
103. Ghosh, A.; Fedorowicz, J. The role of trust in supply chain governance. *Bus. Process Manag. J.* **2008**, *14*, 453–470. [CrossRef]
104. Pooe, D.; Mafini, C.; Loury-Okoumba, V.W. The influence of information sharing, supplier trust and supplier synergy on supplier performance: The case of small and medium enterprises. *J. Transp. Supply Chain. Manag.* **2015**, *9*, 1–11. [CrossRef]
105. Seppänen, R.; Blomqvist, K.; Sundqvist, S. Towards measuring inter-organizational trust-a review and analysis of the empirical research in 1990–2003. *Retrieved August* **2003**, *13*, 2009.
106. Rauch, E.; Matt, D.T.; Dallasega, P. Mobile On-site Factories-Scalable and distributed manufacturing systems for the construction industry. In Proceedings of the IEOM 2015-5th International Conference on Industrial Engineering and Operations Management, Dubai, United Arab Emerites, 3–5 March 2015. [CrossRef]
107. Manzini, R.; Lazzarotti, V. Intellectual Property Protection Mechanisms in Collaborative New Product Development. *R&D Manag.* **2016**, *46*, 579–595. [CrossRef]
108. Rauschecker, U.; Meier, M.; Muckenhirn, R.; Yip, A.L.K.; Jagadeesan, A.P.; Corney, J. Cloud-Based Manufacturing-as-a-Service Environment for Customized Products. In Proceedings of the eChallenges e-2011 Conference, Florence, Italy, 26–28 October 2011.
109. Bonatti, P.; De Coi, J.; Olmedilla, D.; Sauro, L. A Rule-Based Trust Negotiation System. *IEEE Trans. Knowl. Data Eng.* **2010**, *22*, 1507–1520. [CrossRef]